STUDY

Navigating the EU Cybersecurity Policy Ecosystem

A Comprehensive Overview of Legislation, Policies and Actors

Christina Rupp

June 27, 2024

Stiftung Neue Verantwortung is now interface

Since 2014, our team has worked on building an independent think tank and publishing well-researched analysis for everyone who wants to understand or shape technology policy in Germany. If we have learned something over the last ten years, it is that the challenges posed by technology cannot be tackled by any country alone, especially when it comes to Europe. This is why our experts have not only focused on Germany during the past years, but also started working across Europe to provide expertise and policy ideas on AI, platform regulation, cyber security, government surveillance or semiconductor strategies.

For 2024 and beyond, we have set ourselves ambitious goals. We will further expand our research beyond Germany and develop SNV into a fully-fledged European Think Tank. We will also be tapping into new research areas and offering policy insights to a wider audience in Europe, recruiting new talent as well as building expert communities and networks in the process. Still, one of the most visible steps for this year is our new name that can be more easily pronounced by our growing international community.

Rest assured, our experts will still continue to engage with Germany's policy debates in a profound manner. Most importantly, we will remain independent, critical and focused on producing cutting-edge policy research and proposals in the public interest. With this new strategy, we just want to build a bigger house for a wider community.

Please reach out to us with questions and ideas at this stage.

Table of Contents

Executive Summary

In recent years, the European Union (EU) has progressively become an important player in cyber and IT security policy. This is highlighted by an ever-expanding EU cybersecurity regulatory and policy ecosystem. For instance, the EU has set up dedicated entities like the European Union Agency for Cybersecurity (ENISA), adopted a horizontal legal framework with the Network and Information Security Directive (NIS), and introduced numerous further legal acts and policies addressing cyber and IT security, particularly during the 2019-2024 European Commission.

However, as a side effect and consequence of this evolution, taking stock, monitoring and navigating within the EU cybersecurity policy ecosystem has become an increasingly complex endeavor – not only for policy- and decision-makers in the public and private sectors but also for other stakeholders such as civil society and academia. At the same time, a comprehensive overview of the policy and actor landscape is essential for the effective implementation and coordination of cybersecurity legislation and policies within Member States and across the EU.

This compendium addresses this need by providing an extensive review of 154 EU legal acts and policies touching upon cyber and IT security and detailing the roles and activities of 26 key actors within the EU's institutional cybersecurity architecture. Additionally, the compendium offers an outlook on forthcoming EU cybersecurity policies, points to relevant resources for finding information on EU cybersecurity policy, and lists cybersecurity-related definitions employed by the identified documents.

With these components, the compendium is conceptualized to support Member States and stakeholders within and beyond the EU in navigating the EU cybersecurity policy ecosystem and gaining a deeper understanding of relevant interactions across policies and between actors.

While striving to be as comprehensive as possible, this compendium may not yet account for all EU legal acts and policy documents that include cyber or IT security-related elements, given the cross-cutting and rapidly evolving nature of EU cybersecurity policy. Therefore, the author welcomes input on additional documents to consider, information on related developments, and suggestions for improving this resource.

The Evolution of EU Cybersecurity Policy

When faced with a large-scale cyber incident, European Union (EU) Member States

bear the "primary responsibility for [...] response,"[1] along with their prerogative for national security matters (Art. 4(2) Treaty on the European Union, TEU). At the same time, a "significantly increasing level, complexity and scale of cybersecurity threats"[2] and the "public impact, cross-border nature and spill-over risk of cybersecurity threats"[3] make international cooperation and common approaches vital to address resulting challenges and contribute to a resilient cybersecurity posture across the EU.

Against this backdrop, it is not surprising that a lot has changed since the EU first adopted a Resolution on a common approach and specific actions in the area of network of information security in 2002, which called upon Member States, the European Commission, and industry stakeholders to enhance their efforts directed at increasing information security. For instance, in 2004, the EU established the European Network and Information Security Agency (ENISA), now called the European Union Agency for Cybersecurity; in 2013, the Commission and the EU's High Representative for Foreign Affairs and Security (HR/VP) published the first EU Cybersecurity Strategy, "An Open, Safe and Secure Cyberspace"; and in 2016, EU Member States and the European Parliament adopted the EU's first horizontal cybersecurity legislation, the first Network and Information Security (NIS) Directive.

A keyword search in the EU document database EUR-Lex typifies the evolution of EU action on cyber and IT security policy since 1990 (see Figure 1). For 2023 alone, the database provides 1144 results for documents mentioning "cybersecurity", "cyber security", or "information (IT) security".[4]

1 Council Conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises (13048/21).

2 Council Conclusions on the Future of Cybersecurity: implement and protect together (10133/24).

3 Ibid.

4 Given EUR-Lex's limitation of combining a maximum of two search terms, the numbers depicted in Figure 1 aggregate the results for two keyword searches for in-text mentionings for visual purposes: (1) "cyber security" or "cybersecurity" and (2) "information security" or "IT security." The search queries illustrated in both Figure 1 and 2 were conducted on April 5, 2024.

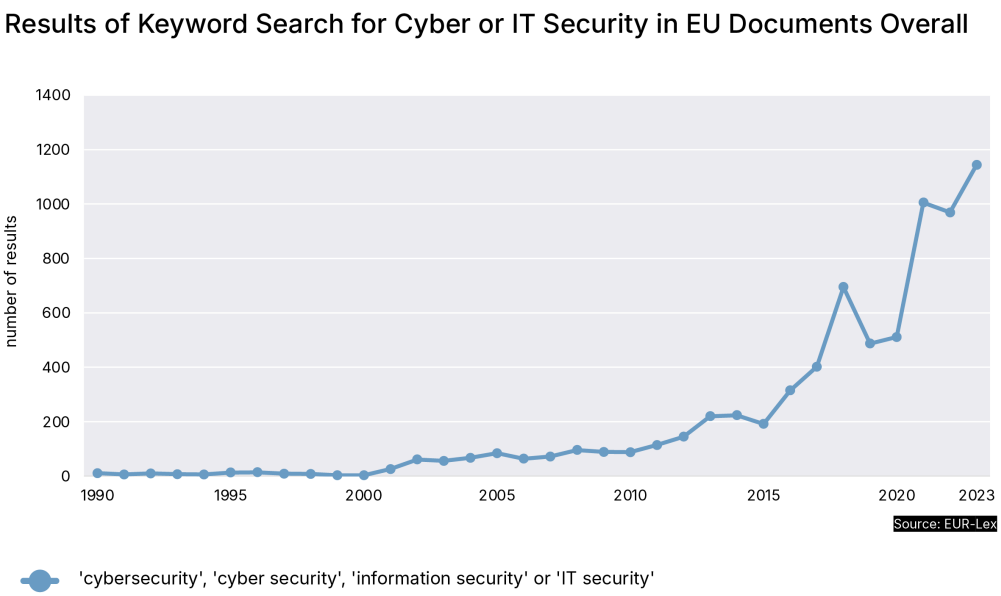


Figure 1: Results of Keyword Search for Cyber or IT Security in EU Documents Overall

This observable increase in mentions is not only valid for the search within EU documents overall. It is also reflected in an elevated number of EU legal acts touching upon cyber and/or IT security underpinning the EU's heightened regulatory activity on the matter (see Figure 2). Especially during the 2019-2024 Commission, there has been a notable increase in the number of EU legal acts explicitly mentioning cyber or IT security.

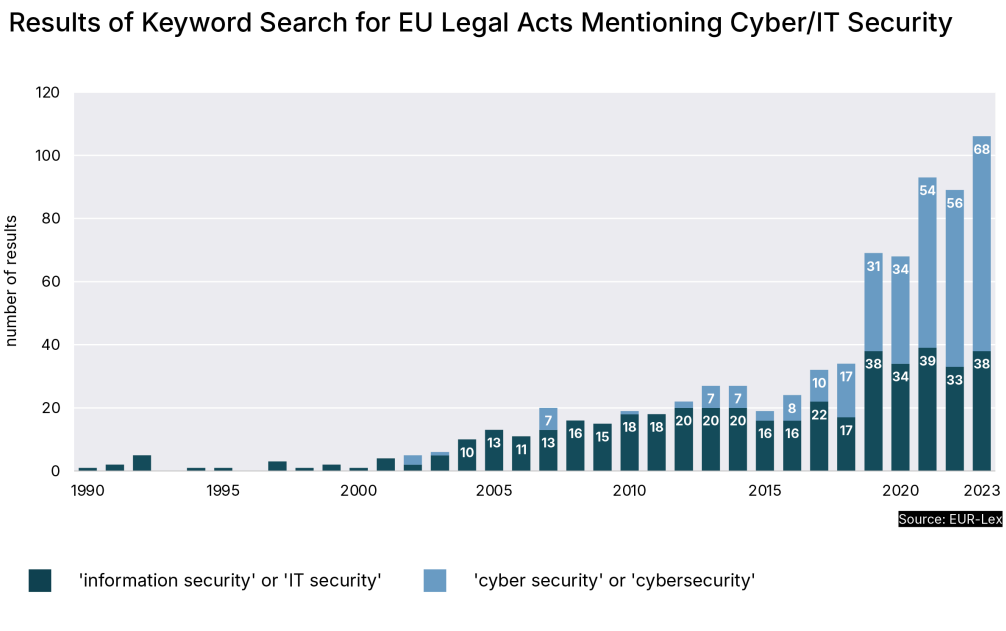


Figure 2: Results of Keyword Search for EU Legal Acts Mentioning Cyber/IT Security

These numbers indicate that the EU has progressively addressed and thus become an important player in the cyber and IT security policy realm, also resulting in an ever-expanding EU cybersecurity regulatory and policy ecosystem.

Not only these abstract numbers but also concrete regulatory and policy developments in various policy areas and sectors showcase the EU's elevated attention to cyber and IT security. The revised NIS Directive (2023); new legal acts on the resilience of critical entities (CER Directive, 2023), digital operational resilience of financial entities (DORA, 2023), and the cybersecurity of EU Institutions, Bodies, and Agencies (EUIBAs, Regulation 2023/2841); the establishment of a European cybersecurity certification scheme (Cybersecurity Act, 2019); the possibility of controlling the exports of cyber-surveillance tools in specific circumstances (Regulation 2021/821); the initiative for a Cybersecurity Skills Academy (2023); or the revised implementing guidelines of the EU's Cyber Diplomacy Toolbox (2023) are just a few very prominent cybersecurity-related developments at the EU level during the last few years.

What to Find Where in Compendium

As a side effect of the evolution of EU cybersecurity policy as outlined in Chapter 1, taking stock, monitoring and navigating within the EU cybersecurity policy[5] ecosystem has become an increasingly complex endeavor – for policy and decision-makers in the public and private sector as well as other stakeholders such as civil society and academia alike. The more a policy field evolves, the more important it becomes to maintain a comprehensive overview of efforts in place and underway. A policy field's cultivation also makes extensive coordination procedures among involved political levels and entities more necessary. Consequently, an overview of the policy and actor landscape is a fundamental prerequisite for effectively implementing and applying cybersecurity-related legislation and policies and informing a smart, structured, and sustainable cybersecurity policy, both at the EU and Member State level. An overview can further contribute to minimizing fragmentation by facilitating common understandings across Member States.

Given the absence of a publicly available comprehensive overview of EU cybersecurity policy, this compendium sets out to take stock and shed light on the current state of EU cybersecurity policy by providing:

5 For ease of understanding, the term 'EU cybersecurity policy', when used throughout this compendium, entails all documents listed and explained in this compendium, thus both legal acts and policies.

- an **explainer** of the different types of EU legal acts and policies describing their characteristics (Chapter 3);
- a **tabular overview** of cybersecurity-related EU legislation and policies (Chapter 4);
- a **comprehensive substantial review** of identified cybersecurity-related EU legislation and policies, the compendium's centerpiece (Chapters 5-12);
- 26 **profiles of actors** within the Union's institutional cybersecurity architecture, specifically EUIBAs and coordination bodies, describing their tasks, activities, and relationships among one another that are of relevance to cyber or IT security (Chapter 13);
- an **overview of relevant EU cybersecurity-related legislative and non-legislative initiatives** underway, which have not yet entered into force, also indicating relevant sources for tracking the progress of individual files (Chapter 14).

Within the scope of this compendium are all (i) EU legal acts published in the EU's Official Journal and (ii) EU policies that were published up until or were in force by May 31, 2024, and contain cybersecurity and/or information security-related components (explicitly or implicitly).[6] Hence, the imperative for inclusion in this compendium is that the legal act or policy touches upon security considerations in relation to network and information systems.

A total of 154 documents[7] were identified that match this scoping. Because EU cybersecurity policy is a dynamic and rapidly evolving field (as discussed in Chapter 1), this compendium highly likely does not yet account for all EU legal acts and policy documents that fall within the delineated scope. Therefore, we greatly appreciate any pointers or suggestions for additional documents to which the scope applies.

Every identified document was assigned to one of eight policy areas, which are each dedicated a chapter within this compendium:

6 In accordance, for instance, the compendium does not touch upon the Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, which entered into force in June 2024, or the proposed Cyber Resilience Act and Cyber Solidarity Act which were close to adoption at the time of the compendium's publication.

7 The number includes all documents of a type explained in Chapter 3. Prior legal acts that are no longer in force were omitted from the count. The numbers are the following for each policy area: 17 (overarching policies), 31 (internal market), 12 (economy, monetary and commercial policy), 13 (internal security, justice and law enforcement), 21 (energy, transport and health policy), 10 (education, research and space policy), 44 (foreign and security policy) and 6 (cybersecurity of EUIBAs).

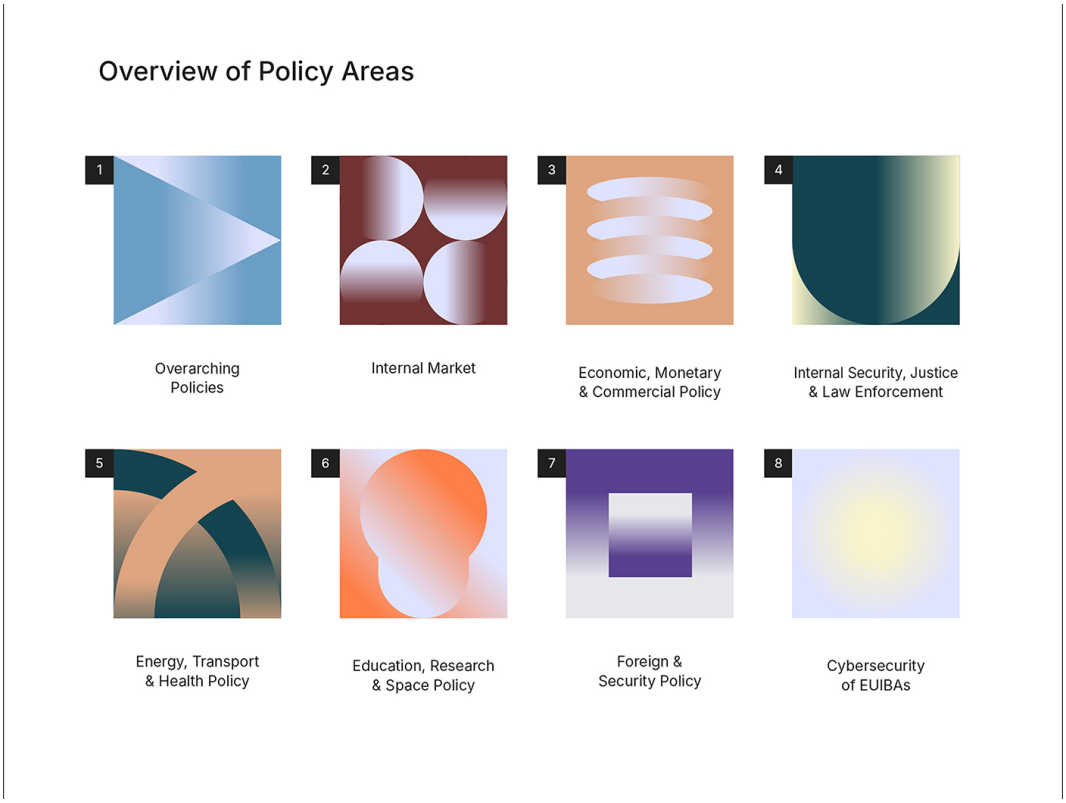


Figure 3: Policy Areas of Compendium

These policy areas reflect the cross-cutting nature of cyber and IT security policy. The assignment of legal acts and policies to these policy areas further builds on the principle of conferral, meaning that the EU needs competence – exclusively or shared with the Member States – to take action in a particular policy field (Art. 5 TEU). In accordance, any competencies not specified in EU primary law "remain with the Member States" (Art. 5(2) TEU).[8] Thus, any EU legal act or EU policy addressing cybersecurity must also be traceable to a specific area in which the EU holds competence. Against this backdrop, each section (except for policy area 1 (overarching policies) and 8 (cybersecurity of EUIBAs)) explains the EU's mandate and competence in the respective policy area at the outset.

Within each policy area chapter, the review of a legal act or policy is either covered in the form of a dedicated deep dive or in chronological order within issue area-specific sections. The summaries of each legal act or policy's cybersecurity-related components provide a comprehensive, but not necessarily fully exhaustive overview. Accordingly, the summaries are deliberately not meant to represent a legally authoritative synopsis or guideline but rather seek to highlight

8 The EU must further comply with the principle of subsidiarity, meaning that "in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member State" (Art. 5(3) TEU). Moreover, as a general rule, "the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties" (Art. 5(4) TEU), also known as the principle of proportionality.

areas and aspects of policy relevance and importance. As much as deemed useful, the policy reviews refer to the legal act's or policy's original wording. Inherently actor-specific provisions of acts and policies are discussed within the respective actor profiles in Chapter 13.

In addition to these chapters, the compendium's annex includes

- a **list of relevant EU websites** offering information on EU cybersecurity policy and updates on related policy developments (Annex I);
- an **overview of cybersecurity-related definitions** used within the identified EU documents (Annex II);
- and a **list of abbreviations** used throughout this compendium (Annex III).

Through all of these elements, this compendium can contribute to Member States' recent call for the need for comprehensible overviews on "the relevant horizontal and sectoral legislative frameworks and their interplay" as well as "the roles and responsibilities of all relevant EU entities, stakeholders and networks [...] active in the cybersecurity domain."[9] In addition, the compendium is not only of interest to European decision-makers, entities and stakeholders seeking to navigate within the complex legislative and policy environment. It can also assist actors in other parts of the world, such as legislators, regulatory bodies, private sector entities seeking to sell their products in the EU internal market or non-governmental organizations, in better understanding the EU's approach to cybersecurity and its institutional landscape across various policy areas.

EU Legislation and Policies: A Basic Explainer

Before examining what specific legislation and policies say on cyber and IT security (policy), it is important to understand the types of documents covered within this compendium. To this end, this Chapter explains their characteristics, involved actors, and, if applicable, the extent to which the various document types are legally binding.

EU legislation can come in five different types that differ in their application, binding nature and addressee (Art. 288 Treaty on the Functioning of the European Union, TFEU). While Member States hold the primary responsibility for the correct and timely implementation of EU legal acts, the Commission (in its role as the

9 Council Conclusions on the Future of Cybersecurity: implement and protect together (10133/24).

"guardian of the treaties"[10]) takes on the task of ensuring adherence.[11]

Regulations are EU legal acts that "have general application, are binding in their entirety and are directly applicable"[12] in all EU Member States. They do not require national transposition and can be invoked directly before Member States' national courts.

Directives are EU legal acts that have general application and may be addressed to either one, several, or all EU Member States. Unlike regulations, directives are binding only "as to the result to be achieved,"[13] granting Member States the power and flexibility to "choose the form and methods"[14] for achieving the specified result. Transposition into national law is required before directives become applicable in the Member States to which they are addressed to.

Decisions are EU legal acts that may be of general or specific application and "may have one or more addressees (one or several EU Member States, one or several companies or individuals)."[15] Like regulations, they are binding in their entirety and directly applicable.

These three types of legislation are adopted through one of the EU's two legislative procedures, the **ordinary legislative procedure** or the **special legislative procedure** (Art. 289 and 294 TFEU). The ordinary legislative procedure is the most common legislative procedure of the EU. As co-legislators, the European Parliament and the Council of the EU jointly adopt legislative acts proposed by the European Commission, which is the only EU institution with the power to initiate such acts.[16] The special legislative procedure is only used in certain cases as stipulated in particular treaty provisions. In contrast to the ordinary legislative procedure, the Council acts as the sole legislator. Yet, the Council must either receive consent on the legislative proposal from the European Parliament or consult it.[17]

In addition to legal acts adopted through the ordinary or special legislative

---

10 European Commission (n.d.): What the European Commission does in law.

11 For instance, if an EU country fails to "fully incorporate a directive into its national law" (EUR-Lex (n.d.): Enforcement of EU law) by the specified deadline or misapplies EU law, the Commission is empowered to take corrective measures. Corrective measures employed by the European Commission include the pre-infringement process known as EU Pilot and the subsequent infringement procedure. EU Pilot is used when the Commission identifies a "potential non-compliance with EU law" (European Commission (n.d.): EU Pilot). It is "a mechanism for informal dialogue between the Commission and the Member State" (ibid.) in question and aims to resolve the issue through cooperation. If a breach is evident, acknowledged, or persists following the pre-infringement process, a formal infringement procedure may be initiated, potentially leading to a referral to the Court of Justice of the European Union. In certain instances, the Commission may request the imposition of financial sanctions on the concerned Member State(s). For further information, see European Commission (n.d.): Implementing EU law and EUR-Lex (n.d.): Enforcement of EU law.

12 EUR-Lex (2022): European Union regulations.

13 EUR-Lex (2022): European Union directives.

14 Ibid.

15 EUR-Lex (2021): European Union decisions.

16 For more information on the adoption process within the EU's ordinary legislative procedure, see Council of the EU (n.d.): The ordinary legislative procedure, EUR-Lex (n.d.): Ordinary legislative procedure (Codecision), and EUR-Lex (n.d.): Trilogue.

17 For more information on the EU's special legislative procedure, see EUR-Lex (n.d.): Special legislative procedure.

procedures, which can be categorized as legislative acts, the European Commission, or exceptionally the Council, can adopt non-legislative acts. **Delegated and implementing acts**, for instance, a delegated regulation or an implementing directive, are the most common of such acts (Art. 291 and 292 TFEU).[18] Delegated acts by the European Commission supplement or amend non-essential parts of legislative acts. They are adopted, for instance, when they are provided for within a particular legal act or when adjustments to legislative acts are necessary to incorporate advancements in technical and scientific fields. Experts from EU Member States are consulted by the Commission before the adoption of such acts. Implementing acts, adopted by the Commission or, in exceptional cases, the Council, establish "uniform conditions for the implementation"[19] of legislative acts. These acts commonly address administrative or technical aspects and are adopted following consultations with committees consisting of technical experts from EU Member States.

In addition to regulations, directives, and decisions, EU legal acts also comprise **recommendations** and **opinions** as non-legally binding types of outputs.[20] Recommendations, on the one hand, allow EU institutions to express their views and propose a course of action "without imposing any legal obligation"[21] on the addressee. Opinions, on the other hand, allow EU institutions to articulate statements "without imposing any legal obligation on the subject of the opinion."[22]

Apart from legal acts, the Council of the EU may also articulate its political stance on matters within the EU's sphere of activity and adopt non-legally binding documents, reflecting "political commitments or positions."[23] **Council conclusions**, for instance, may be adopted following a debate in a Council meeting and "contain a political position on a specific topic."[24] **Council resolutions** typically outline forthcoming initiatives foreseen in a specific policy domain. While both examples of documents have no legal effect, they may call upon the Commission or other EUIBAs to propose specific measures or pursue further actions.

Moreover, the Commission can publish other types of non-legally binding documents, such as **Communications** on a specific topic. Sometimes the Commission does so together with the High Representative of the Union for Foreign Affairs and Security Policy / Vice President of the Commission (HR/VP) in the form of **Joint Communications**.

18 For further information, see EUR-Lex (n.d.): Delegated acts and EUR-Lex (n.d.): Implementing acts.

19 EUR-Lex (n.d.): Implementing acts.

20 For further information, see EUR-Lex (n.d.): Recommendation and EUR-Lex (n.d.): Opinion.

21 European Commission (n.d.): Types of EU law.

22 Ibid.

23 Council of the EU (n.d.): Council conclusions and resolutions.

24 Ibid.

Table 1: Overview of Types of EU Legal Acts and Policies

	Adopted by	Binding Nature	Addressee	Cybersecurity-Related Example
Regulation	• European Parliament and the Council of the EU (ordinary legislative procedure) • Council of the EU (special legislative procedure, in exceptional cases implementing acts) • European Commission (delegated or implementing act)	Binding in their entirety	All EU Member States	Digital Operational Resilience Act (DORA, 2022/2554)
Directive		Binding as to the result to be achieved	One, several, or all EU Member States	Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive, 2022/2555)
Decision		Binding in their entirety	One or several EU Member States, one or several companies or individuals	Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States
Delegated Act (e.g. Delegated Regulation)	European Commission	Binding in their entirety	*Depends on the legislative act it amends or supplements*	Commission Delegated Regulation supplementing Directive 2022/2557 of the European Parliament and of the Council by establishing a list of essential services (2023/2450)
Implementing Act (e.g. Implementing Decision)	European Commission, in exceptional cases the Council of the EU	Binding in their entirety	*Depends on the legislative act it aims to implement*	Commission Implementing Regulation laying down rules for the application of Regulation 2019/881 (2024/482)
Recommendation	European Commission, other EU institutions e.g. European Parliament, Council of the EU, European Central Bank	Not binding		Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises
Opinion		Not binding		NA
Council conclusions	Council of the EU	Not binding		Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities

Council resolution		Not binding	Council Resolution on Encryption
Communication	European Commission (sometimes as a Joint Communication with HR/VP)	Not binding	Joint Communication on the EU Policy on Cyber Defence (JOIN(2022) 49 final)

Tabular Overview of EU Cybersecurity Policy

The following tabular overview lists all the EU legal acts and policies covered within this compendium. The month/year column specifies the date of their respective entry into force (for legal acts) or the date of their publication (for policies). The tables also specify the document's type as explained in Chapter 3, the policy area assigned to it and lays out in which chapter and section the corresponding policy review can be found. If applicable, the tables also indicate any (repealed) previous legislation of cybersecurity relevance and/or subsequent corresponding legal acts (such as implementing/delegated acts), guidelines or other documents of relevance. In the latter cases, the date displayed in the month/year column specifies the date of the entry into force/publication of the initial document.[25] Drawing on EUR-Lex information, the table also include the "responsible body" in whose purview a particular legal act falls at the bottom of a row, if such an indication was available (e.g. [DG CONNECT]).

Overarching Policies

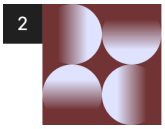
Month/ Year	Legal Act/Policy	Type	Section
May 2024	Council conclusions on the Future of Cybersecurity: implement and protect together (10133/24)	Council Conclusions	5.1 General

25 For instance, for the Cyber Diplomacy Toolbox the table lists 'June 2017', even though subsequent documents of relevance, revised implementing guidelines, were issued in June 2023.

April 2024	Commission Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography	Recommendation	5.4 Emerging Technologies
December 2023	Commission Recommendation on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament (2023/2829) [DG JUST]	Recommendation	5.5 Democratic Processes
December 2022	Decision of the European Parliament and of the Council establishing the Digital Decade Policy Programme 2030 (2022/2481) Subsequent corresponding legal acts, guidelines or other documents of relevance: • September 2023: 2023 Report on the state of the Digital Decade • n.d.: National Digital Decade strategic roadmaps [DG CONNECT]	Decision	5.3 Digital Transformation
October 2021	Council Conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises (13048/21)	Council Conclusions	5.2 Incident and Crisis Response
June 2021	Commission Recommendation on building a Joint Cyber Unit (2021/1086)	Recommendation	5.2 Incident and Crisis Response
May 2021	Regulation establishing the Digital Europe Programme (2021/694) Subsequent corresponding legal acts, guidelines or other documents of relevance: • December 2023: Digital Europe - Cybersecurity Work Programme 2023-2024 [DG CONNECT]	Regulation	5.3 Digital Transformation
March 2021	Communication: 2030 Digital Compass: the European way for the Digital Decade (COM(2021) 118 final)	Communication	5.3 Digital Transformation
December 2020	Communication from the Commision on the European Democracy Action Plan (COM(2020) 790 final)	Communication	5.5 Democratic Processes
December 2020	Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final) Subsequent corresponding legal acts, guidelines or other documents of relevance:	Joint Communication	5.1 General

	• June 2021: First implementation report on the EU Cybersecurity Strategy (2021/0166 (NLE) and JOIN(2021) 14 final) • March 2021: Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade (6722/21) Previous strategies: • 2017: Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (JOIN(2017) 450 final) [September 2017) and Council Conclusions on the Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" (14435/17) [November 2017] • February 2013: Joint Communication: EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final)		
July 2020	EU Security Union Strategy (COM(2020) 605 final) Subsequent corresponding legal acts, guidelines or other documents of relevance: • May 2024: Seventh Progress Report (COM(2024) 198 final) • October 2023: Sixth Progress Report (COM(2023) 665 final) • December 2022: Fifth Progress Report (COM(2022) 745 final) • May 2022: Fourth Progress Report (COM(2022) 252 final) • December 2021: Third Progress Report COM(2021) 799 final • June 2021: Second Progress Report (COM(2021) 440 final) • December 2020: First Progress Report (COM(2020) 797 final)	Strategy	5.1 General
March 2019	Council conclusions on cybersecurity capacity and capabilities building in the EU (7737/19)	Council Conclusions	5.1 General
June 2018	Council conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises (10086/18)	Council Conclusions	5.2 Incident and Crisis Response
September 2017	Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises (2017/1584)	Recommendation	5.2 Incident and Crisis Response

Internal Market



Month/ Year	Legal Act/Policy	Type	Section
September 2023	Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (2023/1781, Chips Act) [DG CONNECT]	Regulation	6.6 General Rules
July 2023	Regulation on machinery (2023/1230) [DG GROW]	Regulation	6.3 Product Safety and Market Surveillance
June 2023	Communication from the Commission: Implementation of the 5G cybersecurity Toolbox (C(2023) 4049 final)	Communication	6.2 Electronic Communications Networks
May 2023	Regulation on general product safety (2023/988) [DG JUST]	Regulation	6.3 Product Safety and Market Surveillance
January 2023	Directive on measures for a high common level of cybersecurity across the Union (2022/2555, NIS 2 Directive) Subsequent corresponding legal acts, guidelines or other documents of relevance: • September 2023: Commission Guidelines on the application of Article 3(4) of Directive (EU) 2022/2555 (NIS 2 Directive) • September 2023: Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive) Previous legislation: Directive concerning measures for a high common level of security of network and information systems across the Union (2016/1148, NIS Directive) • January 2018: Commission Implementing Regulation laying down rules for application of Directive 2016/1148 as regards	Directive	6.1 Deep Dives

	further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (2018/151) • February 2017: Commission Implementing Decision laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (2017/179) [DG CONNECT]		
October 2022	Council conclusions on ICT supply chain security (13664/22)	Council Conclusions	6.7 Council Conclusions and Resolutions
September 2022	Regulation on contestable and fair markets in the digital sector (2022/1925, Digital Markets Act) [DG COMP]	Regulation	6.6 General Rules
June 2022	Regulation on European data governance (2022/868, Data Governance Act) [DG CONNECT]	Regulation	6.5 Data Protection and Data Economy
December 2020	Council Conclusions on the cybersecurity of connected devices (2020/C 427/04)	Council Conclusions	6.7 Council Conclusions and Resolutions
December 2020	Council Resolution on Encryption - Security through encryption and security despite encryption (13084/1/20)	Council Resolution	6.7 Council Conclusions and Resolutions
January 2020	Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures Subsequent corresponding legal acts, guidelines or other documents of relevance: • July 2020: Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity • June 2023: Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity	Publication	6.2 Electronic Communications Networks
December 2019	Council Conclusions on the significance of 5G to the European	Council Conclusions	6.2 Electronic Communications

	Economy and the need to mitigate security risks linked to 5G (2019/C 414/03)		Networks
December 2019	Regulation on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users (2019/2144) Subsequent corresponding legal acts, guidelines or other documents of relevance: • August 2022: Commission Implementing Regulation laying down rules for the application of Regulation 2019/2144 as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles (2022/1426) [DG GROW]	Regulation	6.3 Product Safety and Market Surveillance
May 2019	Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (2019/881, Cybersecurity Act) Subsequent corresponding legal acts, guidelines or other documents of relevance: • February 2024: Commission Implementing Regulation laying down rules for the application of Regulation 2019/881 as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (2024/482) • February 2024: Union Rolling Work Programme for European cybersecurity certification (SWD(2024) 38 final) • December 2023: Commission Decision approving a working arrangement between the European Union Agency for Cybersecurity (ENISA) and the United States Cybersecurity and Infrastructure Security Agency (CISA) in the area of cybersecurity (C(2023) 8553 final) • June 2023: Commission Decision approving the Working Arrangement between	Regulation	6.1 Deep Dives

	the European Union Agency for Cybersecurity (ENISA) and the National Cybersecurity Coordination Center of Ukraine (NCCC) and the Administration of the State Service of Special Communication and Information Protection of Ukraine (the Administration of SSSCIP) in the area of cybersecurity (C(2023) 4016 final) Previous legislation: • June 2013: Regulation concerning the European Union Agency for Network and Information Security (ENISA) (526/2013) [DG CONNECT]		
March 2019	Commission Recommendation Cybersecurity of 5G networks (2019/534) [DG CONNECT]	Recommendation	6.2 Electronic Communications Networks
December 2018	Directive establishing the European Electronic Communications Code (2018/1972, Electronic Communications Code) [DG CONNECT]	Directive	6.2 Electronic Communications Networks
April 2017	Regulation on in vitro diagnostic medical devices (2017/746) [DG SANTE]	Regulation	6.3 Product Safety and Market Surveillance
April 2017	Regulation on medical devices (2017/745) Subsequent corresponding legal acts, guidelines or other documents of relevance: • November 2021: Commission Implementing Regulation laying down rules for the application of Regulation 2017/745 as regards the European Database on Medical Devices (Eudamed) (2021/2078) [DG GROW]	Regulation	6.3 Product Safety and Market Surveillance
May 2016	Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (2016/679, General Data Protection Regulation (GDPR) [DG JUST]	Regulation	6.5 Data Protection and Data Economy
August 2014	Regulation on electronic identification and trust services for electronic transactions in the internal market (910/2014, eIDAS Regulation) Subsequent corresponding legal acts,	Regulation	6.4 Electronic Identification

	guidelines or other documents of relevance: • May 2024: Regulation amending Regulation 910/2014 as regards establishing the European Digital Identity Framework (2024/1183) • September 2015: Commission Implementing Regulation on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (2015/1502) [DG CONNECT]		
May 2014	Directive on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (2014/53) Subsequent corresponding legal acts, guidelines or other documents of relevance: • October 2021: Commission Delegated Regulation supplementing Directive 2014/53/EU with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f) (2022/30) [DG GROW]	Directive	6.2 Electronic Communications Networks

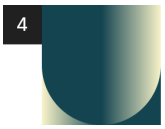
Economic, Monetary and Commercial Policy

Month/ Year	Legal Act/Policy	Type	Section
June 2023	Regulation on markets in crypto-assets (2023/1114) [DG FISMA]	Regulation	7.2 Digital Finance
January 2023	Regulation on digital operational resilience for the financial sector (2022/2554, DORA) [DG FISMA]	Regulation	7.1 Deep Dive
May 2021	Regulation setting up a Union regime for the	Regulation	7.3 Export

	control of exports, brokering, technical assistance, transit and transfer of dual-use items (2021/821) Subsequent corresponding legal acts, guidelines or other documents of relevance: • January 2024: Commission Recommendation on guidelines setting out the methodology for data gathering and processing for the preparation of the annual report on the control of exports, brokering, technical assistance, transit and transfer of dual-use items (2024/214) • January 2024: White Paper on export controls (COM(2024) 25 final) • September 2023: Commission Delegated Regulation as regards the list of dual-use items (2023/2616) • September 2022: 2022 Export Control Annual Report (COM(2022) 434 final) • October 2021: Commission Delegated Regulation as regards the list of dual-use items (2022/1) • February 2021: 2020 Annual Report (COM(2021) 42 final) [DG TRADE]		Controls
February 2021	Regulation establishing the Recovery and Resilience Facility (2021/241) [DG ECFIN]	Regulation	7.4 Investments and Financing
December 2019	Regulation establishing a European Supervisory Authority (European Banking Authority) (1093/2010)	Regulation	Covered in Chapter 13
December 2019	Regulation establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority) (1094/2010)	Regulation	Covered in Chapter 13
December 2019	Regulation establishing a European Supervisory Authority (European Securities and Markets Authority) (1095/2010)	Regulation	Covered in Chapter 13
April 2019	Regulation establishing a framework for the screening of foreign direct investments into the Union (2019/452) Subsequent corresponding legal acts, guidelines or other documents of relevance: • October 2023: Third Annual Report on the screening of foreign direct investments into the Union (COM(2023) 590 final) • September 2022: Second Annual Report on the screening of foreign direct investments into the Union (COM(2022) 433 final) • November 2021: First Annual Report on the screening of foreign direct investments into the Union (COM(2021) 714 final) [DG TRADE]	Regulation	7.4 Investments and Financing
January 2016	Directive on payment services in the internal market (2015/2366) Subsequent corresponding legal acts, guidelines	Directive	7.5 Payment Services

	or other documents of relevance: • January 2023: Directive amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (2022/2556) [DG FISMA]		

Internal Security, Justice and Law Enforcement



Month/ Year	Legal Act/Policy	Type	Section
May 2023	Regulation establishing a collaboration platform to support the functioning of joint investigation teams (2023/969) [DG JUST]	Regulation	8.3 IT Systems of the Area of Freedom, Security and Justice
January 2023	Directive on the resilience of critical entities and repealing Council Directive 2008/114 (2022/2557, CER Directive) Subsequent corresponding legal acts, guidelines or other documents of relevance: • November 2023: Commission Delegated Regulation supplementing Directive 2022/2557 by establishing a list of essential services (2023/2450) [DG HOME]	Directive	8.1 Deep Dive
June 2022	Regulation on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system) (2022/850) [DG JUST]	Regulation	8.3 IT Systems of the Area of Freedom, Security and Justice
July 2021	Regulation establishing the Internal Security Fund (2021/1149)	Regulation	8.4 Judicial and Police Cooperation
February 2021	Council conclusions on the permanent continuation of the EU Policy Cycle for organised and serious international crime: EMPACT 2022 + (6481/21) Subsequent corresponding legal acts, guidelines or other documents of relevance: • May 2023: EMPACT Terms of Reference (8975/23)	Council Conclusions	8.5 Council Conclusions

	• March 2023: Council conclusions setting the EU's priorities for the fight against serious and organised crime for EMPACT 2022-2025 (7101/23) • December 2022: EMPACT Operational Action Plan 2023: Cyber attacks (13747/1/22)		
December 2018	Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) (2018/1727) [DG JUST]	Regulation	Covered in Chapter 13
December 2018	Regulation on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) (2018/1726) Previous legislation: Regulation establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (1077/2011)	Regulation	8.3 IT Systems of the Area of Freedom, Security and Justice
October 2018	Regulation establishing a European Travel Information and Authorisation System (ETIAS) (2018/1240) [DG HOME]	Regulation	8.3 IT Systems of the Area of Freedom, Security and Justice
June 2016	Council conclusions on improving criminal justice in cyberspace (10007/16)	Council Conclusions	8.5 Council Conclusions
June 2016	Regulation on the European Union Agency for Law Enforcement Cooperation (Europol) (2016/794) [DG HOME]	Regulation	Covered in Chapter 13
September 2013	Directive on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013/40) [DG HOME]	Directive	8.2 Cybercrime

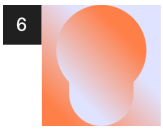
Energy, Transport and Health Policy

Month/ Year	Legal Act/Policy	Type	Section
October 2023	Directive on energy efficiency (2023/1791) • December 2018: Directive amending Directive 2012/27 on energy efficiency (2018/2002)	Directive	9.1 Energy

December 2020	Commission Delegated Regulation supplementing Regulation 376/2014 as regards the common European risk classification scheme (2020/2034) [DG MOVE]	Regulation	9.2 Civil Aviation
December 2020	Commission Implementing Regulation amending Implementing Regulation 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures (2019/1583) [DG MOVE]	Regulation	9.2 Civil Aviation
July 2019	Directive on common rules for the internal market for electricity and amending Directive 2012/27 (2019/944) [DG ENER]	Directive	9.1 Energy
July 2019	Regulation on risk-preparedness in the electricity sector (2019/941)	Regulation	9.1 Energy
July 2019	Regulation on the internal market for electricity (2019/943) Subsequent corresponding legal acts, guidelines or other documents of relevance: • October 2020: Commission Implementing Decision establishing priority lists for the development of network codes and guidelines for electricity for the period from 2020 to 2023 and for gas in 2020 (2020/1479) [DG ENER]	Regulation	9.1 Energy
April 2019	Commission Recommendation on cybersecurity in the energy sector (2019/553)	Recommendation	9.1 Energy
February 2019	Commission Recommendation on a European Electronic Health Record exchange format (2019/243)	Recommendation	9.3 Health
September 2018	Regulation on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency (2018/1139) Subsequent corresponding legal acts, guidelines or other documents of relevance: • September 2023: Commission Implementing Regulation laying down technical requirements and administrative procedures for the approval of organisations involved in the design or production of air traffic management/air navigation services systems and constituents and amending Implementing Regulation 2023/203 (2023/1769) • February 2023: Commission Implementing Regulation laying down rules for the application of Regulation 2018/1139, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations (2023/203)	Regulation	9.2 Civil Aviation

	• October 2022: Commission Delegated Regulation laying down rules for the application of Regulation 2018/1139, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations (2022/1645) • January 2021: Commission Delegated Regulation amending Regulation 139/2014 as regards runway safety and aeronautical data (2020/2148) • June 2019: Commission Implementing Regulation on the rules and procedures for the operation of unmanned aircraft (2019/947) • March 2017: Commission Implementing Regulation laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight (2017/373) [DG MOVE]		
April 2018	Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society (COM(2018) 233 final)	Communication	9.3 Health
December 2017	Council conclusions on Health in the Digital Society — making progress in data-driven innovation in the field of health (2017/C 440/05)	Council Conclusions	9.3 Health
April 2011	Directive on the application of patients' rights in cross-border healthcare (2011/24) Subsequent corresponding legal acts, guidelines or other documents of relevance: • June 2022: Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU • October 2019: Commission Implementing Decision providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth (2019/1765) • n.d.: EHealth Network Rules of Procedure [DG SANTE]	Directive	9.3 Health

Education, Research and Space Policy



Month/ Year	Legal Act/Policy	Type	Section
November 2023	Council Recommendation on improving the provision of digital skills and competences in education and training (C/2024/1030)	Recommendation	10.1 Education
November 2023	Council Recommendation on the key enabling factors for successful digital education and training (C/2024/1115)	Recommendation	10.1 Education
April 2023	Communication from the Commission: Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy') (COM(2023) 207 final)	Communication	10.1 Education
March 2023	Regulation establishing the Union Secure Connectivity Programme for the period 2023-2027 (2023/588) [DG DEFIS]	Regulation	10.3 Space
June 2021	Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (2021/887) Corresponding legal acts, guidelines or other documents of relevance: • March 2023: Strategic Agenda • October 2021: Guidelines on the assessment of the capacity of National Coordination Centres to manage funds to fulfil the mission and objectives laid down in Regulation 2021/887 • January 2021: Decision on the location of the seat of the European Cybersecurity Industrial, Technology and Research Competence Centre (2021/4) [DG CONNECT]	Regulation	10.2 Research
May 2021	Council Decision establishing the Specific Programme implementing Horizon Europe – the Framework Programme for Research and Innovation (2021/764) Subsequent corresponding legal acts, guidelines or other documents of relevance: • March 2024: Commission Implementing Decision on adopting the 2025-2027 strategic research and innovation plan under the Specific Programme implementing Horizon Europe – The Framework Programme for Research and Innovation (C(2024) 1741 final) • March 2023: Horizon Europe 2023-2024 Work Programme - Cluster 3 Previous legislation: Council Decision establishing the specific programme	Decision	10.2 Research

	implementing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) (2013/743) [DG RTD]		
May 2021	Regulation establishing the Union Space Programme and the European Union Agency for the Space Programme (2021/696) Subsequent corresponding legal acts, guidelines or other documents of relevance: • May 2021: Council Decision on the security of systems and services deployed, operated and used under the Union Space Programme which may affect the security of the Union (2021/698) [DG DEFIS]	Regulation	10.3 Space

Foreign and Security Policy

Month/ Year	Legal Act/Policy	Type	Section
February 2024	Council Decision on Union support for the activities of the International Atomic Energy Agency in the area of nuclear security (2024/656) Prior decisions: • November 2020: Council Decision on Union support for the activities of the International Atomic Energy Agency (IAEA) in the areas of nuclear security and in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (2020/1656) • October 2013: Council Decision on the Union support for the activities of the International Atomic Energy Agency in the areas of nuclear security and verification and in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (2013/517) [HR/VP, EEAS]	Council Decision	11.7 Support to Other International Organizations
May 2023	Council Conclusions on EU Policy on	Council	11.4 Cyber

	Cyber Defence (9618/23)	Conclusions	Defence
May 2023	Council Decision on an assistance measure under the European Peace Facility to support the Georgian Defence Forces (2023/920) Previous documents of relevance: • December 2022: Council Decision on an assistance measure under the European Peace Facility to support the Georgian Defence Forces (2022/2352) [HR/VP, EEAS]	Council Decision	11.4 Cyber Defence
May 2023	Council Decision on an assistance measure under the European Peace Facility to support the Armed Forces of the Republic of Moldova (2023/921) [HR/VP, EEAS]	Council Decision	11.4 Cyber Defence
April 2023	Council Decision on a European Union Partnership Mission in Moldova (2023/855) [HR/VP, EEAS]	Council Decision	11.4 Cyber Defence
November 2022	Joint Communication on the EU Policy on Cyber Defence (JOIN(2022) 49 final)	Joint Communication	11.4 Cyber Defence
June 2022	Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (10016/22)	Council Conclusions	11.5 Hybrid Threats and Campaigns
June 2022	Council Decision on an assistance measure under the European Peace Facility to support the Armed Forces of the Republic of Moldova (2022/1093) [HR/VP, EEAS]	Council Decision	11.4 Cyber Defence
May 2022	Council conclusions on the development of the European Union's cyber posture (9364/22)	Council Conclusions	11.1 Strategic Documents
March 2022	A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security (7371/22)	Other	11.1 Strategic Documents
December 2021	Council Decision on an assistance measure under the European Peace Facility to support the Ukrainian Armed Forces (2021/2135) [HR/VP, EEAS]	Council Decision	11.4 Cyber Defence
December 2021	Joint Communication: The Global Gateway (JOIN(2021) 30 final)	Communication	11.6 Development Cooperation and Cyber Capacity-Building
September	European Union Military Vision and	Other	11.4 Cyber

2021	Strategy on Cyberspace as a Domain of Operations (EEAS(2021) 706 REV4)		Defence
June 2021	Council Decision in support of the Cyber Security and Resilience and Information Assurance Programme of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (2021/1026) • July 2023: Council Decision amending Decision (CFSP) 2021/1026 in support of the Cyber Security and Resilience and Information Assurance Programme of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (2023/1515) [HR/VP, EEAS]	Council Decision	11.7 Support to Other International Organizations
June 2021	Regulation establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe (2021/947) Subsequent corresponding legal acts, guidelines or other documents of relevance: • July 2021: Commission Delegated Regulation supplementing Regulation 2021/947 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe (2021/1530) • n.d.: Multi-Annual Indicative Programme. Thematic Programme On Peace, Stability And Conflict Prevention 2021 - 2027 [DG INTPA]	Regulation	11.6 Development Cooperation and Cyber Capacity-Building
April 2021	Regulation establishing the European Defence Fund (2021/697) Previous legislation: Regulation establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry (2018/1092)	Regulation	11.4 Cyber Defence
May 2019	Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2019/797)	Council Decision	11.3 Sanctions Regime

	Subsequent corresponding legal acts, guidelines or other documents of relevance: • May 2024: Council Decision (CFSP) 2024/1391 • May 2023: Council Decision (CFSP) 2023/964 • May 2022: Council Decision (CFSP) 2022/754 • May 2021: Council Decision (CFSP) 2021/796 • November 2020: Council Decision (CFSP) 2020/1748 • October 2020: Council Decision (CFSP) 2020/1537 • July 2020: Council Decision (CFSP) 2020/1127 • May 2020: Council Decision (CFSP) 2020/651 [HR/VP, EEAS]		
May 2019	Council Regulation concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2019/796) Subsequent corresponding legal acts, guidelines or other documents of relevance: • November 2020: Council Implementing Regulation (EU) 2020/1744 • October 2020: Council Implementing Regulation (EU) 2020/1536 • July 2020: Council Implementing Regulation (EU) 2020/1125	Council Regulation	11.3 Sanctions Regime
November 2018	EU Cyber Defence Policy Framework (14413/18) Previous framework: • November 2014: EU Cyber Defence Policy Framework (15585/14)	Other	11.4 Cyber Defence
June 2018	Council conclusions on EU External Cyber Capacity Building Guidelines (10496/18)	Council Conclusions	11.6 Development Cooperation and Cyber Capacity-Building
June 2018	Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (JOIN(2018) 16 final)	Joint Communication	11.5 Hybrid Threats and Campaigns
April 2018	Council conclusions on malicious cyber activities (7925/18)	Council Conclusions	11.2 Cyber Diplomacy
December 2017	Council Decision establishing permanent structured cooperation	Council Decision	11.4 Cyber Defence

	(PESCO) and determining the list of participating Member States (2017/2315) Subsequent corresponding legal acts, guidelines or other documents of relevance: • March 2018: Council Decision establishing the list of projects to be developed under PESCO (2018/340) • November 2019: Council Decision amending and updating Decision (CFSP) 2018/340 establishing the list of projects to be developed under PESCO (2019/1909) • November 2021: Council Decision amending and updating Decision (CFSP) 2018/340 establishing the list of projects to be developed under PESCO (2021/2008) [HR/VP, EEAS]		
June 2017	Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") (10474/17) Subsequent corresponding legal acts, guidelines or other documents of relevance: • October 2017: Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (13007/17) • June 2023: Revised Implementing Guidelines of the Cyber Diplomacy Toolbox (10289/23)	Council Conclusions	11.2 Cyber Diplomacy
April 2016	Joint Framework on countering hybrid threats (JOIN(2016) 18 final)	Joint Communication	11.5 Hybrid Threats and Campaigns
February 2015	Council Conclusions on Cyber Diplomacy (6122/15)	Council Conclusions	11.2 Cyber Diplomacy

Cybersecurity of EU Institutions, Bodies and Agencies

8

Month/ Year	Legal Act/Policy	Type	Section
January 2024	Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (2023/2841) Prior document providing a basis for CERT-EU: • December 2018: Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) (2018/C 12/01)	Regulation	12.1 Deep Dive
June 2023	Decision of the High Representative of the Union for Foreign Affairs and Security Policy on the security rules for the European External Action Service (2023/C 263/04)	Decision	12.2 Rules for Particular EUIBAs
January 2017	Commission Decision on the security of communication and information systems in the European Commission (2017/46) Subsequent corresponding legal acts, guidelines or other documents of relevance: • April 2018: Commission Decision laying down implementing rules for Article 6 of Decision 2017/46 on the security of communication and information systems in the European Commission (2018/559) • December 2017: Commission Decision laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Commission Decision 2017/ 46 on the security of communications and information systems in the Commission (C(2017) 8841) [not publicly available] Previous legislation [not in force anymore]: • August 2006: Commission Decision concerning the security of information systems used by the European Commission (C(2006) 3602)	Decision	12.2 Rules for Particular EUIBAs
March 2015	Commission Decision on Security in the Commission (2015/443)	Decision	12.2 Rules for Particular EUIBAs

Policy Area 1: Overarching Policies

General

— Council Conclusions on the Future of Cybersecurity: Implement and Protect Together

In May 2024, the Council adopted ﷺ Council Conclusions on the Future of Cybersecurity: Implement and Protect Together. In its conclusions, the Council sets out by noting the "key role and shared responsibility of Member States, and the EU to set and implement a clear and agile regulatory and policy framework laying down our collective ability to protect, detect, deter and defend against, cyberattacks and recover from them" (p. 5). The conclusions are centered around four elements and highlight the following exemplary issues:

Table 2: Overview of Provisions Contained in Council Conclusions on the Future of Cybersecurity

Elements	Exemplary Provisions

Focus Areas for Policy-Making	• Council notes that "increasing the cyber resilience of entities and the cybersecurity of products with digital elements should be a continued focus for policy makers, including steps such as vulnerability management, supply chain security, the development of the necessary skills throughout the workforce and increased international dialogues on standards and cooperation" (p. 6)
	• Council acknowledges "significant human, financial and operational resources required from society, businesses and governments for their implementation" (p. 6)
	• Council calls
	  • on Commission, ENISA, European Cybersecurity Competence Centre (ECCC), CERT-EU, European Cybercrime Centre (EC3), NIS Cooperation Group, CSIRTs Network, European Cyber Crises Liaison Organisation Network (EU-CyCLONe), national CSIRTs, competent authorities and National Coordination Centres (NCCs) "to support all stakeholders with [...] implementation" (p. 6)
	  • "for actions facilitating and supporting compliance and reducing administrative burden, especially for micro, small and medium enterprises" (p. 6)
	  • on Commission
	  • to "swiftly move forward with the adoption of delegated and implementing acts, especially those that are mandatory for

	the implementation of the NIS2 Directive and the Cyber Resilience Act" (p. 7) • to "develop a clear overview of the relevant horizontal and sectoral legislative frameworks and their interplay" (p. 7) • "for the further development of the Cybersecurity Skills Academy and implementation of its actions to strengthen the EU cybersecurity workforce" (p. 9) • "for international cooperation in particular on the potential for mutual recognition of skills frameworks" (p. 9) • on "Commission, the ECCC and relevant national authorities to stimulate and support use by, in particular, European businesses, research institutions and academia of EU cyber security funding" (p. 9) • on "Commission, the High Representative and ENISA, together with NIS Cooperation Group, within their respective mandates, to swiftly develop a coherent and comprehensive approach across sectors to risk assessment and scenario building, based on a common methodology" (p. 12) • on "NIS Cooperation Group to continue working on the [information and communications technology] ICT Supply Chain toolbox" (p. 12) • Council invites "Commission to prepare, with the support of ENISA and other relevant EU entities, a mapping of relevant reporting obligations set out in the respective EU legislative acts [...] to identify opportunities to reduce the administrative burden" (p. 7) • Council urges Commision to "ensure a coherent approach in future initiatives, which should strengthen or complement existing structures, avoiding unnecessary complexity and duplication", further stressing the need for "thorough impact assessments for all new legislative initiatives" (p. 7) • Council "expresses concern on the slow and challenging development of the European cybersecurity certification schemes, and calls for the smooth adoption of high quality schemes" (p. 8) • Council supports "active promotion" of Active Cyber Protection (ACP) and Coordinated Vulnerability Disclosure (CVD) (p. 10) Council "encourages the timely development of European cybersecurity certification schemes [...] for the certification of the European Digital Identity Wallets" (p. 11)
Strengthening the Institutional Framework	• Council "invites Member States driven cooperation networks such as the NIS Cooperation Group, and, supported by ENISA, the CSIRTs Network and EU-CyCLONe to establish a multi-annual strategic perspective" (p. 13) • Council calls • on Commission and HR/VP "to develop across policy domains a clear overview of the roles and responsibilities of all relevant EU entities, stakeholders and networks, both civilian and military, active in the cybersecurity domain, including in their interaction" (p. 13) • on Commission "to take duly into account the development of ENISA's role reviewing the Cybersecurity Act" (p. 14) • on ENISA "to establish clear priorities, including focusing on supporting the Member States through existing structures" (p. 14) • on Commission and ECCC "to gain financial autonomy and finalise its institutional set up" (p. 15) • on Member States, Commission, HR/VP, ENISA, ECCC, CSIRTs Network and Europol "to thoroughly, openly and in a coordinated manner engage with all relevant private sector stakeholders to fortify cybersecurity measures, foster collaborative initiatives, and

	formulate robust strategies to mitigate the risks posed by cyber threats" (p. 15) • on Member States and Commission "to increase voluntary information sharing in view of a common situational awareness" (p. 16) • on Commission and relevant EUIBAs to make best use of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) (p. 16) • on Commission "to swiftly evaluate the current cybersecurity Blueprint and, on this basis, propose a revised Cybersecurity Blueprint" (p. 18) • Council encourages CERT-EU "to develop its role further" pursuant to Regulation 2023/2841 (p. 14)
Internal/ External Nexus for Cybersecurity Policy	• Council "invites the Member States and relevant EU entities to engage with countries and actors outside of the Union in order to increase international cooperation against cybercrime" (p. 19) • Council "stresses the need to create awareness on the importance of secure connectivity and trusted suppliers in third countries, including by offering technical assistance and by sustaining investment in secure and trusted connectivity, which incentivises increased alignment with the EU Toolbox on 5G cybersecurity" (p. 20)
Cybersecurity Dimension of Emerging and Disruptive Technologies	• Council "stresses the attention needed from an EU cybersecurity policy perspective to the challenges and opportunities presented by emerging and disruptive technologies that are critical to our future development such as AI, quantum and 6G technology" (p. 22) • Council "invites Member States, the Commission, ENISA and the NIS Cooperation Group to consider concrete non-legislative risk-based initiatives such as roadmaps and action plans to further guide EU action in this area, incentivising innovation and addressing risks efficiently by leveraging a broad range of existing tools and mechanisms" (p. 22) • Council "underlines the need to promote a consistent, coherent and transparent policy approach to free and open-source software" (p. 23)

The Council concludes by calling for a review of the EU's Cybersecurity Strategy, particularly inviting both the Commission and the HR/VP "to assess the results and gaps of the current Strategy and its impact, and to present on this basis a revised strategy without undue delay" (p. 24).

— EU Cybersecurity Strategy for the Digital Decade

In December 2020, the Commission and the HR/VP shared the ﬀ EU Cybersecurity Strategy for the Digital Decade with the Council and the European Parliament. The document builds on previous EU cybersecurity strategies from 2017[26] and 2013. The Strategy sets out to "ensure a global and open Internet with

26 In relation to the 2017 EU Cybersecurity Strategy, the Council adopted Conclusions on the Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" in November 2017.

strong guardrails to address the risks to the security and fundamental rights and freedoms of people in Europe" (p. 5), paired with the ambition to "supporting this strategy through an unprecedented level of investment in the EU's digital transition over the next seven years" (p. 5f.). Specifically, it lays out the following areas of EU action, priorities, and measures:

Table 3: Overview of Measures Outlined in the EU Cybersecurity Strategy for the Digital Decade

Area of EU action	Priorities	Measures
"Thinking Global, Acting European"		

1: Resilience, technological sovereignty and leadership	Resilient infrastructure and critical services	• Commission will propose/already proposed
		  • revision of NIS Directive (p. 5) [see Chapter 6.1]
		  • "review of the legislation on the resilience of critical infrastructure" (p. 6) [see Chapter 8.1]
		  • "rules for cybersecurity in cross-border electricity flows" (p. 6)
		  • measures for "strengthen[ed] digital operational resilience" of the financial sector (p. 6) [see Chapter 7.1]
		• "Commission will continue to proceed with a deepening of the Galileo cybersecurity strategy for the next generation of Global Navigation Satellite System services" (p. 6)

	Building a European Cyber Shield	• Commission proposes the establishment of "a network of Security Operations Centres across the EU", to be backed up by "over EUR 300 million to support public-private and cross-border cooperation in creating national and sectoral networks" (also encouraging co-investment by Member States) (p. 7)
	An ultra-secure communication infrastructure	• Further efforts to develop and deploy a "secure quantum communication infrastructure (QCI) for Europe" (p. 7) • "Explor[ation of] the possible deployment of a multi-orbital secure connectivity system" by the Commission (p. 8)
	Securing the next generation of broadband mobile networks	• Commission encourages the implementation of key measures of the 5G Toolbox by Member States (p. 8) [see Chapter 6.2] • Vis-à-vis non-EU countries, the Commission, European External Action Service (EEAS) and its delegations "stand ready" to provide them with information the EU's 5G approach (p. 9)
	An Internet of secure things	• "Consider[ation … of] new horizontal rules to

		improve the cybersecurity of all connected products and associated services placed on the Internal Market" by the Commission (p. 9)
	Greater global Internet security	Commission seeks to • "develop a contingency plan [...] for dealing with extreme scenarios affecting the integrity and availability of the global [Domain Name System] DNS root system" (p. 10) • "encourage relevant stakeholders including EU companies, Internet Service Providers and browser vendors to adopt a DNS resolution diversification strategy" (p. 10) • "contribute to secure Internet connectivity by supporting the development of a public European DNS resolver service" (the DNS4EU initiative) (p. 10) • "accelerate the uptake of key internet standards including IPv664 and well-established internet security standards and good practices for DNS, routing, and email security" (p. 11) • "consider the need for a mechanism for more systematic monitoring and gathering of aggregated data on Internet traffic and for advising on potential disruptions" (p. 11)

	A reinforced presence on the technology supply chain	• "Investment in cybersecurity (notably through the Digital Europe Programme, Horizon Europe and recovery facility) to reach up to €4.5 billion in public and private investments over 2021-2027" through the ECCC and network of NCCs (p. 12) [see Chapter 10.2]
		• Commission intends to
		  • "support [...] the development of a dedicated cybersecurity Masters programme" (p. 12)
		  • "contribute to a common European Cybersecurity Research and Innovation Roadmap beyond 2020" (p. 12)

	A cyber-skilled EU workforce	• Reference to the "revised Digital Education Action Plan[, which] will raise cybersecurity awareness among individuals, especially children and young people, and organisations, especially SMEs" (p. 12) • "Develop[ment of] awareness tools and guidance to increase the resilience of EU businesses against cyber-enabled intellectual property theft" by "the Commission [...] together with the EU Intellectual Property Office at Europol, ENISA, Member States and the private sector" (p. 12)

2: Building operational capacity to prevent, deter and respond	A Joint Cyber Unit (JCU)	• Objectives of JCU [see Chapter 5.2]
		  • "ensure preparedness across cybersecurity communities"
		  • "provide continuous shared situational awareness"
		  • "reinforce coordinated response and recovery" (p. 14)

		• Proposition of four steps for the realization of the JCU 1. "mapping available capabilities at national and EU level" 2. "establishing a framework for structured cooperation and assistance" 3. "implementing the framework drawing on resources provided by participants so that the Joint Cyber Unit becomes operational" 4. "expand[ing] by strengthening coordinated response capacity with input from industry and partners" (p. 14) • Presentation of "the process, milestones and timeline for defining, preparing, deploying and expanding the Joint Cyber Unit" by the Commission by February 2021 (p. 15)
	Tackling cybercrime	• Development of an "action plan to improve digital capacity for law enforcement agencies" by the Commission (p. 15) • Reinforcement of Europol's "role as a centre of expertise to support national law enforcement authorities combatting cyber-enabled and cyber-dependent crime, contributing to the definition of common forensic standards" (p. 15) • Commission "to use all appropriate means, including infringement proceedings, to ensure" full transposition and implementation of the 2013 Directive on attacks against information systems by Member States (p. 15) [see Chapter 8.2]

	EU cyber diplomacy toolbox	• "Advance[ment] of strategic intelligence cooperation on cyber threats and activities" by way of setting up a Member States' EU cyber intelligence working group residing within INTCEN (to be encouraged and facilitated by the HR/VP) (p. 17)
		• Presentation of "a proposal for the EU to further define its cyber deterrence posture" by the "High Representative, with the involvement of the Commission" (p. 17)
		• Cyber Diplomacy Toolbox [see further Chapter 11.2]
		  • HR/VP to explore "additional measures under the cyber diplomacy toolbox, including the possibility for further options for restrictive measures as well as by exploring qualified majority voting (QMV) for listings under the horizontal sanctions regime against cyber-attacks" jointly with the Council and the Commission (p. 17)
		  • Proposition of revised Cyber Diplomacy Toolbox implementing guidelines by HR/VP (involving the Commission) (p. 17)
		  • "Further integrat[ion of] the cyber diplomacy toolbox in EU crisis mechanisms" and "reflect[ion] upon the interaction between the cyber diplomacy toolbox and the possible use of Article 42.7 TEU [the mutual

			defence clause] and Article 222 TFEU [the solidarity clause]" (p. 17) • "Further efforts to strengthen the cooperation with international partners, including NATO, to advance the shared understanding of the threat landscape, develop cooperation mechanisms and identify cooperative diplomatic responses" (p. 17)
	Boosting cyber defence capabilities		• Presentation of "a review of the Cyber Defence Policy Framework (CDPF)" (p. 18) [see further Chapter 11.4] • "Foster[ed] cooperation among Member States on cyber defence research, innovation and capability development, encouraging Member States to make use of the full potential of" the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) (p. 18) [see further Chapter 11.4] • "Development of an EU "Military Vision and Strategy on Cyberspace as a Domain of Operations" for [Common Security and Defence Policy] CSDP military missions and operations" (p. 19) [see further Chapter 11.4] • "Reinforce[ment of the] cybersecurity of critical space infrastructures under the Space Programme" (p. 19) [see further Chapter 10.3]
3: Advancing a global and open cyberspace	EU leadership on standards, norms and frameworks in cyberspace	Stepping up on international standardization	• Commitment to "step up its engagement in, and leadership on international standardisation processes, and enhance its representation in international and European standardisation bodies as well as other standard development organisations" (p. 20)
		Advance responsible state behaviour in cyberspace	• "Develop[ment of] an EU position on the application of international law in cyberspace" (p. 20) • Advancing the proposal for a Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA) within the United Nations (p. 20) • HR/VP to "strengthen and encourage the implementation of confidence-building measures between states" (p. 21) • "Sustained efforts to protect human rights defenders, civil society and academia working on issues such as cybersecurity" (p. 21)

		Budapest Convention on Cybercrime	• Continued support for non-EU countries intending to become a party to the Budapest Convention (p. 21) • Efforts to finalize the Budapest Convention's Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence (p. 21)
	Cooperation with partners and the multi-stakeholder community	• Reinforcement and expansion of EU cyber dialogues "with third countries to promote [the EU's] values and vision for cyberspace, sharing best practices, and seeking to cooperate more effectively" (p. 21) • Establishment of "structured exchanges with regional organisations" such as the African Union (AU), the ASEAN Regional Forum, the Organisation of American States (OAS), and the Organization for Security and Co-operation in Europe (OSCE) (p. 21 f.) • Formation of "an informal EU Cyber Diplomacy Network to promote the EU vision of cyberspace, exchange information and regularly coordinate on developments in cyberspace" (p. 22) • "Advance[ment of] EU-NATO cooperation, notably on cyber defence interoperability requirements" (p. 22) • "Reinforce[ment of] regular and structured exchanges with stakeholders, including the private sector, academia and civil society" by the Commission and the HR/VP (p. 22)	
	Strengthening global capacities to increase global resilience	• Development of an "EU External Cyber Capacity Building Agenda" (p. 22) • Establishment of an "EU Cyber Capacity Building Board" (p. 22) • Continued focus of EU cyber capacity-building (CCB) "on the Western Balkans and in the EU's neighbourhood, as well as on partner countries experiencing a rapid digital development" (p. 23)	
Cybersecurity in the EU Institutions, Bodies and Agencies			

• Commission will propose
  • a Regulation on Information Security in the EU institutions bodies and agencies;
  • a Regulation on Common Cybersecurity Rules for EU institutions, bodies and agencies [see further Chapter 12.1];
  • and a new legal base for CERT-EU to reinforce its mandate and funding (p. 24 f.)
• Development of a "Cyber Awareness Programme [...] for all EU institutions, bodies and agencies to raise staff's awareness, cyber hygiene and support a common cyber security culture" (p. 24)			

The first report on the implementation of the 2020 EU Cybersecurity Strategy was

published in June 2021.

The Council reacted to the Strategy by adopting ﷺ Conclusions on the EU's Cybersecurity Strategy for the Digital Decade three months later. The Conclusions welcome the Cybersecurity Strategy and, inter alia, stress "the need to raise more awareness on cyber issues at the political and strategic decision-making levels by providing decision-makers with relevant knowledge and information" (p. 6) and reflect on the strategy's components. Looking ahead, the Council "encourages the Commission and the High Representative for Foreign Affairs and Security Policy to establish a detailed implementation plan setting the priorities and the schedule of planned actions" (p. 17). The Council itself commits to "monitor[ing] the progress in the implementation of these Conclusions by means of an Action Plan which will be regularly reviewed and updated by the Council in close cooperation with the European Commission and the High Representative" (p. 17).[27]

— Security Union Strategy

The EU's ﷺ Security Union Strategy "focuses on building capabilities and capacities to secure a future-proof security environment" (p. 2) for the period 2020-2025. It was published in July 2020. In relation to cybersecurity, the strategy begins by noting that "the ever-increasing ways in which digital technologies benefit our lives ha[ve] also made the cybersecurity of technologies an issue of strategic importance" (p. 3). Specifically, in the context of the strategy's chapter on a "rapidly changing European security threat landscape" (p. 2-5), it mentions "a wave of cybercrime", "continued cyber-enabled theft of intellectual property" and "cyber theft of trade secrets" (all p. 3) as cybersecurity-related threats. The Strategy further stresses the need for "economic operators [..to] take greater responsibility for the cybersecurity of products and services they place on the market" and for "individuals [...] to have at least a basic understanding of cybersecurity to be able to protect themselves" (both p. 5). Of cybersecurity relevance are the following strategic priorities and corresponding actions of the strategy:

Table 4: Exemplary Actions Within EU Security Union Strategy

Strategic Priority	Sub-Priority	Exemplary Actions
"A future-proof security	Critical infrastructure protection	• Inclusion of cyber-related "robust critical infrastructure protection and resilience measures" within the legislative framework (Directive 2016/1148

27 To the best of the author's knowledge, both the implementation and action plan are not publicly accessible.

environment"	and resilience	and Directive 2008/114) to account for "increased interconnectedness and interdependency", e.g., through a revision of the NIS Directive (p. 6) • Sector-specific initiatives "on the digital operational resilience for financial sectors" & "stronger resilience of critical energy infrastructure against [...] cyber [...] threats" (p. 7)
	Cybersecurity	• Exploration of "new and enhanced forms of cooperation between intelligence services, EU INTCEN, and other organisations involved in security" (p. 8) • Development of a "culture of cybersecurity by design" as a long-term need, e.g., through the EU cybersecurity certification framework (p. 8) • "Set[ting] out a clear process, milestones and timeline" for the proposed Joint Cyber Unit by the Commission (p. 9) [see further Chapter 5.2] • "Creat[ion of] mandatory and high common standards for the secure exchange of information and the security of digital infrastructures and systems across all EU institutions, bodies and agencies" (p. 9) [see further Chapter 12.1]
"Tackling evolving threats"	Cybercrime	• Full implementation of Directive 2013/40 [see further Chapter 8.2] • Elevation of the "fight against cybercrime [... to a] strategic communication priority across the EU" (p. 11) • Examination of the "feasibility of an EU cybercrime-related rapid alert system" by the Commission with the involvement of Europol and ENISA (p. 11)
"A strong European security ecosystem"	Cooperation and information exchange	• Reinforcement of "security partnerships between the EU and third countries [...] to increase cooperation to counter shared threats such as [...] cybercrime" (p. 23)
	Strengthening security research and innovation	• Support for "creat[ing] safer and more secure new technologies" (p. 24)
	Skills and awareness raising	• Enhancement of "human capacity for cybersecurity preparedness and response" (p. 25)

The Commission regularly publishes progress reports on the Security Union Strategy, as listed in the tabular overview contained in Chapter 4.

— Council Conclusions on Cybersecurity Capacity and Capabilities Building in the EU

In March 2019, the Council adopted ﷺ Conclusions on cybersecurity capacity

and capabilities building in the EU. Within the Conclusions, the Council, inter alia, stresses the following elements (p. 5-6):

Table 5: Overview of Council Conclusions on Cybersecurity Capacity and Capabilities Building in the EU

Vis-à-vis	Provisions

Member States	• Council invites Member States to
	  • "build on their national cybersecurity strategies and mainstream cybersecurity, taking into account sector-specific requirements"
	  • "perform continuous monitoring, evaluation/assessment of the impact of measures taken to strengthen cyber resilience and enhance cyber capabilities and capacities at national level"
	  • "mainstream cybersecurity and digital literacy in curricula at all levels of education"
	  • "carry out cybersecurity awareness and cyber hygiene initiatives for the public and end users, targeting public sector employees"
	  • "further develop the cybersecurity technical and operational capabilities of their CSIRTs in incident prevention, mitigation and incident response"
	  • "continue to help law enforcement authorities develop specific competences in coordination with the competent European authorities in order to effectively fight cybercrime at EU level"
	  • "increase investment in cyber capacity building"
	• Council encourages Member States to
	  • "conduct cybersecurity exercises at national level as well as to conduct and/or participate in cybersecurity exercises at EU level"

EUIBAs	• Council calls on the Commission and ENISA to
	  • "continue their support in developing the capacity and capability of the Network of CSIRTs by Member States to better cooperate, share information on incidents and respond effectively to large-scale cross-border incidents"
	  • "carry out cybersecurity awareness programmes and training targeting employees of the EU institutions, agencies and bodies"

Member States & EUIBAs	• Council calls on EU and Member States to
	  • "share information and best practices on a voluntary basis in order to contribute to the identification and tackling of the main cyber capacity building needs at national and EU level"
	  • "take cybersecurity into consideration in calls for ICT procurement, as appropriate"
	• Council invites EU and Member States to
	  • "support cybersecurity research and to promote cybersecurity as an issue in other fields of study"
	  • "develop cybersecurity research reflecting societal needs and integrating the research results into the market"

Incident and Crisis Response

— Joint Cyber Unit

In June 2021, the Commission issued a ﷺ Recommendation on building a Joint Cyber Unit (JCU), which "identif[ies] the actions necessary to coordinate EU efforts to prevent, detect, discourage, deter, mitigate and respond to large-scale cyber incidents and crises through a Joint Cyber Unit" (p. 7).

The Recommendation envisions the participation of the following actors in the JCU:

- the Commission, EEAS (including EU INTCEN), ENISA, Europol, CERT-EU, CSIRTs Network, EU-CyCLONe as *operational participants* and
- the Chairs of the NIS Cooperation Group and HWPCI, EDA and a "representative of the relevant PESCO projects" as *supporting participants* (p. 8).

The Recommendation assigns a particular role to ENISA within the JCU. The Commission advises to entrust ENISA with "ensur[ing] the coordination and support of Member States and relevant" EUIBAs, inter alia, by assuming the following tasks: "acting as secretariat, organising meetings and contributing to the implementation of actions both at Member State and EU level" (p. 9).

The realization of the JCU shall serve two objectives: (1) "ensur[ing] a coordinated EU response to and recovery from large-scale cyber incidents and crises", including the coordination of "mutual assistance mechanisms [...] subject to the request from one or more Member States" (p. 8) and (2) "shar[ing] best practices, harness[ing] continuous shared situational awareness, and ensur[ing] necessary preparedness" (p. 8) through a variety of measures, to be ensured/enabled by Member States and EUIBAs:

Table 6: Objectives and Measures of the Joint Cyber Unit

Objective	Measures
(1) "Coordinated response to and recovery from large-scale incidents and crises" (p. 8)	• "establishment, training, testing and coordinated deployment of EU Cybersecurity Rapid Reaction Teams" [The Recommendation defines Cybersecurity Rapid Reaction Teams as "a team composed of recognised cybersecurity experts, drawn notably from the CSIRTs of the Member States, with support from ENISA, CERT-EU and Europol, which is ready to remotely assist participants impacted by large-scale incidents and crises" (p. 7)] • "coordinated deployment of a virtual and physical platform, [...]

	which should serve as a supporting infrastructure for technical and operational cooperation between participants and to gather relevant staff and other resources from participants" • "creation and maintenance of an inventory of operational and technical capabilities available in the EU across cybersecurity communities in the Union that are ready to be deployed in the case of large-scale cybersecurity incidents or crises" • "reporting to the Commission and the High Representative on experience gained in cybersecurity operational cooperation activities within and across cybersecurity communities"
(2) Provision of "continuous shared situational awareness and preparedness against cyber-enabled crises across cybersecurity communities [1], as well as within those communities" (p. 8f.)	Supporting operations • "development of the Integrated EU Cybersecurity Situation report by gathering and analysing all relevant information and threat intelligence" [The Recommendation defines cybersecurity communities as "collaborative civilian, law enforcement, diplomacy and defence groups representing both Member States and relevant EU institutions, bodies and agencies which exchange information in pursuit of shared goals, interests and missions in relation to cybersecurity" (p. 7)] • "use of adequate and secure tools [...] for rapid information-sharing among participants and with other entities" • "exchange of information and expertise necessary to prepare the Union to manage cyber-enabled large-scale incidents and crises" • "adoption and testing of national Cybersecurity Incident and Crisis Response Plans" • "development, management and testing [...] of the EU Cybersecurity Incident and Crisis Response Plan" [The Recommendation defines the EU Cybersecurity Incident and Crisis Response Plan as "a compilation of roles, modalities and procedures leading to the completion of the EU Cybersecurity Crisis Response Framework described in point (1) of the Commission Recommendation of 13 September 2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises" (p. 7)] • "assistance of participants in concluding information-sharing agreements, as well as operational cooperation agreements with private sector entities" • "establishment of structured synergies with national, sectoral and cross-border monitoring and detection capabilities" • "assistance of participants in the management of large-scale incidents and crises [... inter alia through contributions] to shared situational awareness, supporting diplomatic action, political attribution as well as attribution in the context of criminal investigations, [...] aligning public communication and facilitating incident recovery" [1] Cybersecurity communities are defined as "collaborative civilian, law enforcement, diplomacy and defence groups representing both Member States and relevant EU institutions, bodies and agencies which exchange information in pursuit of shared goals, interests and missions in relation to cybersecurity" (p. 7)

The Recommendation concludes by specifying "milestones and [a] timeline" (p. 7) for the JCU's establishment (further specified in the Recommendation's annex, p. 11-15). Accordingly, it was envisioned that the JCU would have been fully operational by 30 June 2023.

Five months after the Commission published its Recommendation on the JCU, the Council adopted ✓✓ Conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises. In its Conclusions, the Council "acknowledges the Commission Recommendation on building a Joint Cyber Unit, as an initiative to be considered in further developing the EU cybersecurity crisis management framework" (p. 8). The Council emphasizes that "an incremental, transparent and inclusive process is essential for enhancing trust and, therefore, critical to the further development of an EU cybersecurity crisis management framework" (p. 8), while it concurrently underlines that "any possible participation in or contributions by Member States to a potential Joint Cyber Unit [would be] of a voluntary nature" (p. 8). Underpinning the Council's stance in this respect, EU Member States further highlighted "the need to consolidate, as a matter of priority, existing networks and interactions within each community, as well as to establish a thorough mapping of possible information sharing gaps and needs within and across cyber communities and also within and across European [IBAs], and subsequently agree on possible primary objectives and priorities of a potential [JCU]" (p. 10). Hence, with respect to the JCU, the Council "calls for further consideration on a legal basis for the potential Joint Cyber Unit throughout the entire process [... and] further reflection on individual elements of the Recommendation on the Joint Cyber Unit, including with regard to the idea of the EU Cybersecurity Rapid Reaction Teams, and to the EU Cybersecurity Incident and Crisis Response Plan" (p. 11). Looking ahead, the Council "calls upon the EU and its Member States to consider the potential of a Joint Cyber Unit initiative" (p. 11) and commits itself to "provid[ing] further guidance for complementing the EU cybersecurity crisis management framework" (p. 11).

— Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises

In June 2018, the Council adopted ✓✓ Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises. In it, the Council, inter alia, stresses the following elements:

Table 7: Overview of Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises

Objectives	Exemplary Provisions
Fostering the preparedness and crisis prevention	• Council "calls upon the Member States to ensure that their national crisis management mechanisms adequately address cybersecurity incidents and crises as well as use, and where necessary provide, appropriate procedures for cooperation at EU level at the technical,

(p. 4)	operational and political level"
Increasing the situational awareness (p. 4)	• Council "calls upon the EU and its Member States to cooperate and, based on national conclusions from Member States, contribute to EU situational awareness at all levels (technical, operational, political) both before and during large-scale cybersecurity incidents and crises through quick and effective sharing of situational information, where appropriate as well as with key strategic partners"

Ensuring the effective response (p. 5)	• Council calls upon Member States to
	  • "swiftly identify, develop and implement further means of operational cooperation, [...] in relation to early warnings, mutual assistance and principles and modalities for coordination when Member States respond to cross-border risks and incidents"
	  • "identify and put in place appropriate procedures and concrete measures for timely information sharing and situational awareness at operational level amongst competent authorities"

Streamlining the public communication (p. 5f.)	• Council "calls upon the EU institutions, agencies and bodies and Member States to ensure effective and, where necessary and possible, coordinated communication towards the public through existing mechanisms"
Building on the lessons learned and post incident analysis (p. 6)	• Council "calls upon the EU and its Members States, based on their national conclusions, to promote and share the analysis of operational and strategic aspects of lessons of large-scale cybersecurity incidents, crises, and exercises throughout the community of relevant actors involved"

Developing a European Cybersecurity Crisis Cooperation Framework (p. 6)	• Council calls upon the EU and Member States to
	  • "jointly work towards the development of European Cybersecurity Crisis Cooperation, putting in place the practical operationalisation and documentation of all the relevant actors, processes and procedures within the context of existing EU crises management mechanisms"
	  • "undertake necessary steps to remove obstacles and/or fill in gaps identified both in terms of information flows and in terms of interoperability of the existing procedures, processes and mechanisms where necessary"

— Commission Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises

In September 2017, the Commission issued a ⬚ Recommendation on coordinated response to large-scale cybersecurity incidents and crises. It recommends the establishment of "an EU Cybersecurity Crisis Response Framework" (p. 4) on the basis of a Blueprint included in the Recommendation's Annex. The Blueprint attached to the Recommendation "applies to cybersecurity incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU institutions with such a wide-ranging and significant impact of technical or political significance that they

require timely policy coordination and response at Union political level," also referred to as a "cybersecurity crisis" (p. 6). The response to cybersecurity crises at the EU level may involve existing crisis management procedures such as the Integrated Political Crisis Response (IPCR) arrangements[28], the ARGUS rapid alert system, and the EEAS Crisis Response Mechanism (the Blueprint further explains these instruments in p. 19-22). The processes and activities outlined in the Blueprint are based on the principles of proportionality, subsidiarity, complementarity, and confidentiality of information (p. 6f.). The Blueprint is subdivided on the basis of three "objectives of cooperation": "effective response," "shared situational awareness," and "public communication messages" (p. 7f.). For each of these objectives, the Blueprint lists measures to be taken at three different levels, namely the technical, operational, and the "strategic/political level."[29]

Each level shall undertake the following activities:

- Technical level: "incident handling during a cybersecurity crisis" and "monitoring and surveillance of incident including continuous analysis of threats and risk" (p. 8);
- Operational level: "preparing decision-making at the political level" and "coordinat[ing] the management of the cybersecurity crisis (as appropriate)" (p. 10);
- Strategic/political level: "strategic and political management of both cyber and non-cyber aspects of the crisis including measures under the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities" (p. 12).

For every level, the Blueprint suggests potential entities to be involved and lists activities to be undertaken under each of the three priority objectives. A few examples of such activities are listed below:

Table 8: Overview of Blueprint Measures

Objective	Level	Exemplary Measures
Shared situational awareness	1: Technical level (p. 9)	• Preparation of an EU Cybersecurity Technical Situation Report on incidents and threats by ENISA → Council, the Commission, the HRVP and the CSIRTs Network • Provision of forensic analysis and technical information by Europol/EC3 and CERT-EU → CSIRTs

28 Council Implementing Decision 2018/1993 notes in its recital that the IPCR has already been "used to exercise the Union response to major crises caused by cyber-attacks", among other threat scenarios (recital (12)).

29 As potential actors to be involved at the technical level, the Recommendation lists the designated competent authorities and single points of contact (SPOCs) pursuant to the NIS 2 Directive, national CSIRTs, ENISA, Europol/EC3, CERT-EU, the Commission, and the EEAS (e.g., via the SIAC) (p. 8f.). At the operational level, the Recommendation additionally mentions national cybersecurity agencies, sectoral authorities, and the Council as actors to be possibly involved in the response to large-scale cybersecurity incidents and crises (p. 10f.). At the highest level, the political/strategic level, the Recommendation alludes to the potential involvement of national "Ministers responsible for cybersecurity", the President of the European Council, the respective Council presidency, the Political and Security Committee (PSC), the Horizontal Working Party on Cyber Issues (HWPCI) and the HR/VP (p. 12).

		Network • Preparation of a EU Cybersecurity Incident Situation Report by the chair of the CSIRTs Network with the support of ENISA "in case of a major incident" → Presidency, the Commission, and the HR/VP

	2: Operational level (p. 11)	• Preparation of COREPER or PSC meetings "as appropriate" by HWPCI
		• In case of activation
		  • IPCR: for instance, preparation of an Integrated Situational Awareness and Analysis (ISAA) report "with contributions from ENISA, CSIRTs Network, Europol/EC3, EUMS INT, INTCEN and all other relevant actors"
		  • ARGUS: direct contribution by CERT-EU and EC3 to information exchange within the Commission
		  • EEAS Crisis Response Mechanism: reinforcement of "information collection and aggregat[ion of] all-source information and prepar[ation of] an analysis and assessment on the incident"

	3: Strategic/ political level (p. 12)	• "Identify[ing] the impacts of the disruptions caused by the crisis on the functioning of the Union"
Response	1: Technical level (p. 9f.)	• Exchange of "technical details and analysis on the incident" within CSIRTs Network → ENISA "not later than 24 hours from when the incident is detected" • Cooperation on "analy[zing] the available technical artefacts and other technical information related to the incident with a view of determining the cause and possible technical mitigation measures" among CSIRTs Network members • "Coordinat[ion of] technical response activities [by Member State CSIRTs] with the assistance of ENISA and the Commission"

	2: Operational level (p. 11)	"Upon request from the political level"
		• "Cross-border cooperation with single points of contact and national competent authorities (NIS Directive) to mitigate the consequences and effects"
		• "Cooperation and, if decided, coordination of technical capacities towards a joint or collaborative response in accordance with the CSIRTs Network [Standard Operating Procedures] SOPs"
		• In case of activation
		  • IPCR: "preparing decisions and coordinating under the IPCR arrangements"
		  • ARGUS: "decision-making within the ARGUS process"
		  • EEAS Crisis Response Mechanism: "support EEAS decision-making through the EEAS Crisis Response Mechanism including as regards contacts with third countries and international organisations as well as any measure aimed at

		protecting CSDP missions and operations and EU delegations"
	3: Strategic/ political level (p. 12)	• "Activat[ion of] additional crisis management mechanisms/instruments depending on the nature and impact of the incident" • "Tak[ing] measures within the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities"
Public communications	1: Technical level (p. 10)	• Development and dissemination of "technical advisories and vulnerability alerts" by national CSIRTs (coordination with the EEAS and the HRVP Spokesperson service "if the crisis entails an external or [CSDP] dimension") • "Facilitat[ion] the production and dissemination of common CSIRTs Network communications" by ENISA
	2: Operational level (p. 12)	• "Agree upon public messages regarding the incident" • Coordination of any public communication "with the EEAS and the HRVP Spokesperson service" in cases when "the crisis entails an external or [CSDP] dimension"
	3: Strategic/ political level (p. 12)	• "Decid[ing] upon a common communication strategy towards the public"

The Blueprint outlines further how these activities may specifically be integrated in the IPCR based on the IPCR's Standard Operating Procedures (see further pp. 13-17).

Digital Transformation

— Digital Decade Policy Programme 2030

The ⬚⬚ Digital Decade Policy Programme 2030 was established in 2022 to "creat[e] an environment favourable to innovation and investment by setting a clear direction for the digital transformation of the Union and for the delivery of digital targets[30] at Union level by 2030, on the basis of measurable indicators" (Art. 1(1), point (a)). As part of one of its eleven general objectives, the Programme includes cooperation by the European Parliament, the Commission, Council, and Member States on "improving resilience to cyberattacks, contributing to increasing

30 Article 4 of the Decision lists four digital targets, including, for instance, "the digitalisation of public services" through "100 % online accessible provision of key public services", among other indicators.

risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity" (Art. 3(1), point (k)), to be facilitated by multi-country projects. On an annual basis, the Commission shall draw up a "report on the state of the Digital Decade," to be shared with the Council and European Parliament (Art. 6).[31] Member States, on the other hand, shall share with the Commission "national digital decade strategic roadmaps" (by October 2023), which shall comprise, among other things, the "main planned, adopted and implemented policies, measures and actions that contribute to achieving the general objectives and the digital targets" (Art. 7).[32]

— Digital Europe Programme

�� Regulation 2021/694 introduces the Digital Europe Programme for the EU's budget period until 2027 in an effort to accelerate "the digital transformation of the European economy, industry and society" (Art. 3(1)). The Programme provides a planned funding of over €7.5 billion to support projects in five key areas, with over €1.6 billion allocated to cybersecurity. Funding in the area of cybersecurity shall:

- "support the building-up and procurement of advanced cybersecurity equipment, tools and data infrastructures" in cooperation with Member States;
- "support the building-up and best use of European knowledge, capacity and skills related to cybersecurity and the sharing and mainstreaming of best practices";
- "ensure a wide deployment of effective state-of-the-art cybersecurity solutions across the European economy" with a particular focus on "public authorities and SMEs";
- "reinforce capabilities within Member States and private sector" for compliance with the NIS Directive;
- "improve resilience against cyberattacks, contribute towards increasing risk-awareness and knowledge of cybersecurity processes, support public and private organisations in achieving basics levels of cybersecurity [...]";
- and "enhance cooperation between the civil and defence spheres with regard to dual-use projects, services, competences and applications in cybersecurity [...]" (Art. 6(1)).

The implementation of respective initiatives rests primarily with the ECCC and the Network of NCCs (Art. 6(2)). The Commission adopted the Digital Europe Cybersecurity Work Programme 2023-2024 to specify the cybersecurity-related initiatives under the Digital Europe Programme.[33] The following table provides a

31 In 2023, the Commission published its first Report on the Digital Decade.

32 A list of published national roadmaps can be found here. The Commission is tasked with supporting and advising Member States in drafting their national roadmaps.

33 This is the Commission's second Cybersecurity Work Programme that covers the period of 2023 to 2024. The first Work Programme covered the period of 2021 to 2022.

non-exhaustive overview of some of the deployment actions, objectives, and sought deliverables of the work programme:

Table 9: Overview of Objectives and Deliverables of the Digital Europe Cybersecurity Work Programme 2023-2024

Deployment Action	Objectives	Examples of Sought Deliverables
"Security Operation Centres" (pp. 14-27, Work Programme)	"support joint actions to create an advanced (state-of-the-art) threat detection and cyber early warning ecosystem"	The ECCC will work with Member States to • build and strengthen National Security Operation Centres (SOCs), connect them at the EU level via "cross-border SOC platforms," and • strengthen the "SOC ecosystem" by facilitating "a stronger collaboration between local SOCs, National SOCs and Cross-Border SOC platforms" [The Working Programme defines national SOCs as "public entities [which are] given the role at national level to act as clearinghouses for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting Cyber Threat Intelligence (CTI), reviews and analyses" (p. 15)]
"Support for the Implementation of the proposed Cyber Resilience Act" (pp. 29-33, Work Programme)	• "support European SMEs [...] to strengthen their cybersecurity capacities and to support the implementation" of the Cyber Resilience Act (CRA) • "support the implementation [...] through tools that support, and where possible automate, internal compliance procedures, including testing and specification drafting with focus towards European SMEs"	• Provision of "financial support for SMEs and other stakeholders for CRA compliance" • Establishment of an "openly available platform with CRA-related resources" by projects • Organization of "workshops, events, networking and exchange of experience of stakeholders" in "close coordination with the EU Cybersecurity Skills Academy" • Design and development of tools that "simplify and automate CRA compliance" and "CRA compliance documentation obligations"
"Cybersecurity Emergency Mechanism" (pp. 39-41, Work Programme)	"increase the level of protection and resilience to cyber threats, in particular for large industrial installations and infrastructures, by assisting Member States in their efforts to improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise"	• Provision of "preparedness support services" such as the development of "penetration testing scenarios," "threat assessment and risk assessment services" and "risk monitoring services" to entities in "sectors indicated as critical

		infrastructure sectors in NIS2" (including governmental entities, operators of essential services ...)
"Standardisation in the Area of Cybersecurity" (pp. 42-43, Work Programme)	"support further standardisation in the area of cybersecurity, notably in view of the implementation of the proposed" CRA	• Organization of "events, workshops, stakeholder consultations, and production of white papers" to foster the "development of harmonised standards and conformity" with the CRA • Provision of "support for participation of relevant European experts in European and international cybersecurity standardisation fora"
"Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies" (pp. 43-48, Work Programme)	• "capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislation on cybersecurity" • "supporting the implementation of the proposed [CRA] by market surveillance authorities/notifying authorities/national accreditation bodies"	• "Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole" • "Better compliance with NIS2 [...] and higher levels of situational awareness and crisis response in Member States" • "Support actions and cooperation for further advanced of cybersecurity certification" • Increase the capacities and capabilities of market surveillance authorities to ensure "effective supervision and enforcement of the CRA" • Increase the capacities and capabilities of notifying authorities and national accreditation bodies to ensure the effective "implementation of the CRA"
Other deployment actions include: deploying the Network of National Coordination Centres with Member States (1.9), the development and deployment of advanced key technologies (1.2), post quantum cryptography (1.4), and the coordination between the cybersecurity civilian and defence spheres (1.6).		

— 2030 Digital Compass: The European Way for the Digital Decade

In March 2021, the Commission published the ⬚ 2030 Digital Compass: the European way for the Digital Decade. The Digital Compass sets out a vision for 2030 based on four target areas, of which three particularly address cybersecurity-related objectives:

Table 10: Overview of Cybersecurity-Related Objectives of the 2030 Digital Compass

Target Area	Objective
A digitally skilled population and highly skilled digital professionals	• "Broad-based digital skills should also build a society which can [...] protect itself against cyberattacks [...]" (p. 4)
Secure and performant sustainable digital infrastructures	• "Achiev[ment of] gigabit connectivity by 2030 is key", for instance by roll-out of "Very High Capacity Networks including 5G being [...], based on swift and efficient allocation of spectrum and respect of the 5G cybersecurity toolbox" (p. 5)
Digitalisation of public services	• "Ensure that democratic life and public services online [...] benefit from a best–in-class digital environment providing for easy-to-use, efficient and personalised services and tools with high security and privacy standards" (p. 10)

Emerging Technologies

— Commission Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

In April 2024, the Commission published a ﷺ Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. The Recommendation, inter alia, advises Member States to "define a 'Post-Quantum Cryptography [PGC] Coordinated Implementation Roadmap' aimed at synchronising the efforts of Member States to design and implement national transition plans while ensuring cross-border interoperability" and "support the evaluation and selection of relevant Post-Quantum Cryptography EU algorithms [...] and further adoption of such algorithms as Union standards" (p. 4). As part of the suggested Roadmap, the Commission recommends that Member States set up a dedicated subgroup within the NIS Cooperation Group to draft such a roadmap. This subgroup shall discuss post-quantum cryptography with other stakeholders such as Europol or NATO, as part of its deliberations. After being set up, the PGC subgroup within the NIS Cooperation Group shall strive to adopt the Roadmap after two years to be "followed by the development and further adaptation of Post-Quantum Cryptography transition plans of individual Member States" (p. 5). In turn, the Commission foresees a monitoring and period assessment role for itself. On this basis, the Commission, among other activities, may "determine whether additional actions, including proposing binding acts of Union law, are required" (p.

5). The Recommendation shall be reviewed at the latest in April 2027.

Democratic Processes

— Commission Recommendation on Inclusive and Resilient Electoral Processes in the Union and Enhancing the European Nature and Efficient Conduct of the Elections to the European Parliament

In December 2023, the Commission adopted a ﷺ Recommendation on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament. With respect to cybersecurity, the Recommendation notes, for instance, that "in addition to the obligations under [the NIS 2 and CER Directives], where applicable, Member States should strive to ensure a similar level of resilience of entities operating election-related infrastructure, by performing and updating risk assessments, conducting tests, and enhancing support for and the resilience of entities that play a significant role in the conduct of elections" (recital (33)) and carry out "specific measures [...] to further enhance the cybersecurity of voter registration databases, e-voting systems and other information systems used to manage electoral operations" (recital (34). The Recommendation sets out 11 principles, of which two address cybersecurity specifically:

Table 11: Overview of Cybersecurity-Related Provisions Contained in Commission Recommendation 2023/2829

Principles	Specification
IV. Encouraging election integrity and fair campaigning	"Political parties and campaign organisations are encouraged to adopt campaign pledges and codes of conduct on election integrity and fair campaigning", which shall, inter alia, include "active steps to maintain good cyber hygiene, such as regular cybersecurity checks, in order to recognize, deter and prevent attacks" (p. 13 f.)

VII: Protecting election-related infrastructure and ensuring resilience against cyber and other hybrid threats	Member States should
	• "take measures ensuring preparedness for, responsiveness to and recovery from cybersecurity incidents related to elections, taking into account the requirements established by" the NIS 2 Directive, particularly by
	  • "ensur[ing] that technology used in elections is designed, developed and produced to ensure a high level of cybersecurity,"
	  • "ensur[ing] cooperation between public and private entities involved in the cybersecurity of elections,"
	  • and "increas[ing] awareness on cyber hygiene of political parties, candidates, election officials and other entities related to elections" (p. 15)

	• "carry out or update risk assessments regarding the resilience of election-related infrastructure and of entities operating it, and collect and aggregate data resulting from such risk assessments including any relevant tests of the cyber resilience of their electoral systems" and "share experiences in the framework of the European Cooperation Network on Elections, and where appropriate, in joint sessions with the NIS Cooperation Group" (p. 15) • "continue and deepen their cooperation and exchange of information and best practices in the European Cooperation Network on Elections and NIS Cooperation Group, including, when necessary, through joint meetings, and updates, as necessary, to the Compendium on Cyber Security of Election Technology" (p. 15)

— European Democracy Action Plan

In December 2020, the Commission put forward a ⬚ Communication on the European Democracy Action Plan. In its introduction, as part of a section on the "digital transformation of our democracies", the Action Plan notes, inter alia, that "digitalisation enabled new ways to finance political actors from uncontrolled sources [and] cyber-attacks can target critical electoral infrastructure" (p. 2). Against this backdrop, the Action Plan lays out the following cybersecurity-related provisions to meet its specified objectives:

Table 12: Overview of Cybersecurity-Related Provisions of the European Democracy Action Plan

Objective	Specific Objective	Action
Protecting election integrity and promoting democratic participation	Strengthened cooperation in the EU to ensure free and fair elections	• "Set[ting] up a new joint operational mechanism and other support measures, building on the work of the European Cooperation Network on Elections, to promote resilient electoral processes and take further practical measures to protect election infrastructure against threats, including against cyber-attacks" (p. 9) • Update of "compendium on cyber security of election technology" (p. 8) • Organization of "further practical exercises" (p. 8)
Strengthening media freedom and media pluralism	Safety of journalists	• Provision of "sustainable funding for projects with a focus on legal and practical assistance to journalists in the EU and elsewhere, including safety and cybersecurity training for journalists and diplomatic support" (p. 15)
Countering disinformation	Improving EU and Member State capacity to counter disinformation	• "Commission and the HR/VP will explore conceptual and legal aspects of devising appropriate instruments [for countering foreign interference and influence operations], seeking synergies with the" Cyber Diplomacy Toolbox (p. 22)

Policy Area 2: Internal Market

The Treaty of the EU provides for the establishment of an internal market (Art. 3(3) TEU), which "comprise[s] an area without internal frontiers in which the free movement of goods, persons, services and capital" (Art. 26(2) TFEU). The EU and Member States share competences on the internal market overall (Art. 4(2), point (a) TFEU), whereas the EU holds the exclusive competence for "the establishing of the competition rules necessary for the functioning of the internal market" (Art. 3(1), point (b) TFEU).

Deep Dives: NIS 2 Directive and Cybersecurity Act

— Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS 2)

⬢⬢ Directive on measures for a high common level of cybersecurity across the Union (2022/2555)
Link: data.europa.eu/eli/dir/2022/2555/oj
Entry into force: 16 January 2023 Deadline for national transposition: 17 October 2024, measures to apply from 18 October 2024
Previous legislation: Repeals Directive 2016/1148 (NIS 1) from 18 October 2024 onwards
Subsequent documents of relevance: • September 2023: Commission Guidelines on the application of Article 3(4) of Directive (EU) 2022/2555 (NIS 2 Directive) • September 2023: Commission Guidelines on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)
Objective (Art. 1): "achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market"
Subject matter (Art. 1): "This Directive lays down: • (a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs); • (b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive

(EU) 2022/2557; • (c) rules and obligations on cybersecurity information sharing; • (d) supervisory and enforcement obligations on Member States".
Actors established/regulated by NIS 2 Directive: • NIS Cooperation Group (Art. 14) [see further Chapter 13] • CSIRTs Network (Art. 15) [see further Chapter 13] • EU-CyCLONe (Art. 16) [see further Chapter 13]
Deep Dive Structure → Scope → Competent Authorities, Single Points of Contacts and CSIRTs → National Cybersecurity Strategy → Cyber Crisis Management → Vulnerability Disclosure → Cybersecurity Risk Management → Reporting → Information-Sharing → Union-Level Cooperation and State of the Union Report → Supervision and Enforcement → Implementing and Delegated Acts → Review

Scope

In its application, the NIS 2 Directive distinguishes between essential and important entities. Both types of entities can be public or private. In general, essential entities are subject to more extensive obligations and a higher extent of supervision than important entities.

As a general rule, public or private entities fall in the scope of the NIS 2 Directive when they qualify at least as a medium-sized enterprise,[34] "provide their services or carry out their activities within the Union," and its type is listed in the NIS 2's Annex I or II (see further Table 13). Irrespective of the size requirement, the Directive applies to entities on the basis of circumstantial factors. In accordance, an entity is within the NIS 2's scope if

- it "is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;"
- "disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;"
- "disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;"
- or "the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the

34 To qualify as a medium-sized enterprise, the entity must have more than 50 employees and an annual turnover exceeding 10 million euros (Commission Recommendation concerning the definition of micro, small and medium-sized enterprises, Recommendation 2003/361).

Member State" (Art. 2(2)).

Moreover, it applies to entities when "services are provided by" "providers of public electronic communications networks or of publicly available electronic communications services," "trust service providers" and "top-level domain name registries and domain name system service providers" (Art. 2(2), point (a)) as well as "entities providing domain name registration services" (Art. 2(4)). All entities designated as critical entities under the CER Directive are also within the scope of NIS 2 (Art. 2(3)).

An entity is deemed essential when it fulfills any of the following criteria:

- it qualifies at least a medium-sized enterprise and additionally qualifies as an entity of the type outlined in Annex I (Art. 3(1), point (a));
- it is a "qualified trust service provider[...,] top-level domain name registr[y ... or] DNS service provider[...] (Art. 3(1), point (b));
- it is a "provider[...] of public electronic communications networks or of publicly available electronic communications services" (Art. 3(1), point (c));
- it is a "public administration entity [...] of central government as defined by a Member State in accordance with national law"[1];
- or it is an entity that is designated as a 'critical entity' under the CER Directive.

[1] The NIS 2 Directive excludes "public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences" (Art. 2(7)) from its scope of application. It is at a Member State's discretion to exclude specific entities when they operate in these areas or provide services to the previously enumerated excluded public administration entities from complying with particular obligations (see further Art. 2(8)).

EU Member States may choose to classify previously designated "operators of essential services" in the framework of the NIS 1 Directive as essential entities (Art. 3(1), point (g)). Member States may also designate essential entities based on the circumstantial factors listed above (Art. 3(1), point (e)).

Any other entities of a type listed in Annex I or II that do not qualify as essential under any of the points enumerated above are considered as important entities. In terms of jurisdiction, an essential or important entity falls under the jurisdiction of the particular Member State in which it is established (Art. 26).[35]

35 Exceptions to this general rule are (i) "providers of public electronic communications networks or providers of publicly available electronic communications services" for whom the location of the provision of their services is decisive, (ii) "DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as

The following table provides an overview of the (sub)sectors listed in Annex I and II and gives examples of types of entities[36], subsumed under the respective sectors:

Table 13: Sectors in the Scope of the NIS 2 Directive

"Sectors of high criticality" (Annex I)	

Energy	• Electricity
	  • for example, "distribution system operators"
	• District heating and cooling
	  • "operators of district heating or district cooling"
	• Oil
	  • for example, "operators of oil transmission pipelines"
	• Gas
	  • for example, "LNG system operators"
	• Hydrogen
	  • "operators of hydrogen production, storage and transmission"

Transport	• Air
	  • for example, "air carriers"
	• Rail
	  • for example, "railway undertakings"
	• Water
	  • for example, "operators of vessel traffic services"
	• Road
	  • for example, "road authorities"

Banking	• "credit institutions
Financial market infrastructures	• for example, "operators of trading venues"
Health	• for example, "healthcare providers"
Drinking water	• for example, "suppliers and distributors of water intended for human consumption"
Waste water	• "undertakings collecting, disposing of or treating urban waste

well as providers of online marketplaces, of online search engines or of social networking services platforms" where jurisdiction depends on "where the decisions related to the cybersecurity risk-management measures are predominantly taken" and (iii) public administration entities for which their establishing Member State determines jurisdiction (see further Art. 26(1) and (2)

36 For a definition of these and further types, see Annex I and II of the NIS 2 Directive.

	water, domestic waste water or industrial waste water"
Digital infrastructure	• for example, Internet Exchange Point (IEP) or domain name system (DNS) service providers
ICT service management (business-to-business)	• for example, managed service providers (MSPs)
Public administration	• for example, "public administration entities at regional level as defined by a Member State in accordance with national law"
Space	• "operators of ground-based infrastructure [...] that support the provision of space-based services"

"Critical sectors" (Annex II)	
Postal and courier services	• "postal service providers"
Waste management	• "undertakings carrying out waste management"
Manufacture, production and distribution of chemicals	• "undertakings carrying out the manufacture of substances and the distribution of substances or mixtures"
Production, processing and distribution of food	• "food businesses"
Manufacturing	• for example, manufacture of medical devices and in vitro diagnostic medical devices and manufacture of computer, electronic and optical products
Digital providers	• for example, "providers of online search engines"
Research	• "research organisations"

In the context of their national transposition of the NIS 2 Directive, EU Member States may choose to include "public administration entities at local level" and "education institutions" in their scope of application (Art. 2(5)).

EU Member States have until 17 April 2025 to draw up a list of entities that fall within the scope of NIS 2, which they must subsequently update at least every two years. Until the same date, EU Member States must, via their competent authorities, share "the number of essential and important entities listed [...] for each sector and subsector" with the Commission and the NIS Cooperation Group (Art. 3 (5)).

As a horizontal framework, the NIS 2 Directive also foresees the possibility of sector-specific Union legal acts to act as *lex specialis* (Art. 4).[37] In cases where "sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities" (Art. 4(1)). When a sector-specific EU legal act "do[es] not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts" (Art. 4(1)). As instrumental in the determination of whether another legal act meets the equivalence requirement, the NIS 2 Directive lists that any such act shall ensure that the

- "cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2)";
- the respective provisions "provide[...] for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive;"
- and "requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of this Directive" (Art. 4(2)).

In September 2023, the Commission published "guidelines clarifying the application of paragraphs 1 and 2," complying with Art. 4(3)).[38]

Who	What	When	Post-Deadline	Legal Basis
Member States	Development of a list of essential and important entities as well as entities providing domain name registration services	17 April 2025	Update at least every two years thereafter	Art. 3(3)
Member States	Notification of the number of essential and important entities listed for each sector and subsector → Commission and NIS Cooperation Group	17 April 2025	Every two years thereafter	Art. 3(5)
Member States	Notification of specified relevant information in relation to essential and important entities → Commission	17 April 2025	Every two years thereafter	Art. 3(5)

37 For instance, DORA represents such a sector-specific legal act for financial entities (see further European Commission: Commission Guidelines on the application of Article 4(1) and (2) of Directive 2022/2555). In this regard, the NIS 2 Directive stipulates that it "does not apply to entities which Member States have exempted from the scope of Regulation (EU) 2022/2554 in accordance with Article 2(4) of that Regulation" (Art. 2(10)).

38 The guidelines can be accessed here.

Competent Authorities, Single Points of Contacts and CSIRTs

From an institutional perspective, EU Member States must designate (a) competent national authority/ies, that is/are in charge of cybersecurity and the directive's supervision and enforcement, as well as a single point of contact (SPOC) (Art. 9). Each EU Member State SPOC is tasked to exercise a "liaison function" to ensure cooperation within its national jurisdiction and with other EU Member States, the Commission, or ENISA. The Commission is tasked with publishing a list of all national SPOCs.

Additionally, EU Member States must ensure that they have a computer security incident response team (CSIRT) (Art. 10), inter alia, tasked with

- "monitoring and analyzing cyber threats, vulnerabilities and incidents at national level;"
- "providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned;"
- and "responding to incidents and providing assistance to the essential and important entities concerned" (Art. 11(3)).

EU Member States can request ENISA's assistance in setting up their CSIRTs and must ensure their national CSIRTs' active involvement in the CSIRTs Network (Art. 10(6) and (10). National CSIRTs shall engage with "relevant stakeholders in the private sector" (Art. 11(4). In the context of enforcing such cooperative relationships, they shall also undertake efforts to "promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to:

- incident-handling procedures;
- crisis management;
- and coordinated vulnerability disclosure" (Art. 11(5)).

EU Member States shall, in particular, ensure inter-agency cooperation and information-sharing between their competent authorities and CSIRTs under the NIS 2 Directive and their national competent authorities designated pursuant to other EU legal acts, inter alia, in the context of the DORA Regulation and the CER Directive (Art. 13).

National Cybersecurity Strategy

In implementing the NIS 2 Directive, EU Member States are required to "adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve these objectives, and appropriate policy and

regulatory measures" (Art. 7(1)). EU Member States shall include, inter alia, specific policies on the following:

- "addressing cybersecurity in the supply chain for ICT products and services;"
- the "inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement;"
- and vulnerability management, "encompassing the promotion and facilitation of coordinated vulnerability disclosure" (Art. 7(2)).

The strategy should also

- specify governance arrangements at the national level, for instance, between competent authorities and single points of contact;
- include "a mechanism to identify relevant assets and an assessment of the risks in that Member State;"
- and identify "measures ensuring the preparedness for, responsiveness to and recovery from incidents" (Art. 7(1)).

The strategy should also include "a policy framework for enhanced coordination" (Art. 7(1), point (g)) among EU Member States' competent authorities under the NIS 2 and the CER Directive.

For a complete list of elements to be included in the national cybersecurity strategy, see further Art. 7. Member States must share their strategies with the Commission at the latest three months after their approval (Art. 7(3)). If necessary, Member States can ask ENISA to provide support "in the development or the update of a national cybersecurity strategy" as well as the identification of "key performance indicators for the assessment of that strategy" (Art. 7(4)).

Who	What	When	Post-Deadline	Legal Basis
Member States	Adoption of a national cybersecurity strategy	Regular assessment	Assessment at least every five years based on KPIs, update where necessary	Art. 7(4)

Cyber Crisis Management

To ensure effective cyber crisis management, EU Member States must additionally have a national competent authority "responsible for the management of large-scale cybersecurity incidents and crises" (Art. 9(1)). Building upon the definition of an incident as "an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems" (Art. 6, point (6)), the NIS 2

Directive defines a large-scale cybersecurity incident as "an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States" (Art. 6, point (7)). To comply with the Directive's provisions in the area of cyber crisis management, EU Member States must put in place a "national large-scale cybersecurity incident and crisis response plan" and "identify capabilities, assets and procedures that can be deployed in the case of a crisis" (Art. 9(3) and (4)).

NIS 2 requires the national plan to stipulate, in particular:

- "the **objectives** of national preparedness measures and activities;
- the **tasks and responsibilities** of the cyber crisis management authorities;
- the cyber crisis management **procedures** [...];
- national **preparedness measures**, including exercises and training activities;
- the relevant public and private **stakeholders and infrastructure involved**;
- [and] national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level" (Art. 9(4) points (a)-(f)).

Once adopted, EU Member States have three months to share their plans with both the Commission and EU-CyCLONe (Art. 9(5)).

Who	What	When	Post-Deadline	Legal Basis
Member States	Notification of cyber crisis management authority	At maximum three months after designation or establishment	At maximum three months after any subsequent changes to the crisis management authority's identity	Art. 9(5)
Member States	Submission of "relevant information relating to [...] their national large-scale cybersecurity incident and crisis response plans" → Commission and EU-CyCLONe	At maximum three months after adoption	-	Art. 9(5)

Vulnerability Disclosure

Member States shall designate national CSIRT as a national "coordinator for the purposes of coordinated vulnerability disclosure [CVD]" (Art. 12(1)). In implementing a national CVD policy, EU Member States must "ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability" to the entity assuming the functions of national CVD coordinator

(Art. 12(1)). If, upon reporting of a vulnerability, it is determined that it "could have a significant impact on entities in more than one Member State", national CVD coordinators shall interact with their counterparts in other EU Member States through the framework of the CSIRTs Network (Art. 12(1)).

At the European level, the NIS 2 Directive entrusts ENISA – upon consultation with the NIS Cooperation Group – with the development and maintenance of a "European vulnerability database" (Art. 12(2)). In terms of information provided, the European vulnerability database shall ensure that it includes

- a description of the vulnerability;
- "the affected ICT products or ICT services;"
- "the severity of the vulnerability in terms of circumstances under which it may be exploited;"
- and "the availability of patches" or relevant mitigatory guidance by national competent authorities or CSIRTs in their absence (Art. 12(2), points (a)-(c)).

Cybersecurity Risk Management

EU Member States must supervise and "ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use [...] and to prevent or minimise the impact of incidents" (Art. 21(1)). These measures shall be endorsed and overseen by an essential or important entities' management body, which may also be held liable in case of non-compliance (Art. 20(1)). In addition, the NIS 2 Directive stipulates that "Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training" (Art. 20(2)).

To comply with this provision, essential and important entities shall have in place at least the following measures/policies:

- "policies on **risk analysis** and **information system security**;
- **incident handling**;
- **business continuity**, such as backup management and disaster recovery, and crisis management;
- **supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- security in network and information systems **acquisition, development and maintenance**, including vulnerability handling and disclosure;
- policies and procedures to assess the **effectiveness of cybersecurity risk-management measures**;
- basic **cyber hygiene** practices and **cybersecurity training**;
- policies and procedures regarding the **use of cryptography** and, where appropriate, encryption;

- **human resources security**, access control policies and asset management;
- [and] the use of **multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate" (Art. 21(2)).

When EU Member States supervise the implementation of such measures by essential and important entities, they shall take into account "the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact" (Art. 21(1)) to ensure a proportionate application. Pursuant to the Cybersecurity Act (Regulation 2019/881), essential and important entities may be required to "demonstrate compliance" with this provision by exclusively "us[ing] particular ICT products, ICT services or ICT processes [...] that are certified under European cybersecurity certification schemes" (Art. 24(1)).

Reporting

The NIS 2 Directive puts in place reporting obligations for essential and important entities to report when they become subject to a "significant incident" (Art. 23). To determine an incident's significance, the directive lists two elements that can give rise to a significant incident:

- a) the incident "has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;" or
- b) the incident "has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage" (Art. 23(3)).

In reporting a significant incident to the national CSIRT or competent authority, the following specific timelines apply for essential and important entities:

Table 14: Reporting Deadlines and Actions Pursuant to the NIS 2 Directive

I. Action to be taken by essential or important entity			
(a) Without undue delay, >24 hours of "becoming aware" of a significant incident	(b) Without undue delay, > 72 hours of "becoming aware" of a significant incident	(c) Upon request by national CSIRT or competent authority	(d) <1 month after (b) has been submitted
Submission of an early warning. The warning shall "where applicable, [...]	Submission of an incident notification. Where applicable, the notification shall update the information provided in the warning of step	Submission of an intermediate report outlining "relevant	Submission of a final report. If the incident is still ongoing at the time, essential and important entities must submit a progress report instead. In the latter case, a

indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact." (Art. 23(4), point (a))	(a) and "indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise." (Art. 23(4), point (b))	status updates." (Art. 23(4), point (c))	final report must also be provided "within one month of their handling of the incident" (Art. 23(4), point (d) and (e)). [The final report is supposed to include (i) "a detailed description of the incident, including its severity and impact", (ii) "the type of threat or root cause that is likely to have triggered the incident", (iii) "applied and ongoing mitigation measures", and (iv) "where applicable, the cross-border impact of the incident" (Art. 23(4), point (d))]

II. Action to be taken by national CSIRT or competent authority	
(a) Without undue delay and, where possible, within 24 hours of receiving the early warning	(b) No specified timeline
Response to notifying entity that "includ[es] initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures." (Art. 23(5))	• Provision of "additional technical support," if requested by the entity (Art. 23(5)) • Provision of "guidance on reporting the significant incident to law enforcement authorities" when a criminal nature of the significant incident is assumed (Art. 23(5))

When essential or important entities report an incident, EU Member States shall guarantee that the information submitted allows "determin[ing] any cross-border impact of the incident" (Art. 23(1)).

Upon assessing an incident's significance, EU Member States – acting via their national CSIRT, competent authority, or SPOC – shall, "where appropriate," inform other EU Member States and ENISA of the incident, especially when the "significant incident concerns two or more Member States" (Art. 23(6)). In any case, national SPOCs must share a "summary report" with ENISA every three months (Art. 23(9)). This report shall include "anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified" (Art. 23(9)). In turn, ENISA is tasked with briefing the NIS Cooperation Group and the CSIRTs Network "about its findings on notifications" twice a year (Art. 23(9)). To increase the comparability of the national summary reports, ENISA "may adopt technical guidance on the parameters of the information to be included in the summary report" (Art. 23(9)). On a national level, either the CSIRT or competent authority

shall also ensure that "information about significant incidents, incidents, cyber threats and near misses notified [...] by entities [that the CER Directive] identified as critical entities" are shared with the national competent authorities designated under that Directive (Art. 23(10)).

The responsibility of essential and important entities to report incidents not only extends to the respective national authorities, but also to the "recipients of their services that are potentially affected by a significant cyber threat" (Art. 23 (2)). "Where applicable," essential and important entities shall provide them with "any measures or remedies [they] are able to take in response to that threat" (Art. 23(2)).

In addition to mandatory reporting obligations laid out in Article 23, Member States must ensure that entities can also voluntarily report relevant information in this respect. For essential and important entities, this relates to "incidents, cyber threats and near misses" (Art. 30). EU Member States shall also provide the basis for any other entity, specifically also those not "fall[ing] within the scope of this Directive" to be able to notify national CSIRTs or competent authorities of "significant incidents, cyber threats and near misses" (Art. 30(1), point (b)). The subsequent actions to be taken by national CSIRT or competent authority are the same as outlined in table 14 above. Yet, Member States can decide to take care of mandatory notifications received first.

Who	What	When	Legal Basis
Member State SPOC	Submission of summary report of notifications received in accordance with Art. 23 (1) and Art. 30 → ENISA	Every three months	Art. 23(9)
ENISA	Briefing about "findings on notification" → NIS Cooperation Group and CSIRTs Network	Every six months	Art. 23(9)

Information-Sharing

EU Member States shall encourage the voluntary exchange of information[39] among essential and important entities "through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared" (Art. 29(2)). The information-sharing is particularly envisioned for scenarios in which the information transmitted, for instance, helps to "prevent, detect, respond to or recover from incidents or to mitigate their impact" or

39 Information in this respect, for instance, relates to "information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks" (Art. 29(1)).

"limit[s...] or imped[es] the ability of [...] threats to spread" (Art. 29(1), point (b)). Essential and important entities shall inform their competent authorities of their participation in or withdrawal from such arrangements (Art. 29(4)). To promote the uptake of such arrangements, ENISA is tasked with assisting their formation through "exchanging best practices and providing guidance" (Art. 29(5)).

Union-Level Cooperation and State of the Union Report

NIS 2 also foresees the voluntary participation in **peer reviews** where representatives from at least two other EU Member States review, for instance, "the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in Articles 21 and 23," "the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities," or "the operational capabilities of the CSIRTs" of one EU Member State (Art. 19(1)). The Commission and ENISA are involved as observers in individual peer reviews (Art. 19(2)).[40] The NIS Cooperation Group is entrusted with developing a "methodology and [the] organisational aspects of peer reviews" together with the Commission, ENISA, and the CSIRTs Network where helpful (Art. 19(1)).

Every two years, ENISA shall draft a "**report on the state of cybersecurity in the Union**" for submission and presentation to the European Parliament (Art. 18). This report "shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union" and must provide assessments on the

- "Union-level cybersecurity risk;"
- the "development of cybersecurity capabilities in the public and private sectors;"
- the "general level of cybersecurity awareness and cyber hygiene among citizens and entities;"
- and a "summary of the findings [...] from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats" (Art. 18(1) points, (a)-(c) and Art. 18 (2)).

On an aggregated basis, the report shall also assess "the outcome of the peer reviews" as well as "the level of maturity of cybersecurity capabilities and resources across the Union [... and] the extent to which the Member States' national cybersecurity strategies are aligned" (Art. 18(1) points (d) and (e)).

Who	What	When	Legal Basis

40 In concrete terms, peer reviews can comprise "physical or virtual on-site visits and off-site exchanges of information" (Art. 19(6)).

NIS Cooperation Group	Development of a methodology for peer reviews	17 January 2025	Art. 19(1)
ENISA	Adoption of a biennial report on the state of cybersecurity in the Union → European Parliament	Every two years	Art. 18(1)

Supervision and Enforcement

To some extent, the supervisory and enforcement powers of EU Member States vary depending on whether an entity is designated as an essential or important entity. In principle, the pursuit of enforcement measures shall be based on "detailed reasoning" (Art. 32(8)). Before pursuing them, a competent authority shall share respective "preliminary findings" with the entity concerned and provide them with a window for submitting their view (the latter except for "duly substantiated cases [requiring] immediate action") (Art. 32(8)). Member States shall ensure that their supervisory and enforcement measures, as well as the imposition of administrative fines, are "effective, proportionate and dissuasive, taking into account the circumstances of each individual case" (Art. 32(1), Art. 33 (1) and Art. 34 (1)).

The NIS 2 Directive foresees at least the following supervisory and enforcement powers for national competent authorities:

Table 15: Supervision and Enforcement Powers

<table>
<tr><th colspan="2">Supervision</th></tr>
<tr><td colspan="2">Essential or important entity</td></tr>
<tr><td colspan="2">Art. 32(2) & Art. 33(2)
"on-site inspections"
"targeted security audits"
"security scans"
requests
"to access data, documents and information necessary to carry out their supervisory tasks"
"for evidence of implementation of cybersecurity policies"</td></tr>
<tr><td>Essential entity</td><td>Important entity</td></tr>
<tr><td>Art. 32(2)
"off-site supervision"
regular and ad hoc security audits
"requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned"</td><td>Art. 33(2)
"off-site ex post supervision"
"requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies"</td></tr>
</table>

<table>
<tr><th colspan="2">Enforcement</th></tr>
<tr><td colspan="2">Essential or important entity</td></tr>
<tr><td colspan="2">Art. 32(4) & Art. 33(4)
“issue warnings about infringements of this Directive by the entities concerned”
order entities to
“cease conduct that infringes this Directive”
“ensure that the[entities’] cybersecurity risk-management measures comply with Article 21” & “fulfil the reporting obligations laid down in Article 23” (both “in a specified manner and within a specified period”)
“inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat”</td></tr>
<tr><td>Essential entity</td><td>Important entity</td></tr>
<tr><td>Art. 32(4), Art. 32(5) & Art. 34(4)
“adopt binding instructions […] as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive”
“designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23”
administrative fines: up to 10 million euros or 2% of the entities’ “worldwide annual turnover in the preceding financial year”, “whichever is higher”
Ultima ratio enforcement powers [1]:
“suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out”
“[…] prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions”
[1] A Member State shall provide for these powers in cases where particular previous enforcement measures did not produce the desired outcome and an entity has also not complied with requested actions in a subsequently specified timeframe (Art. 32(5)).</td><td>Art. 33(4) & Art. 34(5)
“adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive”
administrative fines: up to 7 million euros or 1.4% of entities’ “worldwide annual turnover in the preceding financial year”, “whichever is higher”</td></tr>
</table>

When an essential entity is also designated as a critical entity under the CER Directive, the competent authorities under the NIS 2 Directive shall cooperate and inform those designated under the CER Directive of their intent to pursue supervisory or enforcement measures (Art. 32(9)). In addition, with respect to both essential and important entities, the national competent authorities under the NIS 2 Directive and the DORA Regulation shall cooperate and exchange information (Art. 32(10) and Art. 33(6)). For instance, when an essential or important entity classified

under NIS 2 also represents a critical ICT third-party service provider under the DORA Regulation, Member States must ensure that they inform the Oversight Forum established in the latter regulation "when exercising their supervisory and enforcement powers" (Art. 33(6)). In cases where an entity is the provider of services in at least one Member State or uses "network and information systems" that are located in more than one Member State, the NIS 2 Directive mandates the respective national competent authorities to cooperate with each other (Art. 37). This cooperation involves the sharing of information when supervisory or enforcement activities, the provision of mutual assistance[41], and "joint supervisory actions" (Art. 37(2)) at the end of the spectrum.

Who	What	When	Post-Deadline	Legal Basis
Member State	Notification of rules on penalties applicable to infringements → Commission	17 January 2025	Notification of any subsequent amendment to these rules must be notified without delay	Art. 36

Implementing and Delegated Acts

The NIS 2 Directive outlines various areas where the Commission either shall or may adopt implemented or delegated acts to specify particular provisions further. Areas for such subsequent non-legislative acts relate to:

Table 16: Implementing and Delegated Acts Foreseen Under the NIS 2 Directive

Implementing Acts	Delegated Acts [1]
• A. *May*: functioning of the NIS Cooperation Group (Art. 14(8)) • B. *Must (by 17 October 2024)*: technical and methodological requirements of cybersecurity risk management measures for specific entities [2] (Art. 21(5)) • C. *May*: technical, methodological and sectoral requirements of cybersecurity risk management measures for other essential and important entities [3] (Art. 21(5)) • D. *May*: specification of the type of information, format, and procedure of notification when	• *May*: Specification of "which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme" adopted in line with the Cybersecurity Act (Art. 24(2))

41 For further details on what mutual assistance may entail precisely and in which scenarios it may be enacted, see Art. 37(1).

reporting a significant incident or voluntarily sharing information on incidents, cyber threats, and near misses (Art. 23(11)) • E. *Must (by 17 October 2024)*: specification of "cases in which an incident shall be considered to be significant" for specific entities [4] (Art. 23(11)) • F. *May*: specification of "cases in which an incident shall be considered to be significant" for other essential and important entities (Art. 23(11)) [5]	

[1] The NIS 2 Directive initially foresees that the Commission can exercise this power until 16 January 2028. Either the Council or the European Parliament may withdraw the delegation of power "at any time" (Art. 38(3)). In such a scenario, any delegated acts adopted before the withdrawal remain valid. When drafting a delegated act, the Commission shall consult with Member State representatives. The European Parliament or the Council may object to the entry into force of a particular delegated act (see further Art. 38).
[2] These entities are DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.
[3] When drafting either implementing act B or C, the Commission shall "to the extent possible, follow European and international standards, as well as relevant technical specifications" (Art. 21(5)) and collaborate with both the NIS Cooperation Group and ENISA.
[4] These entities are DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.
[5] When drafting either implementing act E or F, the Commission shall collaborate with the NIS Cooperation Group (Art. 24(11)).

Review

Who	What	When	Post-Deadline	Legal Basis
Commission	Review of NIS 2 functioning and report to "be accompanied, where necessary, by a legislative proposal" → European Parliament and Council	17 October 2027	Every 36 months thereafter	Art. 40

— Regulation on ENISA and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act)

⬚⬚ Regulation on ENISA and on information and communications technology cybersecurity certification (2019/881)
Link: data.europa.eu/eli/reg/2019/881/oj

Entry into force: 27 June 2019 Date of application: 28 June 2021
Previous legislation: Repealed Regulation (EU) No 526/2013 since 27 June 2019
Subsequent documents of relevance: • February 2024: Union Rolling Work Programme for European cybersecurity certification • January 2024: Commission Implementing Regulation (EU) 2024/482
Objective (Art. 1): "ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union"
Subject matter (Art. 1): "This Regulation lays down: • (a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and • (b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union."
Actors established/regulated by the Cybersecurity Act: • ENISA, Art. 3-45 [see further Chapter 13] • European Cybersecurity Certification Group (ECCG), Art. 62 [see further Chapter 13]

Provisions setting out the mandate and objectives as well as the organization of ENISA (Art. 3-45) are discussed in the actor profile of ENISA.

The Cybersecurity Act sets up a European cybersecurity certification framework. The framework's objective is to provide for a "harmonised approach at Union level [...] with a view to creating a digital single market for ICT products[42], ICT services[43] and ICT processes[44]" (Art. 46(1)) by putting in place a procedure for European cybersecurity certification schemes.[45] In general, these schemes are voluntary for manufacturers and providers of ICT products, services, and processes unless a particular EU legal act stipulates them as binding in order to "demonstrate the presumption of conformity with [the legislation's] requirements" (Art. 54(3)). Once issued in any Member State, certificates and statements of conformity are valid in all Member States for their respectively foreseen duration.

The Commission adopts a "rolling work programme" identifying "strategic

42 The Cybersecurity Act defines an ICT product as "an element or a group of elements of a network or information system" (Art. 2, point (12)).

43 An ICT service is defined as "a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems" (Art. 2, point (13)).

44 An ICT process is defined as "a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service" (Art. 2, point (14)).

45 A European cybersecurity certification scheme is defined as "a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes" (Art. 2, point (9)).

priorities for future European cybersecurity certification schemes," to be updated at least every three years (Art. 47). In drafting the work programme, the Commission shall consider the views of the European Cybersecurity Certification Group (ECCG) and the Stakeholder Certification Group (SCCG) (Art. 47(4)). The current work programme can be found here.

Work programmes shall propose the inclusion of particular ICT products, ICT services, or ICT processes, for instance, based on at least one of the following considerations:

- (a) whether a national cybersecurity certification scheme on the specific category already exists or is being developed;
- (b) "relevant Union or Member State law or policy;"
- (c) "market demand;"
- and (d) "developments in the cyber threat landscape" (Art. 47(3)).

The standard procedure then foresees that the Commission can either request the preparation of a candidate scheme or the review of an existing European scheme when it falls inside the scope laid out in the work programme. When the particular schemes do not form part of the work programme, the Commission or ECCG may request preparation or review only in exceptional cases. ENISA may refuse preparing a scheme upon request by the ECCG but must provide reasons for doing so.

The establishment of a European cybersecurity certification scheme ensues from the following steps:

Table 17: Adoption Steps of a European Cybersecurity Certification Scheme

Step 1	Step 2	Step 3	Step 4	Step 5
Request of preparation or review of a (candidate) certification scheme by the Commission or ECCG (Art. 48)	Preparation of a candidate scheme by ENISA, including • the involvement of relevant stakeholders in an open consultation process, • the creation of an ad hoc working group [1], • and close cooperation	Submission of a candidate scheme by ENISA → Commission (Art. 49(6))	Adoption of implementing act by Commission stipulating the provision of a particular European cybersecurity certification scheme [2] (Art. 49(7))	Review of adopted European cybersecurity certification schemes every five years by ENISA (Art. 49(8))

	with the ECCG. (Art. 49(1)-(5))			

[1] The composition of ad hoc working groups includes "experts from Member States' competent authorities" (Art. 20(4)).
[2] The first scheme adopted concerns Common Criteria (Commission Implementing Regulation laying down rules for the application of Regulation 2019/881 as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (2024/482)). Other schemes currently under review relate to Cloud Services and 5G (ENISA: Developing Certification Schemes).

Upon the Commission's adoption of an implementing act specifying a particular European certification scheme, any existing national certification schemes on the same matter shall cease to exist (Art. 57(1)).[46] If a Member State aims to establish any new national cybersecurity certification scheme, it shall inform the Commission and the ECCG of its intention (Art. 57(4)).

In order to make it to stage four and be adopted as a European cybersecurity certification scheme, any scheme must specify particular elements. These elements include

- "evaluation criteria and methods [...] to demonstrate [achievement of...] security objectives;"
- information on whether the scheme assigns any assurance level and whether a scheme permits conformity self-assessments;
- a specification on how long issued certificates under the scheme are valid;
- and "rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with" (see further Art. 54(1)).

Among a scheme's **minimum security objectives** feature:

- the protection of "stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure [and "accidental or unauthorised destruction, loss or alteration or lack of availability"] during the entire life cycle of the ICT product, ICT service or ICT process;"
- the "identif[ication] and document[ation] of known dependencies and vulnerabilities;"
- the "verif[ication] that ICT products, ICT services and ICT processes do not contain known vulnerabilities;"
- and that ICT products, services, or processes are "secure by default and by design" (see Art. 51 for a complete list).

In addition, a scheme can include the provision of **assurance levels**, which the

46 To ensure a smooth transition, "existing certificates that were issued under national cybersecurity certification schemes and are covered by a European cybersecurity certification scheme shall remain valid until their expiry date" (Art. 57(3)).

Cybersecurity Act defines as "a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme" (Art. 2, point (21)). An assurance level specifies the degree of evaluation at a given time. Yet, it does not and does not aim to "measure the security of the ICT product, ICT service or ICT process concerned" (Art. 2, point (21)).

The Cybersecurity Act stipulates the following three assurance levels, which shall be assigned in proportion "with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident" (Art. 52(1)):

Table 18: Overview of Assurance Levels

'basic' Art. 52(5)	'substantial' Art. 52(6)	'high' Art. 52(7)
Minimum evaluation:		
review of technical documentation	"review [...] the absence of publicly known vulnerabilities and testing to demonstrate [...] correct[...] implement[ation of] the necessary security functionalities"	"testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing"
Requirements: "meet the corresponding security requirements, including security functionalities"		
+ "evaluat[ion] at a level intended to minimise the known basic risks of incidents and cyberattacks"	+ "evaluat[ion] at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources"	+ "evaluat[ion] at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources"

For ICT products, services or processes that fall in the category of the 'basic' assurance level, the Cybersecurity Act also foresees an exception by providing the (voluntary unless legally provided for) opportunity for conformity self-assessments by the manufacturer (Art. 53). It is the responsibility of the manufacturer to share the EU statement of conformity and relevant documentation with its national cybersecurity certification authority. A copy of the statement must also be submitted to ENISA.

As part of seeking certification under a European cybersecurity certification scheme, an ICT product, service, or process manufacturer/provider must also

provide additional information publicly, including, for instance, "the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates" (Art. 55(1), point (b)). An ICT product, service, or process manufacturer/provider must also, either toward the respective national cybersecurity certification authority or the conformity assessment body, forward information on "any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service or ICT process that may have an impact on its compliance with the requirements related to the certification" (Art. 56(8)).

To implement the Cybersecurity Act, each EU Member State must designate at least one national cybersecurity certification authority for the purposes of issuing certificates and supervising a scheme's compliance (Art. 58). To ensure compliance, a national cybersecurity certification authority may, for instance, "carry out investigations, in the form of audits, of conformity assessment bodies,[47] European cybersecurity certificates' holders and issuers of EU statements of conformity" (Art. 58(8), point (b)). National cybersecurity certification authorities shall actively participate in the ECCG (Art. 58(6)). National cybersecurity certification authorities must share a report outlining actions on specific activities with ENISA and the ECCG on an annual basis (Art. 58(7), point (g)). On the Union level, national cybersecurity certification authorities shall collaborate with their counterparts in other Member States as well as the Commission, especially in relation to "exchanging information, experience and good practices" (Art. 58(9)). To contribute to a harmonious application of European cybersecurity certification schemes, the activities and processes of a national cybersecurity certification authority may be reviewed by their peers (at least two national cybersecurity certification authorities of other Member States, Art. 59). A year after the adoption of a European cybersecurity certification scheme, the Commission is tasked with publishing a list of all EU-wide conformity assessment bodies (Art. 61(2)).

On a regular basis and at least every two years, the Commission shall "assess the efficiency and use of the adopted European cybersecurity certification schemes" (Art. 56(3)). This should also include evaluating "whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improve the functioning of the internal market" (Art. 56(3)).[48]

47 Conformity assessment bodies are entrusted with "perform[ing] conformity assessment activities including calibration, testing, certification and inspection" (Regulation 765/2008). In order to be designated as such, they must be accredited by a national accreditation body. National cybersecurity certification authorities must inform the Commission about all accredited conformity assessment bodies.

48 For instance, the NIS 2 Directive provides for such an opportunity (see further Art. 24 NIS 2 Directive).

Review

Who	What	When	Post-Deadline	Legal Basis
Commission	Evaluation of • impact, effectiveness and efficiency of ENISA and its working practices, including an assessment on the need to modify its mandate • impact, effectiveness and efficiency of the cybersecurity certification framework "with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improving the functioning of the internal market" • necessity of "essential cybersecurity requirements for access to the internal market"	28 June 2024	Every five years thereafter	Art. 67(1)
Commission	Submission of a report on the evaluation, with the findings to be publicized → European Parliament, Council and ENISA's Management Board	28 June 2024	Every five years thereafter	Art. 67(4)

Electronic Communications Networks

— 5G-Related Policies

In March 2019, the Commission published its ﷺ Recommendation on the cybersecurity of 5G networks[49], inter alia, recommending the establishment of a dedicated NIS Cooperation Group work stream and laying the basis for the adoption of subsequent EU policies in the area of 5G. In October 2019, the NIS Cooperation Group published an EU coordinated risk assessment of the cybersecurity of 5G networks, which builds upon prior national risk assessments shared by EU Member States. The 5G risk assessment identifies five main risk categories and nine related particular risk scenarios:

49 In the Recommendation, the Commission defines 5G networks as "a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy network elements based on previous generations of mobile and wireless communications technology such 4G or 3G. 5G networks should be understood to include all relevant parts of the network." (p. 4).

Table 19: Risks and Risk Scenarios Relating to 5G [this table reproduces Table 1 contained within the EU Toolbox of risk mitigating measures (p. 5)]

Category of Risk	Risk Scenario
Insufficient security measures	1: Misconfiguration of networks
	2: Lack of access controls
5G supply chain	3: Low product quality
	4: Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis
Modus operandi of main threat actors	5: State interference through 5G supply chain
	6: Exploitation of 5G networks by organised crime or organised crime group targeting end-users
Interdependencies between 5G networks and other critical systems	7: Significant disruption of critical infrastructures or services
	8: Massive failure of networks due to interruption of electricity supply or other support systems
End user devices	9: Exploitation of IoT, handsets or smart devices

In December 2019, the Council adopted ﷺ Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G, which call upon "Member States and the Commission with the support of ENISA to take all necessary measures within their competences to ensure the security and integrity of electronic communication networks, in particular 5G networks" (p. 9). Subsequently, in January 2020, the NIS Cooperation Group adopted a ﷺ "EU Toolbox of risk mitigating measures" in relation to the cybersecurity of 5G networks.[50] The Toolbox was subsequently endorsed by both the Commission and the European Council. Building upon the risks identified in the coordinated risk assessment, the Cybersecurity 5G Toolbox outlines a catalog of 19 either strategic or technical mitigation measures, which are complemented by ten supporting actions.[51] Strategic measures, inter alia, include the expansion of national regulatory powers and the strengthening of domestic resilience.[52] On a technical level, the Toolbox stipulates concrete measures that involve, for example, the "application of baseline security requirements", an "evaluati[on of] the

50 Progress reports on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity were published in 2020 and 2023 respectively.

51 The Toolbox, inter alia, specifies the drafting of guidance on implementing security-related measures in existing standards also covering 5G networks or "improv[ed] coordination in incident response and crisis management" (p. 13) as actions to support the attainment of the strategic and technical measures.

52 As strategic measures, the Toolbox lists, for example, the imposition of "strengthened obligations on operators" (p. 20) and working towards "an adequate balance of suppliers at national level" (p. 22).

implementation of security measures in existing 5G standards" and the enhancement of "software integrity, update and patch management" (p. 12).[53] The measures are particularly aimed at mobile network operators and telecom equipment manufacturers and are envisioned for implementation by both Member State entities and EUIBAs. It is at a Member State's discretion "to assess whether it has the resources to enforce the measure or if there is a need to cooperate with other Member States or at EU level" (p. 16). The Toolbox comprises two aspects: First, it describes the various measures, specifies which of the nine identified risk scenarios it serves to mitigate and designates which actors[54] may be involved in their implementation (see further Table 1 in Annex 1). In the second step, the Toolbox draws up risk mitigation plans for each of the nine risk scenarios. Such a risk mitigation plan stipulates each, which of the 19 measures are "most relevant/ high-impact," evaluates their "expected effectiveness" ranging from very high to low, includes potential positive and negative "implementation factors," and concludes with an "indicative timeframe" for the implementation of each measure (see further Table 3 on page 15 and Table 2 in Annex 1).

In June 2023, the Commission followed up with a ⬚⬚ Communication on the implementation of the 5G cybersecurity toolbox. In its Communication, the Commission, inter alia, highlights that it "considers [...] decisions adopted by Member States to restrict or exclude Huawei and ZTE [as] justified and compliant with the 5G Toolbox" (p. 3), since these suppliers would "in fact [represent] materially higher risks than other 5G suppliers" (p. 3). In taking stock of the status quo of the Toolbox's implementation, the Commission "urges Member States that have not yet implemented the Toolbox to adopt urgently relevant measures as recommended in the EU Toolbox" (p. 4). Looking inward, the Commission also announced that it would itself initiate measures to "avoid exposure of its corporate communications to mobile networks using Huawei and ZTE as suppliers", for instance, by "mak[ing] sure that those suppliers are progressively phased out from existing connectivity services of the Commission sites" (p. 4). Further, the Commission recommends other EUIBAs to do the same.

— Radio Equipment Directive

⬚⬚ Commission Delegated Regulation 2022/30 supplements the ⬚⬚ Radio

53 A full list of all strategic and technical measures can be found on page 12f. With regard to applicable EU legislation, the Toolbox notes that "many of the technical measures may be implemented in the context of the transposition of the European Electronic Communications Code" (p. 16) [ee further Chapter 6.2]. The Toolbox's technical measures also establish links with the EU cybersecurity certification schemes as they, for instance, outline the potential for "using EU certification for 5G network components, customer equipment and/or suppliers' processes" (p. 12), as was also initially foreseen in the Commission's 2019 Recommendation.

54 Among the actors listed in the Toolbox's Table 1 feature Member States, relevant authorities, operators, the Commission and ENISA.

Equipment Directive (RED, 2014). The Directive "establishes a regulatory framework for the making available on the market and putting into service in the Union of radio equipment"[55] (Art. 1(1) RED), and the Delegated Regulation further specifies particular essential requirements for radio equipment. Their specification is of cybersecurity relevance, as the "protection of the network or its functioning from harm [Art. 3(3), point (d) RED], protection of personal data and privacy of the user [Art. 3(3), point (e) RED] and of the subscriber and protection from fraud [Art. 3(3), point (f) RED] are [considered as] elements that support protection against cybersecurity risks" (recital (1), Commission Delegated Regulation 2022/30). Against this backdrop, the Delegated Regulation extends the scope of these requirements to "any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment" (Art. 1(1)). The essential requirements contained in the RED create obligations for economic operators. For instance, manufacturers must guarantee that both their design and radio equipment manufacturing comply with these requirements (Art. 10(1) RED). Member States, in turn, are tasked with "tak[ing] appropriate measures to ensure that radio equipment is made available on the market only if it complies with this Directive" (Art. 6 RED) when implementing and applying the RED.

— Electronic Communications Code

The ﷺ Directive on the European Electronic Communications Code (2018) outlines rules for electronic communication networks and services. Among other things, it establishes that Member States must "ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services" (Art. 40(1)).[56] Such measures should mainly aim at "prevent[ing] and minimi[zing] the impact of security incidents[57] on users and on other networks and services" (Art. 40(1)). To contribute to the similarity of specific requirements throughout the EU, ENISA is tasked with supporting coordination among Member States. In addition to taking risk management measures, the

55 Radio equipment is defined as "an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination" (Art. 2(1), point (1)).

56 Electronic communications networks and services are defined in Article 2. To specify the measures these need to implement, the Commission is granted the power to adopt implementing acts (Art. 40(5)). The 'security of networks and services' is being defined as "the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services" (Art. 2, point (21)).

57 A 'security incident' is being defined as "an event having an actual adverse effect on the security of electronic communications networks or services" (Art. 2, point (42)).

providers in the scope of the Electronic Communications Code must also, "without undue delay," notify a Member State's respective competent authority of a "security incident that has had a significant impact on the operation of networks or services" (Art. 40(2)). To decide whether a security incident is significant, the Directive lists five parameters for consideration:

- the "number of users affected;"
- "duration;"
- "geographical spread of the area affected;"
- "extent to which the functioning of the network or service is affected;"
- and "extent of impact on economic and societal activities" (Art. 40(2)).

Member States, via their competent authorities, shall inform each other and ENISA of such incidents if necessary. On an annual basis, the competent authorities must share with the Commission and ENISA a "summary report [...] on the notifications received and the action taken" (Art. 40(2)). To ensure supervision and compliance with this Directive, Member States shall, inter alia, equip their competent authorities with the powers to "issue binding instructions" to providers, for instance, on "measures required to remedy a security incident" (Art. 41(1)), requiring the provision of information by providers (Art. 41 (2)) and receiving support from the national CSIRT (Art. 4(4)). Competent authorities designated under both the Electronic Communications Code and the NIS 2 Directive shall "consult and cooperate" with each other "where appropriate" (Art. 41(5)).

Product Safety and Market Surveillance

— Regulation on General Product Safety

The ⬚⬚ Regulation on general product safety (2023) "lays down essential rules on the safety of consumer products placed or made available on the market" (Art. 1(2)). Its objective is to ensure a "high level of consumer protection" (Art. 1(1)). As a general rule, "only safe products[58] " may be placed or made available in the internal market (Art. 5). In order to be considered safe, a product must "under normal or reasonably foreseeable conditions of use, including the actual duration of use, [...] not present any risk or only the minimum risks compatible with the product's use, [be] considered acceptable and consistent with a high level of protection of the health and safety of consumers" (Art. 3, point (2)). With respect to cybersecurity,

58 The regulation defines a product as "any item, whether or not it is interconnected to other items, supplied or made available, whether for consideration or not, including in the context of providing a service, which is intended for consumers or is likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them" (Art. 3, point (1)).

the determination of a product's safety may include assessing whether, "when required by the nature of the product, the appropriate cybersecurity features necessary to protect the product against external influences, [...] where such an influence might have an impact on the safety of the product" (Art. 6(1), point (g)) were accommodated. The Regulation further notes in its recital that "specific cybersecurity risks affecting the safety of consumers [...] can be dealt with by sectoral legislation" (recital (26)).

— Regulation on Machinery

The ﷺ Regulation on machinery (2023) defines "health and safety requirements for the design and construction of machinery [...] to allow them to be made available on the market or put into service while ensuring a high level of protection of the health and safety of persons" (Art. 1). In relation to cybersecurity, the Regulation establishes links with EU cybersecurity certification schemes, as these may be used to demonstrate conformity with the requirements specified in the Regulation (Art. 20(9)). At the same time, the Regulation stresses in its recital that it "does not preclude the application to products within the scope of this Regulation of other Union legal acts specifically addressing cybersecurity aspects" (recital (25)).

— Regulation on Medical Devices & Regulation on in Vitro Diagnostic Medical Devices

The ﷺ Regulation on medical devices (2017) and the ﷺ Regulation on in vitro diagnostic medical devices (2017) "lay[...] down rules concerning [their] placing on the market, making available on the market or putting into service [...] in the Union" (Art. 1(1), Regulation 2017/746 and Art. 1(1) Regulation 2017/745). Both, inter alia, specify safety requirements for "electronic programmable systems", defined as "devices that incorporate electronic programmable systems and software that are devices in themselves" (Annex I). In this respect, the regulations stipulate that "the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation" (Annex I, 16 Regulation 2017/746 and Annex I, 17 Regulation 2017/745). In addition, manufacturers must comply with "set[ting] out minimum requirements concerning [...] IT security measures" (Annex I, 16.4 Regulation 2017/746 and Annex I, 17.4 Regulation 2017/745). The Regulation on medical devices mandated the development of a European database on medical devices (Euramed), on whose rules the Commission adopted ﷺ Implementing Regulation 2021/2078. The Implementing Regulation stipulates that in relation to IT security and as a general rule, Euramed must adhere to Commission Decision 2017/46.[59] Inter alia, the Commission must provide a

document that specifies “information security requirements for data exchange” (Art. 10(1)). Moreover, the Implementing Regulation lays out that when faced with a potentially harmful IT security incident, risk, or threat, the Commission may decide to suspend access to or functionalities of Euramed (Art. 10(3) and (4)).

— Regulation on Vehicle Type-Approval

The ﷺ Regulation on vehicle type-approval (2020) determines that particular categories of vehicles must meet outlined requirements, for instance, when it comes to “on-board instruments, electrical system, vehicle lighting and [their] protection against unauthorised use including cyberattacks” (Art. 4(5) (d)). In the area of cybersecurity, vehicle manufacturers must meet the requirements specified in UN Regulation No 155, setting out “uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system”.

Electronic Identification

— eIDAS Regulation

The ﷺ Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation, 2014) together with a ﷺ 2024 Regulation establishing the European Digital Identity Framework and a complementing ﷺ Commission Implementing Regulation 2015/1502 provide rules for attaining “an adequate level of security of electronic identification[60] means[61] and trust services[62] used across the Union” (Art. 1). To this end, the Regulation, inter alia, lays down rules for European Digital Identity Wallets[63] and electronic identification schemes. Such schemes are “system[s] for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons”

59 For an overview of Commission Decision 2017/46, see further Chapter 12.2.

60 Electronic identification is defined as “the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person” (Art. 3, point (1)).

61 Electronic identification means is defined as “a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service” (Art. 3, point (2)).

62 Trust services constitute “an electronic service normally provided for remuneration which consists of any of the following”, e.g. “issuance [or validation] of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services” (for further examples of respective services, see Art. 3, point (16)(a)-(n)).

63 The Regulation defines a European Digital Identity Wallet as “an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals” (Art. 3, point (42)), whose “issuance, use and revocation [...] shall be free of charge to all natural persons” (Art. 5a(13)). Their use shall be voluntary (Art. 5a(15)). In principle, the “source code of the application software components of European Digital Identity Wallets shall be open-source licensed”, for which only “duly justified” exceptions are foreseen (Art. 5a(2)).

(Art. 3, point (4))[64] which shall specify levels of assurance levels, such as low, substantial or high (Art. 8). As part of an electronic identification scheme, the Regulation foresees the creation of European Digital Identity Wallets. The Regulation tasks Member States to "provide at least one European Digital Identity Wallet" within a specified timeframe (following the adoption of implementing acts by the Commission) in order to "ensur[e] that all natural and legal persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data" (Art. 5a(1)). In addition to use cases for users and technical specifications, the Regulation stipulates that "European Digital Identity Wallets shall ensure security-by-design" (Art. 5a(12)) and "Member State shall inform users, without delay, of any security breach that could have entirely or partially compromised their European Digital Identity Wallet or its contents" (Art. 5a(6)). When they concern cybersecurity, European Digital Identity Wallets shall be certified in the framework of European cybersecurity certification schemes as provided for by the Cybersecurity Act (Art. 5c(2)). In cases such a scheme(s) "do not, or only partially, cover those cybersecurity requirements [...] Member States shall establish national certification schemes" (Art. 5c(3)). The Commission is tasked with "establish[ing] a list of reference standards and, where necessary, establish specifications and procedures for the certification of European Digital Identity Wallets" (Art. 5c(6)) by 21 November 2024. In terms of review, the Regulation mandates the Commission to assess, "within 24 months after deployment of the European Digital Identity Wallets," the "demand for, and the availability and usability of, European Digital Identity Wallets" (Art. 5f(5)). The Regulation determines that not only the European Digital Identity Wallets but also the "conformity of electronic identification schemes to be notified with the cybersecurity requirements laid down in this Regulation [...] shall be certified by conformity assessment bodies designated by Member States" (Art. 12a(1)). In principle, such certification "shall be carried out under a relevant cybersecurity certification scheme pursuant to [the Cybersecurity Act] or parts thereof, insofar as the cybersecurity certificate or parts thereof cover those cybersecurity requirements" (Art. 12a(3)). Once provided, respective certifications shall have a temporal validity of five years, on the condition that "a vulnerability assessment is carried out every two years" (Art. 12a(3)).[65]

The Regulation further designates how Member States have to act in instances of security breaches for electronic identification schemes[66] in general and European

64 The Regulation further notes that Member States shall ensure interoperability between their electronic identification schemes (Art. 12).

65 Cases where an identified vulnerability is "not remedied within three months of such identification" shall result in the cancellation of the respective certificate (Art. 12a(3)).

66 The Regulation further specifies that the reporting obligations apply to "electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7" (Art. 10 (1)).

Digital Identity Wallets in particular[67].

Table 20: Actions to Be Taken by Member States Following Security Breaches

	Electronic Identification Schemes (Art. 10)	European Digital Identity Wallet (Art. 5e)
When	"breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme" (Art. 10(1))	"breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets" (Art. 5e(1))
General	• "notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission" (Art. 10(1))	Art. 5e (1): • "Member State that provided the European Digital Identity Wallets shall, without undue delay, suspend the provision and the use of European Digital Identity Wallets" • "Where justified by the severity of the security breach or compromise referred to in the first subparagraph, the Member State shall withdraw European Digital Identity Wallets without undue delay" • "Member State shall inform the users affected, the single points of contact [...], the relying parties and the Commission accordingly"
No remediation within three months of suspension/ revocation	• "notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme" (Art. 10(3))	Art. 5e (2): • "Member State that provided the European Digital Identity Wallets shall withdraw European Digital Identity Wallets and revoke their validity" • "Member State shall inform the users affected, the single points of contact [...]), the relying parties and the Commission of the withdrawal accordingly"
Remediated breach or incident	• "notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay" (Art. 10(2))	Art. 5e (3): • "providing Member State shall re-establish the provision and the use of European Digital Identity Wallets and inform the affected users and relying parties, the single points of contact [...] and the Commission without undue delay"

67 The Regulation further specifies that the reporting obligations apply to "European Digital Identity Wallets provided pursuant to Article 5a, the validation mechanisms referred to in Article 5a(8) or the electronic identification scheme under which the European Digital Identity Wallets are provided" (Art. 5e(1)). The European Digital Identity Wallets are, inter alia, not subject to the requirements contained in Art. 10 (Art. 5a(22)).

The Regulation also defines security requirements for trust service providers. In accordance, both "qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide" (Art. 19(1)) referencing the cybersecurity risk management measures contained in the NIS 2 Directive (Art. 19a(1), point (a) and Art. 20(1), see further Art. 21 Directive).

The Regulation further specifies reporting requirements on these trust service providers when "any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein" (Art. 19(2)) occurs. The Regulation foresees the following actions to be taken by trust service providers and supervisory authorities:

Table 21: Reporting Requirements by Trust Service Providers and Notified Supervisory Authorities

Tasks to Be Undertaken by Trust Service Providers	Tasks to Be Undertaken by Notified Supervisory Authorities
Art. 19(2): • "without undue delay but in any event within 24 hours after having become aware of it" → "notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority" • "where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided" "without undue delay" → "notify the natural or legal person of the breach of security or loss of integrity"	• "where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States" → "inform the supervisory bodies in other Member States concerned and ENISA" (Art. 19(2)) • "where it determines that disclosure of the breach of security or loss of integrity is in the public interest" → "inform the public or require the trust service provider to do so" (Art. 19(2)) • submission of a "summary of notifications of breach of security and loss of integrity received from trust service providers" annually > ENISA (Art. 19(3))

Member States are required to publicize, inter alia, statistics on "significant security incidents, data breaches and affected users of European Digital Identity Wallets or of qualified trust services" in "an open and commonly used, machine-readable format" (Art. 48a(2), point (e)).

With regard to governance, the Regulation directs Member States to designate supervisory authorities for the supervision of the European Digital Identity Framework and trust services (Art. 46a and 46b). Among their tasks is informing the competent authorities designated pursuant to the NIS 2 Directive "of the Member States concerned of any significant security breaches or loss of integrity of

which they become aware in the performance of their tasks" and, "in the case of a significant security breach or loss of integrity which concerns other Member States," informing the respective SPOCs designated pursuant to the NIS 2 Directive and this Regulation in the Member States affected (Art. 46a(4), point (c) and Art. 46b(4), point (a)). Member States shall further determine a "single point of contact [SPOC] for trust services, European Digital Identity Wallets and notified electronic identification schemes" (Art. 46c). This SPOC is tasked with "exercis[ing] a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and between the supervisory bodies for the providers of European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity (ENISA) and with other competent authorities within its Member State" (Art. 46c(2)). The Regulation also provides a legal basis for the provision of mutual assistance among Member States (Art. 46d) and establishes the European Digital Identity Cooperation Group[68] (Art. 46e).

Data Protection and Data Economy

— General Data Protection Regulation

The ⬚⬚ General Data Protection Regulation (GDPR, 2016) outlines conditions and limits for the lawfulness of processing data. It creates obligations for controllers and processors of data located within the EU "regardless of whether the processing [itself] takes place in the Union or not" (Art. 3(1)). As one of its six overarching general principles, the Regulation stipulates that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')" (Art. 5(1), point (f)). In further detail, the GDPR also includes a provision outlining security requirements for the processing of data (Art. 32). Accordingly, controllers and processors of personal data must "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" (Art. 32(1)). As examples of such measures, the GDPR lists:

68 The European Digital Identity Cooperation Group comprises Member States' and Commission representatives. The Commission acts as its Secretariat. Inter alia, the Group is tasked with "support[ing] the supervisory bodies in the implementation of the provisions of this Regulation" (Art. 46e(5)) by means of "exchang[ing] views, best practices and information on relevant cybersecurity aspects concerning European Digital Identity Wallets, electronic identification schemes and trust services" (Art. 46e(5), point (iv)), supported by ENISA, "exchang[ing] best practices in relation to the development and implementation of policies on the notification of security breaches" (Art. 46e(5), point (v)), and "organis[ing] joint meetings with the NIS Cooperation Group [...] to exchange relevant information in relation to trust services and electronic identification related cyber threats, incidents, vulnerabilities, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications capacity as well as standards and technical specifications" (Art. 46e(5), point (vi)). ENISA may be invited to participate in the Group's proceedings as an observer when the Group "exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, and when the use of cybersecurity certificates or standards are addressed" (Art. 46e(4)).

- “the pseudonymisation and encryption of personal data;”
- “the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;”
- “the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;”
- and “a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing” (Art. 32(1)).

When a controller experiences a breach in relation to the personal data it processes, it “shall without undue delay and, where feasible, not later than 72 hours after having become aware of it” report it to its respective supervisory authority, “unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons” (Art. 33). EU Member States are, inter alia, responsible for monitoring the application and compliance of controllers and processors with the GDPR and are tasked with “promot[ing] public awareness and understanding of the risks, rules, safeguards and rights in relation to processing” (Art. 57).

— Data Governance Act

The ﷺ Regulation on European data governance (Data Governance Act, 2022), inter alia, establishes the European Data Innovation Board. Tasks of the Board comprise “advis[ing] and assist[ing] the Commission with regard to developing consistent guidelines for cybersecurity requirements for the exchange and storage of data” (Art. 30, point (e)) and “propos[ing] guidelines for common European data spaces, namely purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data [...] addressing [...] adherence to cybersecurity requirements in accordance with Union law” (Art. 30, point (h)). ENISA is among the Board’s members. Further, in relation to non-personal data, the Regulation specifies that “data intermediation services provider[s] shall take necessary measures to ensure an appropriate level of security for the[ir] storage, processing and transmission” and, concerning “competitively sensitive information,” highlights that “data intermediation services provider[s] shall [...] ensure the highest level of security for the[ir] storage and transmission” (Art. 12).

General Rules

— Chips Act

The ﷺ Chips Act (2023) provides “a framework for strengthening the semiconductor ecosystem at Union level” (Art. 1(1)). It addresses cybersecurity

considerations in so far that the established Chips for Europe Initiative also includes the construction of chips based upon security-by-design principles among its operational objective 1 (“building up advanced design capacities for integrated semiconductor technologies,” Art. 5(a), point (ii)), as this can “provide protection against cybersecurity threats” (Art. 4(1)).

— Digital Markets Act

The ﷺ Digital Markets Act (2022) specifies “harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users” (Art. 1(1)). To this end, it lays down obligations for so-called gatekeepers, which are defined as “an undertaking providing core platform services” (Art. 2, point (a)) and further meet specific characteristics such as having “a significant impact on the internal market” (Art. 3(1), point (a) and further specified in Art. 3(2)). Gatekeepers shall, inter alia, ensure that when meeting their obligations under the Digital Markets Act Articles 5-7, the “implementation of those measures complies with [...] legislation on cyber security” (Art. 8(1)). The power to “monitor the effective implementation and compliance with [these] obligations” (Art. 26(1)) rests with the Commission.

Council Conclusions and Resolutions

— Council Conclusions on ICT Supply Chain Security

The ﷺ Council conclusions on ICT supply chain security (October 2022) highlight various cross-sectoral and cyber-specific instruments as well as supporting mechanisms to increase the security of ICT supply chains, inter alia, in an effort to seek “strategic autonomy while preserving an open economy” (p. 5). The Conclusions note the need for an “all-hazard approach [...] in securing ICT assets” (p. 4). It classifies ICT supply chain security to include the “protection of ICT products and services produced, delivered, procured and used in ICT supply chains, including by means of protecting individual components and transmitted data” (p. 4). Among the cross-sectoral instruments and approaches, Member States delineate the “avoidance of vendor lock-in and the diversification of ICT suppliers as one of the important components for ensuring stability and security of the internal market” (p. 7) and take further note that the “EU’s Foreign Direct Investment Screening mechanism[69] [...] could also be applied as a useful tool for safeguarding

69 For an explanation of cybersecurity considerations in relation to the EU’s FDI screening mechanism, see further Chapter 7.4.

security and resilience of the ICT supply chain" (p. 8). The Conclusions also refer to public procurement as a possible tool and therefore invite the Commission, inter alia, to "develop methodological guidelines [...] to encourage the contracting authorities to put appropriate focus on the cybersecurity practices of tenderers and their subcontractors" (p. 7). As part of the cyber-specific instruments, Member States refer to the EU 5G Toolbox,[70] existing horizontal and sector-specific legislation, respective legislative initiatives such as the Cyber Resilience Act and efforts underway to develop cybersecurity certification schemes. EU Member States further encourage ENISA to perform three specific tasks: conducting a best practices stocktaking exercise on supply chain risk management (supported by the NIS Cooperation Group), developing "methodological guidelines" on that basis, as well as "monitor[ing of] investments in the ICT supply chain security of the entities regulated under the forthcoming NIS 2 Directive" (p. 11). EU Member States further express the invitation to the NIS Cooperation Group (supported by the Commission and ENISA) "to develop a toolbox of measures for reducing critical ICT supply chain risks" on the basis of "strategic threat scenarios identified for ICT supply chains" (p. 13) – the ICT Supply Chain Toolbox. With respect to the mandate of other actors at EU level, the Conclusions "invite[...] the ECCC to take into account the ICT supply chain security aspects, including, for instance, secure software development, into their Strategic Agenda" (p. 14). Finally, as so-called supporting mechanisms, the Conclusions, for example, list "boosting financial support incentives related to measures aimed at strengthening ICT supply chain security" (p. 15), for instance, in the framework of Digital Europe[71] or Horizon Europe[72] and leveraging, at the global level, "digital partnerships, cyber dialogues and other relevant EU initiatives, [...] for the promotion of risk-based evaluations of ICT product suppliers and ICT services providers" (p. 16).

— Council Conclusions on the Cybersecurity of Connected Devices

The ﷺ Council conclusions on the cybersecurity of connected devices (December 2020), inter alia, stress the necessity of "a high level of complementarity and comparability of security functionalities of ICT systems and ICT components, which are used in many different sectors of the Digital Single Market" (p. 4) and take positive note of "current developments at Union level to raise the level of cybersecurity of connected devices" (p. 4), for instance, via the Radio Equipment Directive or the development of cybersecurity certification schemes. In order to

70 The EU's 5G Toolbox is explained within Chapter 6.2.

71 The EU's Digital Europe Programme is explained in Chapter 5.3.

72 Cybersecurity-related components of Horizon Europe are reflected within Chapter 10.2.

elevate the level of cybersecurity across connected devices, the Conclusions "call [...] for coordination and close cooperation with all relevant public and private stakeholders, also in view of a possible future horizontal legislation" (p. 5). Specifically with respect to cybersecurity certification, EU Member States underline "the need to establish cybersecurity norms, standards or technical specifications for connected devices" (p. 5) and encourage further respective activities by European Standards Organisations, such as the European Telecommunications Standards Institute (ETSI). The Conclusions further invite "the Commission to consider a request for a candidate cybersecurity certification schemes for connected devices and related services" (p. 6) and note their appreciation for "a discussion on how the goal of cybersecurity could be anchored in a future horizontal legislation that covers cybersecurity risks related to connected devices" (p. 6).

— Council Resolution on Encryption

The ��Council Resolution on Encryption (November 2020) calls for adherence to "the principle of security through encryption and security despite encryption [...] in its entirety" (p. 4). The Resolution highlights the need for striking a balance on the basis of "necessity, proportionality and subsidiarity" between "protecting the privacy and security of communications through encryption" on the one and "upholding the possibility for competent authorities in the area of security and criminal justice to lawfully access relevant data for legitimate, clearly defined purposes in fighting serious and/or organized crimes and terrorism, including in the digital world, and upholding the rule of law" on the other hand (p. 4). The Resolution further notes the possibility of exploring the development of a dedicated EU-wide regulatory framework in this regard (p. 5). EU Member States also stress their support for further promoting and developing encryption as "an anchor of confidence in digitalisation and in protection of fundamental rights" (p. 4), for instance, by engaging in "active discussion" (p. 4) and cooperation with the tech industry.

Policy Area 3: Economic, Monetary and Commercial Policy

The Treaty of the EU stipulates that the EU "shall establish an economic and monetary

union whose currency is the euro" (Art. 3(4) TEU). The Treaty on the Functioning of the EU further specifies that this involves the "the adoption of an economic policy which is based on the close coordination of Member States' economic policies, on the internal market and on the definition of common objectives, and conducted in accordance with the principle of an open market economy with free competition" (Art. 119(1) TFEU). The EU and its Member States share competence in the area of "economic [...] cohesion" (Art. 4(2), point (c) TFEU). The EU holds exclusive competence for "monetary policy for the Member States whose currency is the euro" (Art. 3(1), point (c) TFEU) and the EU's "common commercial policy" (Art. 3(1), point (e) TFEU).

Deep Dive: Digital Operational Resilience Act (DORA)

⬜ Regulation on digital operational resilience for the financial sector (2022/2554)
Link: data.europa.eu/eli/reg/2022/2554/oj
Entry into force: 16 January 2023 Date of application: 17 January 2025
Previous legislation: NA
Subsequent documents of relevance [for other non-legislative acts under preparation pursuant to DORA, see further Chapter 14]: • June 2024: Commission Delegated Regulation specifying the criteria for the designation of ICT third-party service providers as critical for financial entities (2024/1502) • June 2024: Commission Delegated Regulation determining the amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid (2024/1505)
Objective (Art. 1(1)): "achieve a high common level of digital operational resilience"
Subject matter (Art. 1): "This Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows: • (a) requirements applicable to financial entities in relation to: (i) information and communication technology (ICT) risk management; (ii) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities; (iii) reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in Article 2(1), points (a) to (d); (iv) digital operational resilience testing; (v) information and intelligence sharing in relation to cyber threats and vulnerabilities; (vi) measures for the sound management of ICT third-party risk; • (b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities; • (c) rules for the establishment and conduct of the Oversight Framework for critical ICT third-party service providers when providing services to financial entities; • (d) rules on cooperation among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation."
Actors established/regulated by the DORA Regulation: • Oversight Forum, Art. 32

Scope

DORA places information and cybersecurity-related obligations on financial entities, for instance, credit institutions, payment institutions, or investment firms, to attain a "high common level of digital operational resilience" (Art. 1(1)).[73] The Regulation defines digital operational resilience as "the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions" (Art. 3, point (1)). It applies the NIS 2 Directive's definition of security of network and information systems. For financial entities that are also designated as essential or important entities under the NIS 2 Directive, DORA functions as "a sector-specific Union legal act" (Art. 1(2)). The DORA Regulation lays down a 'proportionality principle,' according to which the implementation of rules on ICT risk management (Chapter II) and the application of provisions on (a) ICT-related incident management, classification and reporting (Chapter III); (b) digital operational resilience testing (Chapter IV); and (c) ICT-third party risk management (Chapter V, Section I) shall either "take into account" or "be proportionate" to the financial entities' "size and overall risk profile, and the nature, scale and complexity of their services, activities and operations" (Art. 4(1) and (2)).

Competent Authorities

The competent authorities for supervising compliance with the DORA Regulation depend on the type of financial entity and further applicable legal bases. They shall closely cooperate with each other (Art. 48(1)). For instance, for credit institutions, this is the competent authority designated under Directive 2013/36 (for a complete list of entities and their competent authorities see Art. 46). To ensure cooperation,

73 For a full list of entities within the scope of DORA and exceptions thereto, see Art. 2.

both the European Supervisory Authorities (ESAs)[74] and the competent authorities "may participate in the activities of the [NIS] Cooperation Group for matters that concern their supervisory activities in relation to financial entities" and "may request to be invited to participate in the activities of the [NIS] Cooperation Group for matters in relation to essential or important entities [...] that have also been designated as critical ICT third-party service providers" within the DORA Regulation (Art. 47(1)). Article 47 also provides a basis for consultations and information-sharing among the DORA's competent authorities with the SPOCs and CSIRTs designated under the NIS 2 Directive (Art. 47(2)). Competent authorities under the DORA Regulation "may request any relevant technical advice and assistance" on the part of NIS 2's competent authority and both may formalize their cooperation through "cooperation agreements" (Art. 47(3)). Furthermore, the competent authorities shall engage in close cooperation and "exchange information to carry out their duties pursuant to Articles 47 to 54" with the ESAs and the European Central Bank (ECB) (Art. 48(2)). To ensure cooperation across the financial sector, the DORA Regulation foresees that the ESA Joint Committee (JC) together with the Member States' competent authorities and other actors may "establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across sectors" as well as "develop crisis management and contingency exercises involving cyber-attack scenarios with a view to developing communication channels and gradually enabling an effective coordinated response at Union level" (Art. 49(1)).

ICT Risk Management by Financial Entities

The DORA Regulation defines ICT risk as "any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment" (Art. 3, point (5)). To counter respective circumstances, financial entities are required to have an "internal governance and control framework that ensures an effective and prudent management of ICT risk" (Art. 5(1)), for whose development and implementation a financial entity's management body holds responsibility (Art. 5(2)). In addition to ensuring compliance with these governance-related ICT risk management requirements, DORA further requires that financial entities have a "sound, comprehensive and well-documented ICT risk management framework [in place] as part of their overall risk management system,

74 The role of the ESAs in EU cybersecurity policy is further touched upon within Chapter 13.3.

which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience" (Art. 6(1)). This comprises, inter alia, at least "strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets" (Art. 6(2)), which must be documented. In relation to strategies, financial entities must adopt a digital operational resilience strategy "setting out how the framework shall be implemented" (Art. 6(8)). As part of the strategy, financial entities shall, for instance, specify "clear information security objectives, including key performance indicators and key risk metrics" and elaborate on "different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it" (Art. 6(8), points (c) and (e)). Financial entities shall review the framework annually or upon major incidents, supervisory instructions, or other relevant information (Art. 6(5)).

The ICT risk management framework further encompasses the following elements:

Table 22: Overview of ICT Risk Management Framework Elements

Elements	Examples
ICT systems, protocols, and tools (Art. 7)	• Usage and maintenance of "updated ICT systems, protocols and tools", which, inter alia, are "appropriate to the magnitude of operations supporting the conduct of their activities" and "reliable"
Identification (Art. 8)	• Identification, classification, and adequate documentation of "all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk" (Art. 8(1)) • Continuous identification of "all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets" (Art. 8(2)) • Performance of a "risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets" (Art. 8(3)) • Identification of "all information assets and ICT assets, including those on remote sites, network resources and hardware equipment" and mapping of "those considered critical" (Art. 8(4)) • Identification and documentation of "all processes that are dependent on ICT third-party service providers" and identification of "interconnections with ICT third-party service providers that provide services that support critical or important functions" (Art. 8(5)) • At least annual conduct of a "specific ICT risk assessment on all legacy ICT systems" (Art. 8(7))
Protection and prevention (Art. 9)	• Continuous monitoring and control of "the security and functioning of ICT systems and tools" and "deployment of appropriate ICT security tools, policies and procedures" to minimize ICT risk (Art. 9(1)) • Design, procurement, and implementation of "ICT security policies, procedures, protocols and tools that aim to ensure the resilience,

	continuity and availability of ICT systems [...and] maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit" (Art. 9(2)) • Development and documentation of "an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable" (Art. 9(4), point (a)) • Implementation of "policies and protocols for strong authentication mechanisms" (Art. 9(4), point (d)) • Existence of "appropriate and comprehensive documented policies for patches and updates" (Art. 9(4), point (f))
Detection (Art. 10)	• Existence of "mechanisms to promptly detect anomalous activities", "enabl[ing] multiple layers of control, defin[ing] alert thresholds and criteria to trigger and initiat[ing] ICT-related incident response processes" (Art. 10(1)) • Devotion of "sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents" (Art. 10(3))
Response and recovery (Art. 11)	• Adoption of a "comprehensive ICT business continuity policy" (Art. 11(1)) • Implementation of "associated ICT response and recovery plans" (Art. 11(3)) and at least annual testing (Art. 11(6), point (a)) • Maintenance and periodical testing of "appropriate ICT business continuity plans"(Art. 11(4)) at least annually (Art. 11(6), point (a)) • Conduct of a "business impact analysis of [...] exposures to severe business disruptions" (Art. 11(5)) • Designation of a "crisis management function, which, in the event of activation of their ICT business continuity plans or ICT response and recovery plans, shall, inter alia, set out clear procedures to manage internal and external crisis communications" (Art. 11(7))
Backup policies and procedures, restoration and recovery procedures and methods (Art. 12)	• Development and documentation of "backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data" and "restoration and recovery procedures and methods" (Art. 12(1)) • "Set up [of] backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods" (Art. 12(2)) • Maintenance of "redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs" (Art. 12(4))

Learning and evolving (Art. 13)	• "Capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse the impact they are likely to have on their digital operational resilience" (Art. 13(1))
	• Initiation of "post ICT-related incident reviews after a major ICT-related incident disrupts their core activities", "determin[ing] whether the established procedures were followed and the actions taken were effective, including in relation to the following:
	  • the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;
	  • the quality and speed of performing a forensic analysis, where deemed appropriate;

	• the effectiveness of incident escalation within the financial entity; • the effectiveness of internal and external communication" (Art. 13(2)) • Monitoring of "effectiveness of the implementation of their digital operational resilience strategy" and mapping of "evolution of ICT risk over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents [...] with a view to understanding the level of ICT risk exposure" (Art. 13(4)) • Development of "ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes" (Art. 13(6))
Communication (Art. 14)	• Availability of "crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate" (Art. 14(1)) • Implementation of "communication policies for internal staff and for external stakeholders" (Art. 14(2))

For specific types of entities, the requirement of a "simplified ICT risk management framework" applies (see further Art. 16). As a contribution to the harmonization of ICT risk management tools, methods, processes and policies as part of the ICT risk management framework, DORA tasks the ESAs together with ENISA to "develop common draft regulatory technical standards" in various areas and elements of the simplified framework by 17 January 2024 (Art. 15 and 16).[75] DORA further provides a foundation for financial entities to "exchange amongst themselves cyber threat information and intelligence" when such exchange meets specific objectives and is conducted based on "information-sharing arrangements" (Art. 45(1)). Financial entities shall inform their competent authority of their participation or withdrawal from these arrangements (Art. 45(3)).

ICT-Related Incident Management, Classification and Reporting

In order to "detect, manage and notify ICT-related incidents", financial entities must put in place an "**ICT-related incident management process**" and ensure a recording of "all ICT-related incidents and significant cyber threats" (Art. 17). The Regulation defines an ICT-related incident as "a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity" (Art. 3, point (8)). A significant cyber threat is defined as a "cyber threat the

75 See further, for instance, European Securities and Markets Authority: ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification.

technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident[76] or a major operational or security payment-related incident" (Art. 3, point (13)).[77] Requirements of Articles 17-22 are also applicable to "operational or security payment-related incidents and to major operational or security payment-related incidents, where they concern credit institutions, payment institutions, account information service providers, and electronic money institutions"[78] (Art. 23).

A financial entities' ICT-related incident management process, shall include the following elements:

- existence of "early warning indicators;"
- establishment of "procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted;"
- designation of "roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;"
- development of communication plans as specified in Article 14 and plans for client notification, "internal escalation procedures" and information-sharing with counterparts;
- guarantee that "relevant senior management" are reported to and the management board is being informed of "at least major ICT-related incidents [...] explaining [to them] the impact, response and additional controls to be established as a result of such ICT-related incidents;"
- and establishment of "ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner" (Art. 17(3)).

Moreover, financial entities are required to classify ICT-related incidents and evaluate their impact, inter alia, based on these considerations:

- "number and/or relevance of clients or financial counterparts affected;"
- "duration of the ICT-related incident;"
- "geographical spread;"
- involved "data losses [...] in relation to availability, authenticity, integrity or confidentiality of data;"
- "criticality of the services affected;"

76 A major ICT-related incident denotes "an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity" (Art. 3, point (10).

77 Art. 18(2) further specifies that financial entities "shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk".

78 Applicable to these types of financial entities, an operational or security payment-related incident is defined as "a single event or a series of linked events unplanned by the financial entities [...] whether ICT-related or not, that has an adverse impact on the availability, authenticity, integrity or confidentiality of payment-related data, or on the payment-related services provided by the financial entity" (Art. 3, point (9)). Such an incident is considered major, when it causes a "high adverse impact on the payment-related services provided" (Art. 3, point (11).

- and "economic impact" (Art. 18(1)).

The ESAs, upon consultation with the ECB and ENISA, are tasked with further specifying these criteria, among other aspects, by "develop[ing] common draft regulatory technical standards" (Art. 18(3)).

When a major ICT-related incident occurs, financial entities shall notify them to their respective competent authority (Art. 19(1)).[79]

Table 23: Overview of DORA's Incident Reporting Obligations

I. Action to be taken by financial entity	
(a) "without undue delay as soon as they become aware"	(b) "within the time limits [...] laid down in" common draft regulatory technical standards
Notification of clients about major ICT-related incidents and the "measures that have been taken to mitigate the adverse effects of such incident" (Art. 19(3))	→ competent authority (Art. 19(4)) [1]: • Submission of an initial notification • Submission of "an intermediate report after the initial notification [...] as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available" • Submission of a final report
[1] The Regulation also foresees the possibility that "Member States may additionally determine that some or all financial entities shall also provide the initial notification and each report [...] to the competent authorities or the computer security incident response teams (CSIRTs) designated or established" under the NIS 2 Directive (Art. 19(1)). A similar possibility is specified in relation to the voluntary notification of significant cyber threats (Art. 19(2)).	

II. Action to be taken by competent authority	
(a) Upon receipt of initial notification and each report "in a timely manner"	(b) Upon notification by EBA, ESMA or EIOPA *[as specified in III]*
• Provision of details of the major ICT-related incident → EBA, the ECB (in specific cases) or the competent authorities, SPOCs or CSIRTs designated under the NIS 2 Directive, among other actors, "as applicable, on their respective competences" (Art. 19(6)) • Acknowledgment of receipt and, "where feasible", provision of "relevant and proportionate feedback or high-level guidance to the financial entity" [2] (Art. 22 (1))	"Where appropriate, take all of the necessary measures to protect the immediate stability of the financial system" (Art. 19(7))

79 In cases where financial entities operate across borders and are thus supervised by more than one competent authority, Member States shall determine one single competent authority for the purposes of reporting as further specified in Article 20.

[2] In particular, this may involve the "making available any relevant anonymised information and intelligence on similar threats" or "discuss remedies applied at the level of the financial entity and ways to minimise and mitigate adverse impact across the financial sector" (Art. 22(1)).

III. Action to be taken by "EBA, ESMA, or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority"

"following receipt of information" by competent authority
[as specified in II (a)]

Assessment "whether the major ICT-related incident is relevant for competent authorities in other Member States" and notification of relevant competent authorities in other Member States "as soon as possible" (Art. 19(7))

Irrespective of any feedback received by the respective competent authority (II (a)), "financial entities shall remain fully responsible for the handling and for consequences of the ICT-related incidents reported" (Art. 22(1)). Voluntarily, financial entities can also share "significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients" with their competent authorities (Art. 19(2)). The ESAs are tasked to

- with the involvement of ENISA and the ECB:
  - draft "common draft regulatory technical standards [RTS]," inter alia, "establish[ing] the content of the reports for major ICT-related incidents" and "determin[ing] the time limits for the initial notification and for each report referred to in Article 19(4)" (Art. 20, point (a)) [1];
  - draft "common draft implementing technical standards" (ITS) on "standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat" (Art. 20, point (b));
  - and compile a "joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities" (Art. 21),
- through the Joint Committee, "report yearly on major ICT-related incidents [...] setting out at least the number of major ICT-related incidents, their nature and their impact on the operations of financial entities or clients, remedial actions taken and costs incurred" (Art. 22(2));
- "issue warnings and produce high-level statistics to support ICT threat and vulnerability assessments" (Art. 22(2)).

[1] In the drafting of these RTS, the ESAs shall maintain "a consistent approach to ICT-related incident reporting" (Art. 20, point (a)) that is in line with the NIS 2 Directive (or otherwise justify any related deviations). Furthermore, in relation to DORA's particular scope, the ESAs "shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, and in particular, [...] different time limits may

reflect, as appropriate, specificities of financial sectors" (Art. 20, point (a)).

Who	What	When	Legal Basis
ESAs	Submission of a joint report on the "feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities" → European Parliament, Council and Commission	17 January 2025	Art. 21(3)
ESAs	Report on major ICT-related incidents through Joint Committee	On an annual basis	Art. 22(2)

Digital Operational Resilience Testing

Financial entities shall "establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the[ir] ICT risk-management framework" (Art. 24(1)), with tests to be conducted "on all ICT systems and applications supporting critical or important functions" at least once a year (Art. 24(6)) by internal or external independent testers. Tests may include "vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing" (Art. 25(1)). Specific provisions apply to microenterprises, central securities depositories, and central counterparties. Competent authorities must identify which financial entities are subject to "advanced testing by means of [threat-led penetration testing] TLPT"[80] (Art. 26(1)). Entities to which the requirement of a simplified ICT risk management framework (see further Art. 16(1)) applies and microenterprises are exempt from this identification exercise as a whole. In addition to taking the proportionality principle (Art. 4(2)) into account, competent authorities shall identify entities that are required to carry out TLPT based on the following considerations:

- "impact-related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector;"
- "possible financial stability concerns, including the systemic character of the financial entity at Union or national level;"
- and "specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved" (Art. 26(8)).

80 TLPT is defined as "a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems" (Art. 3, point (17)).

The identified financial entities shall conduct TLPT at a minimum every three years. Depending on a financial entity's "risk profile [...and] operational circumstances", competent authorities hold power to request "reduc[ing] or increas[ing] this frequency" (Art. 26(1)). Every TLPT test "shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions" (Art. 26(2)). Competent authorities shall validate the "precise scope" of a TLPT test based on a prior assessment of the financial entity, outlining "critical or important functions [which] need to be covered by the TLPT" (Art. 26(2)). Specific provisions apply in cases where ICT third-party service providers are involved. The Regulation leaves it at a Member State's discretion to "designate a single public authority in the financial sector to be responsible for TLPT-related matters in the financial sector at national level" (Art. 26(9)). The ESAs, "in agreement with the ECB", are tasked with further clarifying, for instance, the identification criteria through developing joint draft RTS. Article 27 lays out requirements for TLPT testers. For every TLPT testing, financial entities shall share a summarized version of their "relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with the requirements" with the responsible national authority (Art. 26(6)). As part of their digital operational resilience testing programme, all financial entities (except microenterprises) "shall establish procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed" (Art. 24(5)).

ICT Third-Party Risk Management

For purposes of managing ICT third-party risk, which DORA defines as "an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter" (Art. 3, point (18)), the Regulation specifies "key principles for [their] sound management" (Chapter five, section I) and establishes an "oversight framework of critical ICT third-party service providers" (Chapter five, section II).

As part of the principles, the Regulation stipulates that ICT third-party risk shall be managed by financial entities as part of their ICT risk management framework. In cases where financial entities have third-party contractual arrangements in place, they nevertheless "shall, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under this Regulation and applicable financial services law" (Art. 28(1), point (a)). The following table provides a non-exhaustive list of measures to be implemented by financial entities in this respect (for a comprehensive list, see Articles 28 and 29):

Measures by Financial Entities	
Art. 28(2) [1]	• "adopt, and regularly review, a strategy on ICT third-party risk" • "assessment of the overall risk profile of the financial entity and the scale and complexity of the business services" • Regular "review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions" by the financial entity's management board [1] Applicable for all financial entities, except for those financial entities to whom the simplified ICT risk management framework applies and microenterprises.
Art. 28(3)	• "maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers" • "report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided" • "inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important functions as well as when a function has become critical or important"
Art. 28(4)	• conduct ICT third-party risk-related assessments and due diligence "before entering into a contractual arrangement", further specified in Art. 292(1)
Art. 28(5)	• "only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards"
Art. 28(7)	• termination of contractual arrangements in specified scenarios
Art. 28(8)	• "put in place exit strategies" for "ICT services supporting critical or important functions"

Article 30 lists "key contractual provisions", for instance, "provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data" (Art. 30(2), point (c)), which shall be included in any contractual arrangement between financial entities and ICT third-party service providers (see Art. 30(2) and (3) for further elements of these provisions).

DORA also specifies an "oversight framework of critical ICT third-party service providers" (Chapter Five, Section Two). Such critical ICT third-party service providers shall be designated through the ESA's Joint Committee and "upon recommendation of the Oversight Forum".[81] The Regulation lists the following elements for consideration to determine whether an ICT third-party service provider providing ICT services is critical[82]:

81 When not listed, ICT third-party service providers may apply to either ESA to be considered as a critical ICT third-party service provider, ultimately to be decided by the ESA Joint Committee (Art. 31(11)).

- "the systemic impact on the stability, continuity or quality of the provision of financial services in the event that the relevant ICT third-party service provider would face a large scale operational failure to provide its services, taking into account the number of financial entities and the total value of assets of financial entities to which the relevant ICT third-party service provider provides services;"
- "the systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider;"
- "the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider;"
- and "the degree of substitutability of the ICT third-party service provider" (Art. 31(2)).

The ESA Joint Committee shall notify the respective ICT third-party service provider of their status as a critical ICT third-party service provider and the date from which onwards they "will effectively be subject to oversight activities" (Art. 31(5)). The period in between shall be no longer than one month. Upon notification of their designation as critical, the concerned ICT third-party service providers must inform the recipients of their services that are financial entities (Art. 31(5)). The ESA Joint Committee is tasked with publishing and maintaining a list of critical ICT third-party service providers within the EU (Art. 31(9)). The ESA Joint Committee shall only decide on respective designations once the Commission adopts a Delegated Act, further clarifying the criteria on whose basis such a designation takes place (Art. 31(6) and (7)).

In addition, the ESAs shall assign a 'Lead Overseer' amongst them for each of the critical ICT third-party service providers (Art. 31(1), point (b)). They shall cooperate and coordinate in the framework of a Joint Oversight Network (JON). Each Lead Overseer shall be responsible for the oversight of these providers and also acts as their "primary point of contact" (Art. 33(1)). The Lead Overseer is mandated to "assess whether each critical ICT third-party service provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk which it may pose to financial entities" (Art. 33(2)). On that basis, the "Lead Overseer shall adopt a clear, detailed and reasoned individual oversight plan describing the annual oversight objectives and the main oversight actions planned for each critical ICT third-party service provider" (Art. 33(4)) upon coordination with the JON, which is to be made available to the respective critical ICT third-party service provider. Article 33(3) further specifies the components of such an assessment, one of which is the existence of "ICT

82 DORA lists certain exceptions to the designation as critical ICT third-party service providers. In accordance, such a designation shall not apply to "(i) financial entities providing ICT services to other financial entities; (ii) ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) [Art. 127(2) specifies the ECB's basic tasks] of the Treaty on the Functioning of the European Union; (iii) ICT intra-group service providers; (iv) ICT third-party service providers providing ICT services solely in one Member State to financial entities that are only active in that Member State" (Art. 31(8)).

requirements to ensure, in particular, the security, availability, continuity, scalability and quality of services which the critical ICT third-party service provider provides to financial entities" (Art. 33(3), point (a)). If necessary, the Lead Overseers can request the ECB or ENISA "to provide technical advice, share hands-on experience or join specific [JON] coordination meetings" (Art. 34(3)). Member States' competent authorities and the Lead Overseer "shall, in a timely manner, mutually exchange all relevant information concerning critical ICT third-party service providers which is necessary for them to carry out their respective duties" (Art. 48(2)).

To ensure compliance, DORA entrusts the Lead Overseers with the following powers (Art. 35):

- requesting information (see further Article 37);
- carrying out general investigations and inspections (see further Article 38 and 39);
- issuing recommendations on issues covered by the assessment scope specified in Article 33(3) (see further Article 35(1), point (d)) [2];
- and "request[ing], after the completion of the oversight activities, reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service providers in relation to the[se] recommendations" (Art. 35(1), point (c)).

[2] Critical ICT third-party service providers have 60 days to "either notify the Lead Overseer of their intention to follow the recommendations or provide a reasoned explanation for not following such recommendations" (Art. 42(1)).

When engaging in related activities, the Lead Overseer shall "take due account of the framework established by [the NIS 2 Directive] and, where necessary, consult the relevant competent authorities designated or established in accordance with that Directive, in order to avoid duplication of technical and organisational measures that might apply to critical ICT third-party service providers pursuant to that Directive" (Art. 35(2), point (b)). In specified circumstances of non-compliance (see further Art. 35(6)-(11)), the Lead Overseer can impose a "periodic penalty payment" on critical ICT third-party service providers.[83] All of the "Lead Overseer's necessary expenditure in relation to the conduct of oversight" must be paid for by the critical ICT third-party service providers (Art. 42).[84]

83 The Regulation provides further that, in specified circumstances, Member States' competent authorities "may, as a measure of last resort, [...] take a decision [to be shared with Oversight Forum] requiring financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party service provider until the risks identified in the recommendations addressed to critical ICT third-party service providers have been addressed" (Art. 42(6)). The decision of competent authorities may also extend to "requir[ing] financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers" (Art. 42(6)). Article 42(8) lists elements for consideration by Member States' competent authorities when making such a decision, including, for instance, the "gravity and the duration of the non-compliance" (Art. 42(8), point (a)).

84 To this end, the Commission shall adopt a delegated act by 17 July further specifying "the amount of the fees and the way in

To support the Lead Overseer and the ESA Joint Committee in relation to ICT third-party risk, DORA establishes the Oversight Forum as a subcommittee within the ESA Joint Committee (Art. 32(1)).[85] The Lead Overseer shall also consult the Oversight Forum before exercising any of its granted powers (Art. 35(3)). As an additional support mechanism for the Lead Overseer in fulfilling its oversight tasks, DORA foresees assistance from a joint investigation team (see further Article 40). Every five years, the ESAs shall provide the European Parliament, Council, and Commission with a "joint confidential report [...] summarising the findings of relevant discussions [on fostering international cooperation on ICT third-party risk across different financial sectors, Art. 44(1)] held with the third countries' authorities" (Art. 44(2)).

Supervision and Enforcement

To monitor compliance with DORA, national competent authorities shall be equipped with "supervisory, investigatory and sanctioning powers" (Art. 50(1)), comprising, for instance, the ability to "carry out on-site inspections or investigations" (Art. 50(2), point (b)) and imposing "appropriate administrative penalties and remedial measures for breaches" (Art. 50(3)). As part of the latter, Member States shall ensure that their competent authorities are capable of, for example, "requir[ing] the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct" or "issu[ing] public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach" (Art. 50(4)). The Regulation further specifies circumstances to be taken into consideration when contemplating "type and level of an administrative penalty or remedial measure," such as "the extent to which the breach is intentional or results from negligence" or the "materiality, gravity and the duration of the breach" (Art. 51(2)). With respect to criminal penalties, the Regulation grants Member States some flexibility as it stipulates the possibility for not "lay[ing] down rules for administrative penalties or remedial measures for breaches that are subject to criminal penalties under their national law" (Art. 52).

Who	What	When	Post-Deadline	Legal Basis
Member	Notification of laws, regulations, and	17	Notification of	Art.

which they are to be paid" (Art. 43(3)).

85 The Oversight Forum comprises the ESAs chairpersons, Member State representatives and, as observers, "the Executive Directors of each ESA and one representative from the Commission, from the ESRB, from ECB and from ENISA" (Art. 32(4)). Inter alia, the Oversight Forum is tasked with "regularly discuss[ing] relevant developments on ICT risk and vulnerabilities and promot[ing] a consistent approach in the monitoring of ICT third-party risk at Union level" (Art. 32(1)).

States	administrative provisions laid down for implementing DORA Chapter VII → Commission and ESAs	January 2025	subsequent amendments "without undue delay"	53

Regulatory and Implementing Technical Standards

In many of its provisions, DORA provides for developing RTS or ITS for adoption by the Commission through delegated/implementing acts. An overview:

Who	What	When	Legal Basis
ESAs (through Joint Committee) in consultation with ENISA	Submission of draft regulatory technical standards on ICT risk management tools, methods, processes and policies → Commission	17 January 2024	Art. 15
ESAs (through Joint Committee) in consultation with ENISA	Submission of draft regulatory technical standards on simplified ICT risk management framework → Commission	17 January 2024	Art. 16
ESAs (through Joint Committee) in consultation with the ECB and ENISA	Submission of draft regulatory technical standards relating to the classification of ICT-related incidents and cyber threats → Commission	17 January 2024	Art. 18
ESAs (through Joint Committee) in consultation with ENISA and the ECB	Submission of draft regulatory and draft implementing technical standards relating to incident reporting content and templates → Commission	17 July 2024	Art. 20
ESAs (in agreement with ECB)	Submission of TLPT-related draft regulatory technical standards → Commission	17 July 2024	Art. 26(11)
ESAs (through Joint Committee)	Submission of draft implementing technical standards regarding a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers → Commission	17 January 2024	Art. 28(9)
ESAs (through	Submission of draft regulatory technical standards specifying the detailed content of the policy regarding	17 January	Art. 28(10)

Joint Committee)	contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers → Commission	2024	
ESAs (through Joint Committee)	Submission of draft regulatory technical standards on specific contractual arrangements "to determine and assess when subcontracting ICT services supporting critical or important functions" → Commission	17 July 2024	Art. 30(5)
ESAs (through Joint Committee)	Submission of draft regulatory technical standards relating to the on the conduct of oversight activities → Commission	17 July 2024	Art. 41

Review

Who	What	When	Legal Basis
Commission (upon consultation of ESAs and ESRB)	Review and submission of a report "accompanied, where appropriate, by a legislative proposal" (Art. 58 (1) points (a)-(e) further specify aspects to be considered for review) → Council and European Parliament	17 January 2028	Art. 58(1)
Commission (upon consultation of ESAs and the Committee of European Auditing Oversight Bodies)	Review and submission of a report "accompanied, where appropriate, by a legislative proposal, on the appropriateness of strengthened requirements for statutory auditors and audit firms as regards digital operational resilience" → Council and European Parliament	17 January 2026	Art. 58(3)

Digital Finance

— Regulation on Markets in Crypto-Assets

The ﷺ Regulation on markets in crypto-assets (MiCA) from 2023, inter alia, lays down "requirements for crypto-asset service providers"[86] (Art. 1(1)), of which some are also of cybersecurity relevance. For instance, in order for particular entities to receive the authorization to provide specific crypto-asset services, they must, among other aspects, share "technical documentation of the ICT systems and

86 A crypto-asset is a "digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology" (Art. 3, point (5)). An example for a crypto-asset service is the "provi[sion of] custody and administration of crypto-assets on behalf of clients" (Art. 3, point (16) also includes a full list of services considered as a crypto-asset service). In accordance, MiCA defines a crypto-asset service provider as "a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis" (Art. 3, point (15)).

security arrangements, and a description thereof in non-technical language" with the competent authority of their "home Member State" (Art. 60(7). The same applies to entities seeking authorization as a crypto-asset service provider (Art. 62(2)). Furthermore, the Regulation mandates crypto-asset service providers to "take all reasonable steps to ensure continuity and regularity in the performance of their crypto-asset services," also by ensuring compliance with the respective provisions set out in the DORA (Art. 68(7)). Additionally, a custody policy to be included in the framework of an agreement between clients and "crypto-asset service providers providing custody and administration of crypto-assets on behalf of [these] clients" shall "minimise the risk of a loss of clients' [...] access to the crypto-assets due to [...] cyber threats" (Art. 75(3)). By 31 December 2025, the European Securities and Markets Authority (ESMA), "in close cooperation with the [European Banking Authority] EBA," must share its first public "report [...] on the application of this Regulation and developments in markets in crypto-assets" with the Parliament and the Commission, to be continued on an annual basis (Art. 141). In its report, the ESMA shall also shed light on "the number and value of [...] hacks [as well as] the use of crypto-assets for payments related to ransomware attacks [and] cyber-attacks [...] reported in the Union" (Art. 141, point (k)). The Commission shall also include information on these numbers and values as part of its reports – an interim report by 30 June 2025 and a final report by 30 June 2027 – on the MiCA application, "accompanied, where appropriate, by a legislative proposal" (Art. 140). The Commission shall consult the EBA and ESMA when drafting these reports.

Export Controls

— Regulation Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items

In September 2021, the ﷺ Regulation setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (2021/821) entered into force. The Regulation defines dual-use items as "items, including software and technology, which can be used for both civil and military purposes" (Art. 2, point (a)). As a particular category of these dual-use items, the Regulation includes 'cyber-surveillance items,' which constitute "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems" (Art. 2, point (20)). As a general rule, all items contained in Annex I of the Regulation require prior authorization. Annex I specifies ten categories of items in detail, one titled telecommunications and

information security (category five). Concerning cyber-surveillance items not included in Annex I, authorization is required "if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law" (Art. 5(1)). Exporters themselves shall notify their respective competent authority, if they are "aware, according to [their] due diligence findings" that the proposed export of such items may "in their entirety or in part" serve any of the above mentioned use cases (Art. 5(2)). On that basis, Member States via their competent authorities "shall decide whether or not to make the export concerned subject to authorisation" (Art. 5(2)). To help exporters make such determinations, the Commission and Council are tasked with publishing a guideline to that effect.[87] The Regulation does not preclude Member States to "adopt or maintain national legislation imposing an authorisation requirement on the export of cyber-surveillance items not listed in Annex I if the exporter has grounds for suspecting that those items are or may be intended, in their entirety or in part, for any of the uses referred to" (Art. 5(3)). The Commission shall report annually on implementing this Regulation.[88] Concerning the export of cyber-surveillance items, the Commission is instructed to "include [...] the number of applications received by item, the issuing Member State and the destinations concerned by those applications, and on the decisions taken on those applications" (Art. 26(2)).

Investments and Financing

— Recovery and Resilience Facility

Regulation establishing the Recovery and Resilience Facility (2021/241) created the EU Recovery and Resilience Facility (RRF), which is implemented by the Commission and provides funding to Member States, inter alia, to "promote the Union's economic, social and territorial cohesion by improving the resilience, crisis preparedness, adjustment capacity and growth potential of the Member States, by mitigating the social and economic impact of [the COVID-19 crisis]" (Art. 4(1)). The Facility runs until the end of 2026. Investments supporting digital transformation are included as one of its six pillars. To be eligible for the Facility's financial support, Member States must share with the Commission a national recovery and resilience plan (Art. 17 and 18), in which they must allocate at least 20% of all

87 The guideline has not been published to date. A national non-binding guidance by the German Federal Office of Economics and Export Control (BAFA) can be found here.

88 Past annual reports on export controls can be found here.

measures to reaching digital objectives. The Commission shall report annually to the Council and Parliament on the implementation of the Facility, for instance, on its contribution to achieving the EU's digital targets (Art. 31). Among the many types of intervention foreseen under the Facility that may contribute to the objective of digital transformation, the following have a cybersecurity dimension (see further Annex VII):

Table 24: Overview of Cybersecurity-Related RRF Types of Intervention

Policy Field	Type of Intervention
E-government, digital public services (including digitalisation of transport) and local digital ecosystems	• "government ICT solutions, e-services, applications", "including use of advanced technologies (such as [...] cybersecurity [...]) for public services and decision making"
Digital capacities and deployment of advanced technologies	• the "development of highly specialised support services and facilities for public administrations and businesses" such as "national [...] Cyber Centres", and • the "development and deployment of cybersecurity technologies, measures and support facilities for public and private sector users"

The Recovery and Resilience Scoreboard offers the opportunity to track specific measures implemented by Member States in the framework of the Facility.[89]

— Regulation Establishing a Framework for the Screening of Foreign Direct Investments Into the Union

In April 2019, the ⬚ Regulation establishing a framework for the screening of foreign direct investments into the Union (2019/452) entered into force. The Regulation institutes "a framework for the screening by Member States of foreign direct investments [FDI] into the Union on the grounds of security or public order" (Art. 1(1)).[90] To determine whether a particular foreign direct investment in any sector "is likely to affect security or public order," the Regulation enumerates factors to be considered by the Member States or the Commission. Among others, it lists the "potential effects on [...] critical technologies and dual use items as defined in [the EU's export control regime][91], including [...] cybersecurity" (Art. 4(1), point

89 For instance, (a) Czechia uses funds provided by the Facility to ensure "full operation" of a cybersecurity competence center "providing consulting services to authorities," (b) Italy disposes of the Facility's financial support for the creation of their national cybersecurity agency and the "initial deployment of the national cybersecurity services," among other measures, and (c) Slovakia seeks "standardisation of technical and procedural cybersecurity solutions" through the adoption of a "national concept for informatisation of public administration" (see further European Commission: Milestones and targets).

90 A list of national screening mechanisms notified to the Commission can be found here.

(b)). Screening may also encompass, for instance, an assessment of the degree of direct or indirect control of foreign governments on the particular investor (Art. 4(2), point (a)). On an annual basis, Member States shall report to the Commission and the Commission to the Council and Parliament "aggregated information on foreign direct investments that took place in their territory," among other aspects, and on the status quo of the Regulation's implementation respectively (Art. 5). Under the Regulation, the Commission is competent to issue an opinion addressed to a specific Member State when it "considers that a foreign direct investment is likely to affect projects or programmes of Union interest on grounds of security or public order" (Art. 8). For instance, this relates to Horizon 2020, "including actions [...] relating to Key Enabling Technologies such as [...] cybersecurity" (Annex).

Payment Services

— Directive on Payment Services in the Internal Market

Directive 2015/2366 establishes rules for payment services "provided within the Union" in the framework of the internal market, which was amended by Directive 2022/2556 to ensure compliance with relevant provisions of DORA.[92] In order to apply for authorization as a payment institution, entities shall, with respect to cyber and IT security, provide their home Member State's competent authority with descriptions of

- "the applicant's [...] arrangements for the use of ICT services in accordance with" the DORA (Art. 5(1), point (e));
- "the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incident reporting mechanism which takes account of the notification obligations of the payment institution laid down in" DORA (Art. 5(1), point (f));
- "effective ICT business continuity policy and plans and ICT response and recovery plans and a procedure to regularly test and review the adequacy and efficiency of such plans in accordance with" DORA (Art. 5(1), point (h));
- and "security control and mitigation measures taken to adequately protect payment service users against the risks identified" (Art. 5(1), point (j)), "indicat[ing] how they ensure a high level of digital operational resilience in accordance with [DORA], in particular in relation to technical security and data protection, including for the software and ICT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations" (Art. 5(1)).

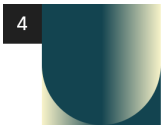
For entities subject to both DORA and Directive 2015/2366, only the DORA's

91 Cybersecurity-related aspects of the EU's export control regime are explained in Chapter 7.3.

92 Annex I includes a list of all the payment services within the scope of Directive 2015/2366 and Article 3 lists particular exclusions that do not fall within the Directive's scope.

incident reporting requirements apply as they supersede similar provisions from Directive 2015/2366 (recital (23), DORA).

Policy Area 4: Internal Security, Justice and Law Enforcement



The Treaty of the EU specifies that the EU "shall offer its citizens an area of freedom, security and justice [AFSJ] without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime" (Art. 3(2) TEU). This also involves judicial and police cooperation. The EU and Member States share competence in this area (Art. 4(2), point (j) TFEU).

Deep Dive: Critical Entities Resilience Directive (CER)

⬜⬜ Directive on the resilience of critical entities and repealing Council Directive 2008/114 (2022/2557)
Link: data.europa.eu/eli/dir/2022/2557/oj
Entry into force: 16 January 2023 Deadline for national transposition: 17 October 2024, measures to apply from 18 October 2024
Previous legislation: Repeals Directive 2008/114 from 18 October 2024 onwards
Subsequent documents of relevance: • November 2023: Commission Delegated Regulation supplementing Directive 2022/2557 of the European Parliament and of the Council by establishing a list of essential services (2023/2450)
Objective (Art. 1): • "ensuring that services which are essential for the maintenance of vital societal functions or economic activities [...] are provided in an unobstructed manner in the internal market" • "enhancing [critical entities'] resilience and ability to provide services" • "achieving a high level of resilience of critical entities in order to ensure the provision of essential services within the Union and to improve the functioning of the internal market"
Subject matter (Art. 1): "This Directive: • (a) lays down obligations on Member States to take specific measures aimed at ensuring

that services which are essential for the maintenance of vital societal functions or economic activities within the scope of Article 114 TFEU are provided in an unobstructed manner in the internal market [...];
- (b) lays down obligations for critical entities aimed at enhancing their resilience and ability to provide services [...] in the internal market;
- (c) establishes rules:
(i) on the supervision of critical entities;
(ii) on enforcement;
(iii) for the identification of critical entities of particular European significance and on advisory missions to assess the measures that such entities have put in place to meet their obligations [...];
- (d) establishes common procedures for cooperation and reporting on the application of this Directive;
- (e) lays down measures with a view to achieving a high level of resilience of critical entities in order to ensure the provision of essential services within the Union and to improve the functioning of the internal market."

Actors established/regulated by CER Directive:

- Critical Entities Resilience Group (CERG, Art. 19) [see further Chapter 13]

Deep Dive Structure
→ Scope
→ Competent Authorities, Single Points of Contact and Cooperation Between EU
→ Member States
→ National Frameworks on the Resilience of Critical Entities
→ Resilience Measures by Critical Entities
→ Review

Scope

Subject matter of the CER Directive forms critical entities, which are defined as a "public or private entity" (Art. 2, point (1)) that were identified by an EU Member State to fall under specified categories outlined in the CER Directive's Annex. The CER Directive notes the importance for its "implement[ation] in a coordinated manner" with the NIS 2 Directive "in light of the relationship between the physical security and cybersecurity of critical entities" (Art. 1(2). In terms of substance, the CER Directive specifies that it "shall not apply to matters covered by [the NIS 2] Directive [...], without prejudice to Article 8 of this Directive" (Art. 1(2)).[93]

Examples of the entities in scope of the CER Directive are (the sectors and subsectors also specified in the NIS 2 Directive for essential entities are assigned a ◇. Those for important entities are marked with a △. ○ indicates sectors which are covered by the CER Directive, but not by the NIS 2 Directive):

Table 25: Sectors, Subsectors and Categories of Entities in the Scope of the CER Directive

93 For reference, Article 8 of the CER Directive excludes critical entities in the banking, financial market infrastructure and digital infrastructure sectors from certain provisions.

"Sectors, subsectors and categories of entities" (Annex)	

◇ Energy	• ◇ Electricity
	  • for example, "transmission system operators"
	• ◇ District heating and cooling
	  • "operators of district heating or district cooling"
	• ◇ Oil
	  • for example, "operators of oil production, refining and treatment facilities, storage and transmission"
	• ◇ Gas
	  • for example, "supply undertakings"
	• ◇ Hydrogen
	  • "operators of hydrogen production, storage and transmission"

◇ Transport	• ◇ Air
	  • for example, "airport managing bodies"
	• ◇ Rail
	  • for example, "infrastructure managers"
	• ◇ Water
	  • for example, "managing bodies of ports"
	• ◇ Road
	  • for example, "road authorities"
	• ○ Public transport
	  • "public service operators"

◇ Banking	• "credit institutions"
◇ Financial market infrastructure	• for example, "operators of trading venues"
◇ Health	• for example, "entities manufacturing medical devices considered as critical during a public health emergency"
◇ Drinking water	• "suppliers and distributors of water intended for human consumption"
◇ Waste water	• "undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water"
◇ Digital infrastructure	• for example, "top-level-domain name registries"
◇ Public administration	• "public administration entities of central governments as defined by Member States in accordance with national law" [The Directive excludes from its scope "public administration entities that carry out their activities in the areas of national security, public security, defence or

	law enforcement, including the investigation, detection and prosecution of criminal offences" (Art. 1(6)). "Member States may [further] decide that Article[s] 11[-18, 21 and 22], in whole or in part, do not apply to specific critical entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities" (Art. 1(7)) as stipulated in the first sentence.]
△ Production, processing and distribution of food	• "food businesses"

EU Member States must "identify the critical entities for the sectors and subsectors set out in the annex" by 17 July 2026 (Art. 6(1)). The CER Directive lays out the following criteria for EU Member States to determine whether an entity is critical:

- (a) it provides "one or more essential services;"
- (b) it is located and operates from the territory of the EU Member States undertaking the determination;
- and (c) an "incident would have significant disruptive effects" (Art. 6(2)).

Whether an effect is deemed to be significantly disruptive, for instance, depends on

- the "number of users relying on the essential service provided;"
- the "geographic area that could be affected;"
- or the "entity's market share in the market for the essential service or essential services concerned" (see Article 7(1) for further criteria).

Upon consultation with the CERG, the Commission shall "adopt non-binding guidelines to facilitate the [significant disruptive effect] criteria" (Art. 7(3)). Additionally, together with EU Member States, the Commission shall compile "recommendations and non-binding guidelines to support Member States in identifying critical entities" (Art. 6(6)). Following the identification of critical entities, EU Member States must share additional information comprising

- "a list of essential services in that Member State where there are any additional essential services as compared to the list of essential services" included in the Commission's delegated act;
- "the number of critical entities identified for each sector and subsector set out in the Annex and for each essential service;"
- and, if applicable, "any thresholds applied to specify" the criteria for assessing whether an incident amounts to a significant disruptive effect (Art. 7(2))

with the Commission in due time. They must do so "whenever necessary and at least every four years" (Art. 7(2)).

EU Member States must inform identified critical entities within one month of their designation as such (Art. 6(3)). They must also inform critical entities of their obligations under Chapters 3 and 4, as well as the date from which they take effect for them.[94]

In terms of domestic information-sharing, EU Member States must ensure that the entities identified under the CER Directive are shared with the competent national authority under the NIS 2 Directive (Art. 6(4)) within a month of the identification.

Who	What	When	Post-Deadline	Legal Basis
Member States	Identification of the critical entities for the sectors and subsectors set out in the Annex	17 July 2026	Every four years, at least	Art. 6(1)
Member States	Submission a list of essential services, the number of critical entities identified for each sector and subsector set out in the Annex and for each essential service and any thresholds applied to specify the criteria for assessing whether an incident amounts to a significant disruptive effect → Commission	Whenever necessary, at least every four years	-	Art. 7(2)

In addition to critical entities, the CER Directive specifies a second set of actors that must meet particular obligations: "critical entities of particular European significance" (Chapter Four). An entity previously designated as critical is of such significance when it "provides the same or similar essential services to or in six or more Member States" (Art. 17(1)). The determination of critical entities of particular European significance is made by the Commission. The Commission does so upon receipt of respective information by EU Member States, followed by consultations with the relevant national competent authorities in which the critical entity operates and the critical entity itself. The critical entity to which these conditions apply is only finally designated as such once the Commission, via a competent authority, notified the critical entity in question of its designation. The entity will be bound by the obligations of the CER Directive's Chapter Four (Art. 17 and 18) from the day following the notification.

The CER Directive also foresees the possibility for the Commission to organize so-called 'advisory missions' "to assess the measures that [a critical entity of particular European significance[95]] has put in place to meet its obligations under

94 Obligations contained in Articles 11-18, 21 and 22 do not apply to critical entities that Member States have identified within the banking, financial market infrastructure, and digital infrastructure sectors (Art. 8).

Chapter III" (Art. 18(1)).[96] Such advisory missions can be requested by one or more Member States or be conducted at the Commission's initiative. The CERG shall be notified when an advisory mission is carried out (Art. 18(10)). The team of an advisory mission "consist[s] of experts from the Member State in which the critical entity of particular European significance is located, experts from the Member States to or in which the essential service is provided, and Commission representatives" (Art. 18 (5)). Any resulting costs in relation to participating in advisory missions will be covered by the Commission (Art. 18(5)). The CER Directive further specifies that "Member States shall ensure that critical entities of particular European significance provide advisory missions with access to information, systems and facilities relating to the provision of their essential services necessary" (Art. 18(5)). Findings of any advisory mission shall be shared with the "Commission, to the Member State that has identified a critical entity of particular European significance as a critical entity [...], to the Member States to or in which the essential service is provided and to the critical entity concerned within three months of [its] conclusion" (Art. 18(4)), which, in turn, are tasked, inter alia, with analyzing and reviewing the report with respect to the critical entities compliance. In terms of information-sharing, the "Member State in which the advisory mission took place and the Commission shall also inform the Critical Entities Resilience Group of the main findings of the advisory mission and the lessons learned" (Art. 18(10)).

Competent Authorities, Single Points of Contact and Cooperation Between EU Member States

To apply and, if required, enforce the Directive, EU Member States must "designate or establish one or more competent authorities" and a "single point of contact [SPOC] to exercise a liaison function" with other EU Member States and the CERG (Art. 9). Member States must notify the Commission within three months of their designation. The Commission is entrusted with "mak[ing] a list of the single points of contact publicly available" (Art. 9(8)). For critical entities in the banking and financial market infrastructure sectors, the competent authorities designated nationally in the context of the CER Directive should "in principle" be the same, as those designated under DORA (Art. 9(1)). Similarly, for the digital infrastructure sector, it should be the competent authority also designated to this effect under the NIS 2 Directive (Art. 9(1)). In any case, designated national competent authorities

95 In addition to critical entities of particular European significance, the CER Directive also provides for advisory missions with respect to critical entities "at the request of the Member State that has identified the critical entity and with the agreement of the critical entity concerned" (see further Art. 13(4)).

96 The Directive tasks the Commission to work towards adopting an "implementing act laying down rules on the procedural arrangements for requests to organise advisory missions, for handling such requests, for the conduct and reports of advisory missions and for handling the communication of the Commission's opinion [...] and of the measures taken" (Art. 18(6)).

under the NIS 2 and CER Directives shall "cooperate[...] and exchange[...] information [...] on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities" (Art. 9(6)). Competent authorities are also instructed to "exchange[...] information and good practices" with critical entities under their jurisdiction (Art. 10(2)).

To guarantee the CER Directive's application "in a consistent manner," Member States are supposed to consult each other, especially in cases where critical entities "use critical infrastructure which is physically connected between two or more Member States," "are part of corporate structures that are connected with, or linked to, critical entities in other Member States," and/or "have been identified as critical entities in one Member State and provide essential services to or in other Member States" (Art. 11(1) points (a)-(c)). The Commission is delegated to "facilitate information exchange among Member States and experts across the Union" (Art. 20(1)).

National Frameworks on the Resilience of Critical Entities

In transposing the CER Directive, EU Member States are required to establish a national framework for the resilience of critical entities. The CER Directive defines resilience as a "critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident" (Art. 2, point (2)). In addition to identifying critical entities, this framework comprises adopting a national **strategy** (Art. 4) and conducting a **risk assessment** (Art. 5). The strategy shall contain, among other elements,

- a governance framework to achieve [...] strategic objectives and priorities;"
- describe "measures necessary to enhance the overall resilience of critical entities;"
- and outline "the process supporting critical entities" (Art. 4(2)).

To ensure consistent implementation with the NIS 2 Directive, national strategies should also include a "policy framework for coordination" at the domestic level between the authorities respectively designated as competent to ensure effective supervision and the sharing of information (Art. 4(2), point (g)). The CER Directive states that the strategy development, for both initial and updated versions, should be "to the extent practically possible, open to relevant stakeholders" (Art. 4(2)).

In addition to the strategy, and based on a delegated act adopted by the Commission in July 2023 proposing a "non-exhaustive list of essential services", EU Member States must carry out a risk assessment, accounting for "the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats or other antagonistic threats, including terrorist offences" (Art. 5(1)). In particular, the risk

assesment shall consider interdependencies between sectors and the "impact that a significant disruption in one sector may have on other sectors" (Art. 5(2), point (c)). "Relevant elements" of these risk assessments should be shared by Member States with the identified critical entities, for instance, to support the carrying out of critical entity risk assessments (Art. 5(3)).

EU Member States must communicate their strategy and risk assessment findings with the Commission at the latest three months after their adoption/completion (Art. 4(3) and Art. 5(4)). Concerning the later provision of information, the Commission is tasked with compiling a "voluntary common reporting template" together with EU Member States (Art. 5(5)). EU Member States must update the strategy, risk assessment, as well as the identification of critical entities at least every four years (Art. 4(1) and Art. 5(1)).

Who	What	When	Post-Deadline	Legal Basis
Member States	Adoption of a strategy for enhancing the resilience of critical entities	17 January 2026	Update at least every four years	Art. 4(1)
Member States	Conduct of risk assessment	17 January 2026	Update at least every four years	Art. 5(1)
Commission	Provision of a summary report of the information provided by the Member States on their strategies and risk assessments → CERG	17 January 2027	Update at least every four years	Art. 19(7)

Resilience Measures by Critical Entities

Critical entities must carry out

- a **risk assessment** to "assess all relevant risks that could disrupt the provision of their essential services" (Art. 12);
- "take appropriate and proportionate technical, security and organisational **measures** to ensure their resilience" (Art. 13);
- and **notify** competent authorities of "**incidents** that significantly disrupt or have the potential to significantly disrupt the provision of essential services" (Art. 15).

These obligations apply to critical entities ten months after they are notified of designation as critical entities (Art. 6(3)).[97] Obligations contained in Articles 11-18, 21 and 22 do not apply to critical entities that Member States have identified within

97 Entities in the banking, financial market infrastructure, and digital infrastructure sectors are exempt from these obligations and Chapter Four "unless national measures provide otherwise" (Art. 6(3)).

the banking, financial market infrastructure, and digital infrastructure sectors (Art. 8).

Once notified by an EU Member State as a critical entity falling under the CER Directive, entities have nine months "to assess all relevant risks that could disrupt the provision of their essential services" as part of their own **risk assessment** (Art. 12(1)). The risk assessment shall include an evaluation as to what degree other sectors, as specified in the annex, "depend on the [provision of its] essential service" and examine "the extent to which [... it] depends on essential services provided by other entities" (Art. 12(2)).

Resilience measures by critical entities shall, inter alia, support

- "prevent[ing] incidents from occurring;"
- "ensur[ing] adequate physical protection of [...] premises and critical infrastructure;"
- "respond[ing] to, resist[ing] and mitigat[ing] the consequences of incidents;"
- as well as "recover[ing] from incidents" (Art. 13(1)) [1].

[1] Entities in the banking, financial market infrastructure, and digital infrastructure sectors are exempt from these obligations and Chapter Four "unless national measures provide otherwise" (Art. 6(3)).

To account for the application of these measures, critical entities must have and enforce a "resilience plan or equivalent document" (Art. 13(2)). The entities must also assign a liaison officer as a point of contact for communication with the national competent authority (Art. 13(3)). The Commission is instructed to consult with the CERG on the development "non-binding guidelines to further specify the technical, security and organisational measures that may be taken" by critical entities to comply with the obligations under this provision (Art. 13(5)).

The CER Directive also establishes **reporting obligations** for critical entities to notify when they become subject to "incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services" (Art. 15(1)).

To determine the significance of a disruption, the directive lists three elements for consideration:

- "the **number** and proportion **of users affected** by the disruption;"
- "the **duration** of the disruption;"
- and "the **geographical area** affected by the disruption" (Art. 15(1)).

In notifying such an incident to the competent authority, the following specific timelines apply for critical entities:

Table 26: Overview of the CER Directive's Incident Reporting Obligations

I. Action to be taken by critical entity	
(a) Without undue delay, within >24h after "becoming aware" of an incident "unless operationally unable to do so"	(b) Where relevant, no later than one month thereafter
Submission of an initial notification (Art. 15(1))	Submission of a detailed report (Art. 15(1))

II. Action to be taken by competent authority/SPOC	
(a) As soon as possible upon receipt of notification	(b) No specified timeline
• Provision of "follow-up information, including information that could support that critical entity's effective response to the incident in question" (Art. 15(4))	• → Notification of SPOCs of other Member State when "incident has or might have a significant impact on critical entities and the continuity of the provision of essential services to or in one or more other Member States" (Art. 15(1)) • → Notification of Commission when incident "has or might have a significant impact on the continuity of the provision of essential services to or in six or more Member States" (Art. 15(3)) • → Communication of the incident with the public when "it would be in the public interest to do so" (Art. 15(4))

The SPOC must "submit a summary report to the Commission and the CERG [...] on the notifications they have received, [...] the nature of notified incidents and the actions taken in accordance with Article 15(3)"[98] (Art. 9(3)). For these summary reports, the Commission shall, together with the CERG, "develop a common reporting template" for voluntary use by competent authorities (Art. 9(3)).

As part of Member States' supervision of critical entities' compliance with their obligations under the CER Directive, competent authorities shall be equipped with the "powers and means to

- (a) conduct on-site inspections of the critical infrastructure [...] and off-site supervision of measures taken by critical entities in accordance with Article 13, and
- (b) conduct or order audits in respect of critical entities" (Art. 21(1)).

National competent authorities under the CER Directive shall inform their NIS 2

98 Art. 15(3) stipulates that national SPOCs shall inform each other when an "incident has or might have a significant impact on critical entities and the continuity of the provision of essential services to or in one or more other Member States".

counterparts when "assesses[ing] the compliance of a critical entity pursuant to this Article" (Art. 21(5)).

To ensure the Directive's application, Member States may require critical entities to provide information and evidence documenting their compliance or "order [them] to take the necessary and proportionate measures to remedy any identified infringement of this Directive" (Art. 21(3)).

Who	What	When	Post-Deadline	Legal Basis
Member States	Notification of the rules on penalties applicable to infringements of the national measures adopted pursuant to this Directive → Commission	17 October 2024	Notify without delay if any amendment takes place	Art. 22

In addition to supervising the application of the CER Directive by critical entities, Member States also shall commit to supporting the latter in this respect. Such support may involve providing guidance resources, advice, training up until financial assistance[99] (Art. 10(1)). Amongst critical entities, Member States shall also "facilitate voluntary information sharing [...] in relation to matters covered by [the CER] Directive" (Art. 10(3)). The CER Directive tasks the Commission with complementing Member States' supportive efforts through the development of "best practices, guidance materials and methodologies, and cross-border training activities and exercises" (Art. 20(2)). Further, the Directive instructs the Commission to "prepare a Union-level overview of cross-border and cross-sectoral risks to the provision of essential services" (Art. 20(1)).

Who	What	When	Post-Deadline	Legal Basis
Member States SPOC	Submission of a summary report on received notifications → Commission and CERG	17 July 2028	Biannually thereafter	Art. 9(3)
Critical Entities	Conduct of risk assessment	Within nine months after being notified of designation as critical entity	Update at least every four years	Art. 12(1)

Review

99 With regard to financial assistance, the Directive tasks the "Commission [to] inform Member States about financial resources at Union level available to Member States for enhancing the resilience of critical entities" (Art. 20(3)).

Who	What	When	Legal Basis
Commission	Submission of a report on Member States' compliance with the CER Directive → European Parliament and Council	17 July 2027	Art. 25
Commission	Periodic review report on the functioning of the CER Directive → European Parliament and Council	First report by 17 June 2029	Art. 25

Cybercrime

— Directive on Attacks Against Information Systems

In September 2013, the ﷺ Directive on attacks against information systems (2013/40) entered into force, which "establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems" (Art. 1). Moreover, it seeks to "facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities" (Art. 1). The Directive includes provisions specifying the illegal access to information systems (Art. 3), illegal system interference (Art. 4), illegal data interference (Art. 5), and illegal interception (Art. 6) as criminal offenses. For these purposes, the Directive defines information systems as "a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance" (Art. 2, point (a)) and data as "a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function" (Art. 2, point (b)). They are considered a criminal offense, "at least for cases which are not minor," when the following circumstances are applicable:

Table 27: Punishable Offenses under Directive 2013/40

Punishable Offense	Definition
Art. 4: illegal access to information systems	"the [intentional] access without right [1], to the whole or to any part of an information system, [...] where committed by infringing a security measure" [1] 'Without right' is defined as "conduct [...] including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law" (Art. 2, point (d)).
Art. 5:	"seriously hindering or interrupting the functioning of an information system by

illegal system interference	inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right"
Art. 6: illegal data interference	"deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right"
Art. 7: illegal interception	"intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right"

Moreover, "the intentional production, sale, procurement for use, import, distribution or otherwise making available, of [...] [a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6, or a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed] without right and with the intention that it be used to commit any of the offences" (Art. 7) may be punishable as a criminal offence. Also, the "incitement, or aiding and abetting" in committing any of these offences can constitute a criminal offence (Art. 8). Already the "attempt to commit" illegal system or data interference (Art. 4 and 5) may be "punishable as a criminal offence" (Art. 9(2)). Member States "shall take the necessary measures" to ensure the punishability of these offences by means of "effective, proportionate and dissuasive criminal penalties" (Art. 9(1)). Under the Directive, Member States can also hold legal persons liable (Art. 10) and sanction them via "effective, proportionate and dissuasive sanctions" of a criminal or non-criminal nature (Art. 11). The Directive specifies particular penalties for the specific criminal offences (Art. 9). For instance, a penalty of a higher degree (maximum term of at least five years) shall be applied when illegal system or data interference are "committed within the framework of a criminal organisation," "cause serious damage," or "are committed against a critical infrastructure information system" (Art. 9(4)). A Member State can establish jurisdiction over a specific offence when the offence has either been committed "in whole or in part within their territory" or "by one of their nationals" (Art. 12(1)), further specified in Art. 12(2) and (3). To comply with their obligations under the Directive, Member States must also designate an "operational national point of contact" and use the network of operational points of contact for purposes of offense-related information-sharing (Art. 13(1)). Member States shall also ensure that they have procedures in place for responding to "urgent requests for assistance" (Art. 13(1) in a timely fashion.

IT Systems of the Area of Freedom, Security and Justice

Over the past years, a multitude of IT systems was set up to support the AFSJ. ﷺ Regulation 2018/1726 specifies the mandate and the activities to be undertaken by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). For instance, eu-LISA performs cybersecurity-related tasks in relation to the following systems[100]:

— Joint Investigation Teams Collaboration Platform

The ﷺ Regulation establishing a collaboration platform to support the functioning of joint investigation teams (2023/969) institutes a voluntary Joint Investigation Teams (JITs) collaboration platform in an effort "to facilitate the cooperation of competent authorities participating in joint investigation teams" (Art. 1, point (b)), for instance, in the area of combating cybercrime. In implementing and managing the collaboration platform, eu-LISA "shall take the necessary technical and organisational measures to ensure a high level of cybersecurity of the JITs collaboration platform and the information security of data within the JITs collaboration platform, in particular in order to ensure the confidentiality and integrity of operational and non-operational data stored in the centralised information system" (Art. 19(1)). To this end, eu-LISA is tasked with developing both a "security plan and a business continuity and disaster recovery plan" and concluding a "working arrangement" with CERT-EU (Art. 19(3)). The Commission shall further specify security requirements through implementing acts (Art. 6, point (b)).

— e-Justice Communication via Online Data Exchange (e-CODEX)

The ﷺ Regulation on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (2022/850) establishes a "computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters,"

100 Other AFSJ IT systems are the Schengen Information System (SIS II), the Visa Information System (VIS), the European Asylum Dactyloscopy Database (Eurodac), the Entry/Exit System (EES), DubliNet, and the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN).

the so-called e-CODEX system. eu-LISA is "responsible for maintaining a high level of security when carrying out its tasks, including the security of the hardware and software IT infrastructure" (Art. 11(1)). Among other measures, this includes the adoption of a security plan and due regard to the security by design principle. The responsibility for the secure operation of e-CODEX access points rests with their respective operating entities. Furthermore, they shall, "without delay," notify eu-LISA, and, if applicable, Member States/EUIBAs of any security incident (Art. 11(4)). Either upon detection of vulnerabilities/incidents or upon notification of such by others, "eu-LISA shall analyse the security incident and inform the entities operating authorised e-CODEX access points impacted by it [...] without delay" (Art. 11(5)). In addition, eu-LISA shall "develop security rules and guidance regarding authorised e-CODEX access points," whose compliance must be demonstrated by the entities operating them (Art. 11(6)). On an annual basis, both Member States and the Commission must share with eu-LISA the "number and type of incidents encountered by entities operating authorised e-CODEX access points [...] which have impacted the security of the e-CODEX system," either "for the connected systems within their territory" (Member States) or when the operating entity is an EUIBA (Commission) (Art. 15(1), point (b) and (2), point (b)).[101] eu-LISA shall report to the Commission every two years on the e-CODEX's security, among other factors (Art. 16(1)).

— European Travel and Information and Authorisation System (ETIAS)

In October 2018, the ⬚⬚ Regulation establishing a European Travel Information and Authorisation System (ETIAS) (2018/1240) entered into force. ETIAS allows determining "whether the presence of [...] third-country nationals [who are exempt from having a visa when crossing the external borders] in the territory of the Member States would pose a security, illegal immigration or high epidemic risk" (Art. 1(1)). Among other tasks, eu-LISA "shall take the necessary measures to ensure the security of the ETIAS Information System" (Art. 59(2)). eu-LISA, the ETIAS Central Unit (hosted within the European Border and Coast Guard Agency) and Member State competent authorities (the ETIAS National Units) are tasked to implement specific security measures, for instance, to "deny unauthorised persons access to the secure web service" (Art. 59(3)). The Regulation also imposes notification requirements for Member States, eu-LISA, and Europol in instances of security incidents, which are defined as "any event that has or may have an impact on the security of ETIAS and may cause damage or loss to the data stored in

101 This notification requirement is applicable to them, "unless an equivalent notification procedure applies under another Union legal act" (Art. 15).

ETIAS" (Art. 60).

Judicial and Police Cooperation

— Internal Security Fund

Until 2027, ⁂ Regulation 2021/1149 from July 2021 provides the legal basis for establishing the EU's Internal Security Fund (ISF). The ISF aims to support "a high level of security in the Union, in particular by preventing and combating [...] cybercrime, by assisting and protecting victims of crime, as well as by preparing for, protecting against and effectively managing security-related incidents, risks and crises" (Art. 3(1)). Financial support of the Fund can, for instance, be used for increasing "cooperation with the private sector, for example in the fight against cybercrime, in order to build trust and improve coordination, contingency planning and the exchange and dissemination of information and best practices" and to contribute to "projects which aim to prevent and fight cybercrime, in particular child sexual exploitation online, and crimes where the internet is the primary platform for evidence collection" (Annex II and IV). Implementing measures under the ISF can also encompass activities supporting operational actions in line with the EU Policy Cycle/European Multidisciplinary Platform Against Criminal Threats (EMPACT). Beneficiaries of ISF funding can, for instance, be Member State entities in the areas of police or law enforcement, but also "legal entities created under Union law or any international organisation relevant for the purposes of the Fund" (Art. 19). Additionally, ISF funding may also – upon the Commission's initiative – be used to "finance Union actions related to the objectives of the Fund" (Art. 20).

Council Conclusions

— Council Conclusions on the Permanent Continuation of the EU Policy Cycle for Organised and Serious International Crime: EMPACT 2022+

In February 2021, the Council decided to extend the mandate of the EU Policy Cycle for organised and serious international crime – now renamed European Multidisciplinary Platform Against Criminal Threats (EMPACT) – permanently via its ⁂ Council conclusions on the permanent continuation of the EU Policy Cycle for organised and serious international crime: EMPACT 2022+. EMPACT serves as an "instrument for structured multidisciplinary cooperation to fight organised and serious international crime driven by the Member States and supported by EU institutions, bodies and agencies in line with their respective mandates" (p. 6),

operating on four-year-long cycles. EMPACT, inter alia, includes the following elements:

- "policy development on the basis of a European Union Serious and Organised Crime Threat Assessment (EU SOCTA)" (p. 6);
- an interim report by Europol (in cooperation with Member States and relevant EU agencies) on "new, changing or emerging threats" to be shared with the Council (p. 6);
- a "General Multi-Annual Strategic Plan (G-MASP) containing Common Horizontal Strategic Goals (CHSGs)", complemented by biennial operational action plans (OAPs) for each "prioritised threat" (p. 6);
- and an "independent evaluation" (p. 6) following each EMPACT cycle (see further EMPACT Terms of Reference).

As part of the current cycle from 2022 to 2025, "cyber attacks," i.e. the "target[ing of] the criminal offenders orchestrating cyber-attacks, particularly those offering specialised criminal services online," are considered as one of the cycle's ten priorities (see further p. 6, ﷺ Council conclusions setting the EU's priorities for the fight against serious and organised crime for EMPACT 2022-2025). Specific actions and objectives in relation to this priority are outlined in the dedicated biennial EMPACT OAP on "cyber attacks". The Standing Committee on Operational Cooperation on Internal Security (COSI) is responsible for "policy setting, implementation and monitoring" (p. 16, 8975/23) in relation to EMPACT and the implementation of the EMPACT's OAPs. Every Member State shall designate a national EMPACT coordinator (NEC) who is in charge of the EMPACT's implementation within the respective Member State (for specific tasks, see further EMPACT Terms of Reference). All NECs meet every six months. The EUIBAs also appoint an EMPACT coordinator. Europol supports EMPACT by providing the EMPACT Support Team (EST), among other tasks.

— Council Conclusions on Improving Criminal Justice in Cyberspace

In June 2016, the Council adopted ﷺ Conclusions on improving criminal justice in cyberspace. Via these Conclusions, EU Member States agreed that "the development of a common EU approach on improving criminal justice in cyberspace should be treated as a matter of priority" (p. 3) and formulated "guidelines [...] to improve the enforcement of the rule of law in cyberspace and obtaining e-evidence in criminal proceedings" (p. 3). Among other components, these guidelines emphasize the importance of full respect for "data protection and fundamental rights frameworks," consider "enhancing cooperation with service providers or any other comparable solution that allows for quick disclosure of data," stress the need for "accelerated and streamlined" "Mutual Legal Assistance (MLA) procedures related to electronic data," and call for the efficient use of "mutual

recognition procedures [...] of e-evidence" (all p. 3). To this end, the Conclusions, inter alia, request the Commission (in coordination with various actors respectively) to

- develop "a common framework for cooperation with service providers for the purpose of obtaining specific categories of data" (p. 3);
- draft "recommendations on how to adapt, where appropriate, existing standardised forms and procedures to request the securing and obtaining of e-evidence" (p. 4);
- set up "a secure online portal for electronic requests and responses concerning e-evidence and the corresponding procedures, [...] as well as for their tracking and tracing" (p. 4);
- provide "guidelines and dedicated training modules [...] on the efficient use of the current frameworks that are used for securing and obtaining e-evidence" (p. 4);
- and "explore possibilities for a common EU approach on enforcement jurisdiction in cyberspace in situations[1] where existing frameworks are not sufficient" (p. 5).

[1] The Conclusions provide the following examples for such situations: "situations where a number of information systems are used simultaneously in multiple jurisdictions to commit one single crime, situations where relevant e-evidence moves between jurisdictions in short fractions of time, or where sophisticated methods are used to conceal the location of e-evidence or the criminal activity" (p. 5).

Member States, on the other hand, are requested to take the following actions, among others:

- ratification and full implementation of the Budapest Convention;
- "ensur[ing] sufficient capacity for handling MLA requests related to investigations in cyberspace and to provide relevant training to the staff on how to handle such requests;"
- and "optimi[zing] the use of the existing 24/7 points of contact and to increase the use of joint investigation teams" (all p. 4).

Policy Area 5: Energy, Transport and Health Policy

Energy, transport, and "common safety concerns in public health matters" are fields of shared competence between the EU and Member States (Art. 4(2), points (g), (i) and (k) TFEU).

- **Energy:** The EU has the mandate to work toward "ensur[ing] the functioning of the energy market," "ensur[ing] security of energy supply in the Union," "promot[ing] energy efficiency and energy saving and the development of new and renewable forms of energy" and "promot[ing] the interconnection of energy networks" (Art. 194 TFEU).
- **Transport:** The EU pursues a "common transport policy," for instance, by setting "common rules applicable to international transport to or from the territory of a Member State or passing across the territory of one or more Member States," specifying "the conditions under which non-resident carriers may operate transport services within a Member State," or adopting "measures to improve transport safety" (Art. 90 and 91 TFEU).
- **Public health:** The EU works to "complement national policies, to ensure health protection in all EU policies and to work towards a stronger Health Union" (European Commission: Public Health. Overview).
- In particular, the EU "shall [...] encourage cooperation between the Member States to improve the complementarity of their health services in cross-border areas" (Art. 168(2) TFEU).

The NIS 2 Directive, inter alia, includes the (i) energy sector, together with its subsectors electricity, district heating and cooling, oil, gas, and hydrogen, (ii) the health sector, and (iii) the transport sector, together with its subsectors air, rail, water and road, as sectors of high criticality. Also cybersecurity-related obligations derived from the CER Directive apply to particular entities in the energy, health, and transport sector.

Energy

— Directive on Energy Efficiency

The ⬚⬚ Directive on energy efficiency (2023) establishes "a common framework of measures to promote energy efficiency within the Union in order to ensure that the Union's targets on energy efficiency are met and enables further energy efficiency improvements" (Art. 1(1)), which also addresses cybersecurity considerations. Specifically, regarding the billing and consumption information for heating, cooling and domestic hot water, Member States shall "promote cybersecurity and ensure the privacy and data protection of final users in accordance with applicable Union law" (Art. 18(2) (d)). By 11 October 2025, the Directive will repeal ⬚⬚ Directive 2018/2002, which includes the same cybersecurity-related considerations.

— Directive on Common Rules for the Internal Market for Electricity

In June 2019, the European Parliament and the Council adopted the ⬚⬚ Directive on common rules for the internal market for electricity, establishing "rules for the

generation, transmission, distribution, energy storage and supply of electricity" (Art. 1). For instance, in relation to the deployment of smart metering systems, the Directive requires Member States to have "due regard of the best available techniques for ensuring the highest level of cybersecurity protection while bearing in mind the costs and the principle of proportionality" (Art. 20). Furthermore, the Directive designates that each transmission system operator[102] must maintain responsibility for "data management, including the development of data management systems, cybersecurity and data protection" (Art. 40).

— Regulation on the Internal Market for Electricity

The ⧉⧉ Regulation on the internal market for electricity (2019) sets out "fundamental principles for well-functioning, integrated electricity markets" (Art. 1, point (b)), inter alia, in an effort to ensure the EU's competitiveness in the global market. The Regulation establishes the European Network of Transmission System Operators for Electricity (ENTSO-E)[103] and an entity of distribution system operators in the Union (EU DSO entity)[104]. Tasks of both include the promotion of cybersecurity and the engagement with "relevant authorities and regulated entities" in this regard (Art. 30(1), point (n) and Art. 55 (1), point (e)). The Regulation is complemented by ⧉⧉ Commission Implementing Decision 2020/1479, which established a new priority list for harmonizing electricity rules. The Commission's priority lists identify the areas to be included in the development of network codes[105], which are established every three years for the electricity sector and every year for the gas sector. The list for 2020 to 2023 includes "sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management" (Art. 1(a)), [106] which is in line with the provisions set out in the ⧉⧉ Regulation on risk-preparedness in the electricity sector (2019). The recital of the latter Regulation also further stresses that it complements the NIS Directive "by ensuring that cyber-incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans" (recital (7),

102 A transmission system operator is defined as "a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity" (Art. 2, point (35)).

103 The ENTSO for Electricity is a platform for cooperation among transmission system operators at Union level. It is tasked with promoting "the completion and functioning of the internal market for electricity and cross-zonal trade and to ensure the optimal management, coordinated operation and sound technical evolution of the European electricity transmission network" (Art. 28(1)).

104 The EU DSO entity is a platform for cooperation among distribution system operators at Union level. It is tasked with promoting "the completion and functioning of the internal market for electricity" and "optimal management and a coordinated operation of distribution and transmission systems" (Art. 52(1)).

105 Network codes are rules that "govern the work of [energy network] operators and determine how access to electricity is given to users across the EU." (European Commission: Electricity network codes and guidelines).

106 These efforts culminated in the Commission Delegated Regulation 2024/1366 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, which entered into force in June 2023.

Regulation 2019/941).

— Commission Recommendation on Cybersecurity in the Energy Sector

The ﷺ Commission Recommendation 2019/553 on cybersecurity in the energy sector identifies key cybersecurity challenges within the energy sector and offers guidance on corresponding cybersecurity preparedness measures. Member States are encouraged to "ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures" (p. 3f.) across different facets of the energy sector. Specifically, as part of these measures, the Commission recommends that Member States make sure that energy network operators:

- adhere to the latest security standards for new installations and "consider complementary physical security measures" (p. 3);
- adopt international cybersecurity standards and relevant technical standards for "secure real-time communication" (p. 3);
- set up a "communication framework with all key stakeholders to share early warning signs and cooperate on crisis management" (p. 3);
- "establish design criteria and an architecture for a resilient grid" (p. 4) capable of preventing cascading effects [1];
- "establish an automated monitoring and analysis capability" (p. 4) for security-events (e.g. unsuccessful log-in attempts) across both "legacy and [I]nternet of Things [IoT] environments" (p. 4) and operators shall conduct regular "cybersecurity risk analysis on all legacy installations" (p. 4);
- and formulate tenders in a way that prioritizes cybersecurity considerations by requesting information on "security features" (p. 4), compliance with existing standards, and "continuous alerting, patching, and mitigation proposals" (p. 4) for discovered vulnerabilities by potential vendors.
  [1] An example are potential cascading effects in the energy sector, where a malicious cyber operation on one part of the system could lead to widespread disruptions in other parts of that system due to the strong interconnection of electricity grids and gas pipelines across Europe (see further pp. 3-4 Commission Recommendation 2019/553).

Member States should report on the implementation of their cybersecurity preparedness measures to the Commission through the NIS Cooperation Group within 12 months of their adoption and every two years after that (p. 5). Subsequently, the Commission will assess the reported information in consultation with Member States and relevant stakeholders to determine whether further measures are necessary (p. 5).

Civil Aviation

— Regulation on Common Rules in the Field of Civil Aviation and Establishing a European Union Aviation Safety Agency

�� Regulation 2018/1139 provides legally binding, comprehensive rules governing civil aviation across the EU. It is directly applicable in all Member States and seeks to "establish and maintain a high uniform level of civil aviation safety in the Union" (Art. 1(1)). It also establishes the European Union Aviation Safety Agency (EASA)[107] with the purpose of "ensuring the proper functioning and development of civil aviation in the Union" (Art. 75(2)). Concerning cyber and information security, the Regulation stipulates that the Commission, EASA, and Member States "shall cooperate on security matters related to civil aviation, including cyber security" (Art. 88(1)). Furthermore, aircrafts must also be designed to withstand "reasonably probable threats, including information security threats" (Annex II) and are "subject to certification" (Art. 14) by the EASA.[108]

The Commission subsequently adopted various implementing and delegated acts to achieve the objectives set out in the Regulation. The following address cyber and information security in the civil aviation sector:

-   Commission Implementing Regulation 2023/1769 supplements Delegated Regulation 2023/1768 by specifying various requirements concerning the EASA's "administration and management systems" (Annex I) for the execution of its duties and obligations. For instance, the EASA "shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety [...]" in coordination with Member States' "relevant authorities responsible for information security or cybersecurity" (Annex I).
-   Commission Implementing Regulation 2023/203 lays down "requirements for the management of information security risks with a potential impact on aviation safety" for organizations (e.g., maintenance organizations and air operators) and competent authorities (e.g., EASA). To identify, manage, detect, respond to, and recover from information security risks or incidents, these organizations and authorities are required to undertake various measures, such as setting up "information security management systems (ISMS)" and performing "information security risk assessments" (Annex I & II).
-   Commission Delegated Regulation 2020/2148 addresses runway safety and aeronautical data and amends Regulation 139/2014, laying down "requirements and administrative procedures related to aerodromes" [1]. According to the amendments of

107 Chapter 13 further explains what the EASA does in the area of cybersecurity (policy).

108 See further European Union Aviation Safety Agency (n.d.): Aircraft certification.

the Delegated Regulation, aerodrome operators shall “establish a security management system to ensure the security of operational data it receives, or produces, or otherwise employs, so that access to that operational data is restricted only to those authorised” (Annex). Aerodrome operators should also “take the necessary measures to protect its aeronautical data against cyber security threats” (Annex). [1] Aerodromes refer to “defined area[s] (including any buildings, installations and equipment) on land or water or on a fixed, fixed offshore or floating structure intended to be used either wholly or in part for the arrival, departure and surface movement of aircraft” (Art. 2(1), Regulation 139/2014).

- ﷺ Commission Implementing Regulation 2019/947 sets out “detailed provisions for the operation of unmanned aircraft systems [UAS] as well as for personnel, including remote pilots and organisations involved in those operations” (Art. 1). In taking the necessary measures to address safety issues concerning UAS operations, Member States’ competent authorities and the EASA shall consider “interdependencies between the different domains of aviation safety, and between aviation safety, cyber security and other technical domains of aviation regulation” (Art. 19(4)).
- ﷺ Commission Implementing Regulation 2017/373 lays down the requirements for “the provision of air traffic management and air navigation services (‘ATM/ANS’) and other air traffic management network functions (‘ATM network functions’) for general air traffic” (Art. 1(1)) as well as their oversight. For instance, ANS and air traffic flow management providers shall “take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cyber security threats which may have an unlawful interference with the provision of their service” (Annex III).

— Other Implementing/Delegated Acts

ﷺ Commission Delegated Regulation 2020/2034 establishes the “common European risk classification scheme (ERCS)” (Art. 1), used to assess “the risk posed by an occurrence to civil aviation” (Art. 2 (1)). The Delegated Regulation complements Regulation 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation. Within the Delegated Regulation, the Commission identified various key risk areas, including “security” (Annex). Security-related risks encompass “an act of unlawful interference against civil aviation”, which may arise from “both physical and cyber security events” (Annex). The ERCS should “allow for the identification of rapid actions needed in reply to high-risk safety occurrences” and “facilitate an integrated and harmonised approach to risk management across the European aviation system,” enabling Member States’ competent authorities and the EASA to “focus on safety improvement efforts [...] as part of the European Plan for Aviation Safety” (recital (4)).

ﷺ Commission Implementing Regulation 2019/1583 (complementing Regulation 300/2008 on common rules in the field of civil aviation security) has the objective of “support[ing] Member States in ensuring full compliance with the most recent amendment [...] of the Convention on International Civil Aviation” (recital (3)), which introduced new standards relating to preventive cybersecurity measures. In accordance, the Implementing Regulation stipulates that Member States’ appropriate authorities shall make sure that airport operators, air carriers, and

entities “identify and protect their critical information and communications technology systems and data from cyber-attacks which could affect the security of civil aviation” and “detail the measures to ensure the protection from, detection of, response to and recovery from cyber-attacks” (Annex) in their respective security programmes.

Health

— eHealth Network

The ﷺ Directive 2011/24 establishes “rules for facilitating the access to safe and high-quality cross-border healthcare” and encouraging “cooperation on healthcare between Member States” (Art. 1). According to Article 14, the EU “shall support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth”[109] (Art. 14(1)). Building upon this Directive, ﷺ Commission Implementing Decision 2019/1765 provides Member States with “rules for the establishment, the management and the functioning of the eHealth Network of national authorities responsible for eHealth” (Art. 1).[110] It stipulates that one of the eHealth Network’s functions may involve “provid[ing] guidance to the Members on security of the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services[111] or other shared European eHealth Services” (Art. 4(1)) while taking into account relevant EU legislation, documents, and recommendations concerning security, particularly cybersecurity. To fulfill this role, the eHealth Network shall cooperate closely with the NIS Cooperation Group and ENISA. As the data processor for the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services, the Commission shall “[s]et up and ensure a secure and reliable communication infrastructure that interconnects networks of the Members” (Annex), also known as the Central Secure Communication Infrastructure. The Commission is also responsible for its security, for instance, by regularly controlling the “integrity of system files, security parameters and granted authorisations” (Annex).

109 The German Federal Ministry of Health (BMG) defines eHealth as applications that utilize the possibilities offered by modern information and communication technologies (ICT) to support the treatment and care of patients (own translation based on Federal Ministry of Health: E-Health).

110 The eHealth Network subsequently issued Guidelines on the electronic exchange of health data under Cross-Border Directive 2011/24, which can be accessed here.

111 The eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services was developed by Member States to facilitate the exchange of health-related data across borders and enhance the “interoperability between national eHealth systems” (recital (8), Commission Implementing Decision 2019/1765.

— Commission Recommendation on a European Electronic Health Record Exchange Format

In February 2019, the Commission adopted ⬜⬜ Commission Recommendation 2019/243, providing a framework for the development of a "European electronic health record exchange format" to facilitate the secure cross-border exchange of electronic health data within the EU. As the "secure access to electronic health record systems" (p. 4) within each Member State constitutes a prerequisite for such exchange, the Commission encourages Member States to uphold rigorous standards for protecting health data and securing the network and information systems supporting these electronic health record systems. In line with the obligations derived from the GDPR and NIS Directive, the Commission also stresses that Member States must implement specific security measures when developing solutions that facilitate the access to and cross-border exchange of electronic health data. These include protecting against "unauthorised or unlawful processing of health data," preventing "accidental loss, destruction, or damage," and ensuring that the personnel of Member States' entities involved in the exchange of electronic health records must be "properly aware of cybersecurity risks and adequately trained" (p. 7). Each Member State should also set up a digital health network at the national level comprising relevant national and regional authorities responsible for digital healthcare, electronic health record interoperability, network and information system security, and data protection. These national digital health networks should focus their discussions on improving the "interoperability and security of national health systems" and facilitating the "secure exchange of health data across borders" (p. 4). The outcomes of these discussions shall be shared with the eHealth Network and the Commission.

— Communication on Enabling the Digital Transformation of Health and Care in the Digital Single Market

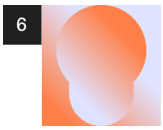
In April 2018, the Commission adopted ⬜⬜ Communication (2018) 233, which addresses the digital transformation of health and care services in the EU. It identifies various areas for further action, including ensuring "citizens' secure access to and sharing of health data across borders" (p. 6). In this regard, the Commission holds out the prospect of a "Commission recommendation on the technical specifications for a European electronic health record exchange format" (p. 8). Another area for further EU action is the generation of "better data to advance research, disease prevention and personalised health and care" (p. 8). In this respect, the Commission, inter alia, aims to "connect national initiatives with European networks of scientific and clinical expertise" in order to "help European

research and industry remain at the forefront" while emphasizing that such initiatives "should take full account of EU policy and technological developments in the field of cybersecurity [...]" (p. 9).

— Council Conclusions on Health in the Digital Society

In its ﷺ Council conclusions on Health in the Digital Society from December 2017, the Council emphasizes the importance of enabling citizens to "better understand and manage their own health with easier access to information and digital tools" (p. 4) in the digital age. With data protection and information security having "utmost importance [in] maintain[ing] public trust in digital health services" (p. 5), the Council calls for Member States' prompt implementation of relevant EU legal frameworks, including the NIS Directive and eIDAS Regulation. The Conclusions also invite Member States and the Commission to "improve data security" by "exchanging information on available technical tools and methodologies for secure data exchange" (p. 7) regarding personal health data, as well as to "develop common approaches to ensure safety, quality, security and interoperability of mobile health tools and applications" (p. 8).

Policy Area 6: Education, Research and Space Policy



In the area of education, the EU is tasked with "carry[ing] out actions to support, coordinate or supplement the actions of the Member States" (Art. 6, point (e) TFEU). In particular, the EU "shall contribute to the development of quality education by encouraging cooperation between Member States and, if necessary, by supporting and supplementing their action, while fully respecting the responsibility of the Member States for the content of teaching and the organisation of education systems and their cultural and linguistic diversity" (Art. 165(1) TFEU). The Treaty on the Functioning of the EU jointly addresses research and space. In terms of EU competencies, it notes that "in the areas of research, technological development and space" (Art. 4(3) TFEU), "the Union shall have competence to carry out activities, in particular to define and implement programmes; however, the exercise of that competence shall not result in Member States being prevented from exercising theirs" (Art. 4(3) TFEU). In doing so, the EU shall strive to enhance "its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely, and encouraging it to become more competitive, including in its industry, while promoting all the research activities deemed necessary by virtue of other Chapters of the Treaties" (Art. 179(1) TFEU).

Education

— Council Recommendations on Digital Education and Digital Skills

In November 2023, the Council issued a ◆◆ Recommendation on improving the provision of digital skills and competences in education and training (C/2024/1030). In its Recommendation, the Council encourages Member States to adopt initiatives that "support a two-way exchange and collaboration between education and training institutions and the private sector" (p. 7). This approach aims to enable professionals in the digital sector to assist educators while educators can acquire expertise in areas such as cybersecurity. Member States should also undertake measures to "attract more learners to vocational programmes in areas such as AI, cybersecurity and software development" (p. 8) and "support higher education institutions in encouraging students, and particularly women" (p. 8) to pursue subjects that emphasize skill development in domains such as cybersecurity. In "develop[ing] a strategic and systematic approach to addressing the shortage of ICT professionals", Member States should consider incorporating programs aimed at alleviating "digital skills shortages", for instance, in the area of cybersecurity, also in light of the Commission's Cybersecurity Skills Academy initiative (p. 10).

On the same day, the Council also issued a ◆◆ Recommendation on the key enabling factors for successful digital education and training (C/2024/1115). The Recommendation addresses the opportunities brought by emerging technologies and potential risks, like cybersecurity threats. Against this backdrop, the Council recommends Member States to take "comprehensive measures to address cybersecurity in all education and training institutions," encourage "all staff to undertake cybersecurity training," and raise "cybersecurity awareness among students and their families" (p. 6).

— Cybersecurity Skills Academy

The ◆◆ Communication on the Cybersecurity Skills Academy by the Commission from April 2023 addresses the "cybersecurity professional talent gap" (p. 4) in the EU. It aims to enhance the Union's "competitiveness, growth and resilience" (Communication title). To achieve this goal, the Commission puts forward the Cybersecurity Skills Academy, designed to serve as a central hub for cybersecurity education and training opportunities, funding avenues, and initiatives supporting cybersecurity skills development. The Academy's four pillars, their respective objectives, and a non-exhaustive overview of exemplary activities and measures

under each pillar are explained in the table below:

Table 28: Objectives and Activities of the Cybersecurity Skills Academy

Pillars	Specific Objectives	Examples of Activities and Measures
(1) "Knowledge generation and training: establish a common EU approach to cybersecurity training"	p. 7: • "Increas[ing] the number of persons with cybersecurity skills in the EU" • "Better target[ing] trainings to market needs" • "Provid[ing] visibility over career pathways"	• Review of European Cyber Skills Framework (ECSF) by ENISA, which provides the foundation of the Academy to "define and assess relevant skills, monitor the evolution of the skill gaps and provide indications on the new needs" (p. 8) • ENISA will further "expand its 'train the trainer' programme" to include public and private critical operators to which the NIS 2 Directive applies (p. 9f.) • Invitation to Member States's National Coordination Centres (NCCs) to set up Cyber Campuses to "facilitate cooperation at national level among academia and providers of cybersecurity skills trainings" and "foster synergies between the public and private sectors" (p. 9) • Creation of "a single point of entry for cybersecurity programmes, existing trainings, and for cybersecurity certifications via the Digital Skills and Jobs Platform" by the Commission (p. 11)
(2) "Stakeholder involvement: committing to close the cybersecurity skills gap"	• "Maximis[ing] the visibility and impact of the various stakeholders' commitments at narrowing the cybersecurity skills gap" (p. 12)	• Member States should include "specific measures to address the cybersecurity skills gap" in their respective national cybersecurity strategies (p. 13) • Stakeholders in the cybersecurity industry should "make concrete commitments," so-called cybersecurity pledges, to "upskill and reskill workers through dedicated actions" (p. 12) [for more information on the pledges, see here] • Member States should "implement the Women in Digital Declaration" to achieve "gender convergence in cybersecurity positions" (p. 12)
(3) "Funding: build synergies to maximise the impact of spending for developing cybersecurity skills"	p. 13: • "Facilitating a better channelling of the funds towards the needs of the market" • "Mainstreaming the use of funding" • "Facilitating synergies between	• The ECCC and ENISA shall "map existing EU funding for cybersecurity skills against market needs, assess effectiveness and identify funding priorities" by the end of 2024 (p. 14) • Creation of "a single point of entry for funding opportunities for cybersecurity skill" by the Commission through the Digital Skills and Jobs Platform (p. 15) [for further information, see here]

	different instruments while avoiding duplication of efforts"	
(4) "Measuring progress: built-in accountability"	• "Measuring the progress to close the cybersecurity skills gap" (p. 15)	• Development of indicators by ENISA (supported by the Commission and the NIS Cooperation Group) to track "the state of the cybersecurity skills and job market" annually as a contribution to ENISA's biennial report on the Union-level state of cybersecurity (p. 15)

Research

— European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres

In June 2021, the ⬚⬚ Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre [ECCC] and the Network of National Coordination Centres (2021/887) entered into force. Relevant provisions on the ECCC are covered in its actor profile [see further Chapter 13]. In addition to the ECCC, the Regulation establishes a Network of National Coordination Centres (or NCCs) and a Cybersecurity Competence Community. The NCC Network comprises national NCCs, to be designated/established by every Member State.[112] The NCCs shall conduct, inter alia, the following activities:

- "acting as points of contact at national level for the Community to support the Competence Centre in fulfilling its mission and objectives;"
- "providing expertise and actively contributing to the [ECCC's] strategic tasks set out in Article 5(2), taking into account relevant national and regional challenges for cybersecurity in different sectors;"
- "promoting, encouraging and facilitating the participation of civil society, industry, in particular start-ups and SMEs, the academic and research communities and other stakeholders at national level in cross-border projects and in cybersecurity actions funded by relevant Union programmes;"
- "providing technical assistance to stakeholders by supporting them in the application phase for projects managed by the Competence Centre in relation to its mission and

112 More information on and a full list of the NCCs can be found here. To qualify as an NCC, the Regulation stipulates that the designated entity shall "be a public sector entity or an entity, a majority of which is owned by the Member State, which performs public administrative functions under national law", "hav[e] the capacity to support the Competence Centre and the Network in fulfilling their mission", "possess or have access to research and technological expertise in cybersecurity" and "have the capacity to engage effectively and coordinate with industry, the public sector, the academic and research community and citizens" (Art. 6(5)).

objectives;"

- and "seeking to establish synergies with relevant activities at national, regional and local level, such as national policies on research, development and innovation in the area of cybersecurity" (Art. 7(1)).

In specified circumstances, Member States "may receive a grant from the Union [...] in relation to carrying out the[ir NCC-related] tasks" (Art. 7(3)).

The role of the concurrently established Cybersecurity Competence Community is to

- provide support to the ECCC "in fulfilling its mission and objectives" and, "where relevant", to the ECCC and the NCCs in the "promoti[on of] specific projects," and
- "where relevant, participate in formal or informal activities and in [community working groups] to carry out specific activities as provided by the annual work programme" (Art. 9).

In terms of membership, the Regulation specifies that the "Community shall bring together the main stakeholders with regard to cybersecurity technological, industrial, academic and research capacities in the Union" (Art. 8(2)), encompassing "SMEs, academic and research organisations, other relevant civil society associations as well as, as appropriate, relevant European Standardisation Organisations, public entities and other entities dealing with cybersecurity operational and technical matters" (Art. 8(2)) that are "established within the Member States" (Art. 8(3)). Following the request of an entity to join the Community, its registration as a community member is subject to an assessment by its respective NCC. Similarly, the ECCC assumes these functions in case EUIBAs seek community membership. The ECCC's Strategic Advisory Group comprises a maximum of 20 nominated experts out of the community membership pool.

— Horizon Europe

In May 2021, the Council established Horizon Europe via its ⧉⧉ Council Decision establishing the Specific Programme implementing Horizon Europe – the Framework Programme for Research and Innovation (2021/764). In the framework of Horizon Europe, €95.5 billion can be allocated until 2027.[113] Cybersecurity is given a dedicated focus in the Programme's cluster "civil security for society" (Art. 3(b)). In this respect, the Council notes that "it is in the Union's interest to ensure that it develops and retains essential cybersecurity strategic capacities in order to secure the Digital Single Market and, in particular, to ensure the protection of

113 Its predecessor programme was the Horizon 2020 programme, which provided funding to research and innovation in the EU from 2014-2020 (see further Council Decision 2013/743).

critical networks and information systems and to provide key cybersecurity services" (Annex I). According to the Horizon Europe Work Programme (2023-2025) for the cluster Civil Security for Society, the ECCC is entrusted with implementing the call for proposals for cybersecurity projects.[114] Projects shall, inter alia, aim at attaining the following impacts: "strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies," "increased software, hardware and supply chain security," and a "reinforced awareness and a common cyber security management and culture" (p. 100).

Space

— Secure Connectivity Programme

In addition to the Space Programme, the Union Secure Connectivity Programme was established through the ﷺ Regulation establishing the Union Secure Connectivity Programme for the period 2023-2027 (2023/588) in March 2023. The Union Secure Connectivity Programme, inter alia, aims to "ensure the provision and long-term availability within the Union's territory and worldwide uninterrupted access to secure, autonomous, high-quality, reliable and cost-effective satellite governmental communication services to government-authorised users" (Art. 3(1), point (a)). The programme is based on two types of infrastructures, having a governmental and commercial designation respectively (Art. 5(1)). As one of its 10 specific objectives, the Secure Connectivity Programme shall "increase [...] the cyber resilience of the Union, by developing redundancy, passive, proactive and reactive cyber protection and operational cybersecurity and protective measures against cyber threats" (Art. 3(2), point (e)). The "annual number and severity of impact of cybersecurity incidents [...] related to the secure connectivity system" (see Annex 7.2) shall serve as one of the indicators for evaluating the attainment of this specific objective. Similar to the Space Programme, the Commission shall, "in its field of competence" and supported by the EUSPA, inter alia, "ensure a high degree of security with regard [...] to the protection of infrastructure, both ground and space, and of the provision of services, particularly against physical or cyber-attacks, including interference with data streams" (Art. 30(1), point (a)). For the governmental side of the programme, the Commission is tasked with conducting a "risk and threat analysis" (Art. 30(3)).

114 Also the 2025-2027 overall strategic research and innovation plan includes measures relating to cybersecurity. It can be accessed here.

— Space Programme

�� Regulation 2021/696 establishes the Union Space Programme until 2027 to, among other objectives, “enhance the safety and security of the Union and its Member States and reinforce the autonomy of the Union” (Art. 4(1), point (c)) and specifies the mandate of the European Union Agency for the Space Programme (EUSPA). Said programme consists of five components:

- (a) Galileo, “an autonomous civil global navigation satellite system (GNSS) under civil control;”
- (b) the European Geostationary Navigation Overlay Service (EGNOS), “a civil regional satellite navigation system;”
- (c) Copernicus, “an operational, autonomous, user-driven, civil Earth observation system under civil control;”
- (d) Space Situational Awareness, including, for instance, “a space surveillance and tracking system aiming to improve, operate and provide data, information and services related to the surveillance and tracking of space objects that orbit the Earth;”
- (e) and GOVSATCOM, a “satellite communications service under civil and governmental control enabling the provision of satellite communications capacities and services to Union and Member State authorities managing security critical missions and infrastructures” (Art. 3(1)).

In terms of the programme’s security, the Commission shall, “in its field of competence” and supported by the EUSPA, inter alia, “ensure a high degree of security with regard [...] to the protection of infrastructure, both ground and space, and of the provision of services, particularly against physical or cyber-attacks, including interference with data streams” (Art. 34(1), point (a)). Every component is managed by a particular entity, which holds responsibility “for the operational security of that component [... and] carry[ing] out risk and threat analysis and all the necessary activities to ensure and monitor the security of that component” (Art. 34(3)). For Galileo and EGNOS, the EUSPA assumes all management functions and the Commission does so for Copernicus. The Commission holds the “overall responsibility” to implement the Union Space Programme (Art. 28(1)). To account for instances in which “the security of systems and services deployed, operated and used under the Union Space Programme” may pose a threat to the Union’s security, the Council adopted Council Decision 2021/698 specifying particular procedures for handling such situations.

Policy Area 7: Foreign and Security Policy

The Treaty of the EU provides that the EU "shall conduct, define and implement a common foreign and security policy [CFSP], based on the development of mutual political solidarity among Member States, the identification of questions of general interest and the achievement of an ever-increasing degree of convergence of Member States' actions" (Art. 24(2) TEU). The competences conferred to the EU "cover all areas of foreign policy and all questions relating to the Union's security, including the progressive framing of a common defence policy that might lead to a common defence" (Art. 24(1) TEU). In terms of its implementation, the Treaty on the EU notes that the CFSP "shall be put into effect by the High Representative and by the Member States, using national and Union resources" (Art. 26(3) TEU). The Common Security and Defence Policy (CSDP) is designated by the Treaty of the EU as "an integral part" (Art. 42(1) TEU) of the EU's CFSP. The Treaty on the EU lays out that the CSDP shall "provide the Union with an operational capacity drawing on civilian and military assets", based on "capabilities provided by the Member States" (Art. 42(1) TEU). CSDP activities may involve, for instance, "joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation" (Art. 43(1) TEU), to be decided by the Council of the EU. On matters relating to the CFSP, the adoption of legislative acts is precluded (Art. 31(1) TEU and declaration 41 annexed to the TFEU).

Strategic Documents

— Council Conclusions on the Development of the European Union's Cyber Posture

In May 2022, the Council adopted its ⬚⬚ Conclusions on the development of the European Union's cyber posture. According to the Conclusions, "the cyber posture aims to combine the various initiatives that concur in EU actions consolidating peace and stability in the cyberspace and in favour of an open, free, global, stable and secure cyberspace, while better coordinating short, medium and long term actions to prevent, discourage, deter and respond to cyber threats and attacks and leveraging cyber capabilities" (p. 5). The posture comprises the following five objectives, which are further specified as follows:

Table 29: Overview of Council Conclusions on the Development of the European

Union's Cyber Posture

Objectives	Overview of Provisions

1: "strengthen[ing the EU's] cyber resilience and capacities to protect"	Vis-à-vis EUIBAs:
	• Council calls on Commission
	  • "to propose EU common cybersecurity requirements for connected devices and associated processes and services through the Cyber Resilience Act" (p. 6)
	  • "to explore options for [...] a mechanism [for stable and long term financing of cybersecurity by combining multiple sources of financing] before the end of 2022" (p. 8)
	• Council invites
	  • Body of European Regulators for Electronic Communications (BEREC), ENISA, and the NIS Cooperation Group "along with the European Commission, to formulate recommendations [... on how to] reinforce the resilience of communications networks and infrastructures within the European Union" (p. 6)
	  • "Commission to propose options to encourage the emergence of a trusted cybersecurity service industry, to strengthen the cybersecurity of the ICT supply chain, to address the potential effects of software vulnerabilities for the EU and its Member States, [...] and to improve cyber threat detection and sharing capabilities in and across Member States" (p. 7)
	  • "Commission to explore options to increase cybersecurity across the whole supply chain of the EU's Defence Technological and Industrial Base" (p. 8)
	Vis-à-vis Member States:
	• Council "calls upon the EU and its Member States to reinforce efforts to raise the overall level of cybersecurity, for example by facilitating the emergence of trusted cybersecurity service providers" (p. 7)
	General:
	• "Importance of mainstreaming cybersecurity considerations in all EU public policies" (p. 8)
	• Necessity of strengthened efforts and reinforced cooperation "in the fight against international cybercrime, in particular ransomware", inter alia, via EMPACT (p. 8)

2: "enhanc[ing] solidary and comprehensive crisis management"	Vis-à-vis EUIBAs:
	• Council invites
	  • Commission, High Representative, and NIS Cooperation Group "to conduct by the end of 2022 a risk evaluation and build risk scenarios from a cybersecurity perspective in a situation of threat or possible attack against Member States or partner countries", coordinated "with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe" (p. 10)
	  • "Commission to present a proposal on a new Emergency Response Fund for Cybersecurity by the end of Q3 2022" (p. 11)
	  • "Commission and other relevant [EUIBAs] to carry out by the end of 2022 a mapping of existing tools for secure communication in the cyber field" (p. 11)
	General:
	• "Importance of establishing a programme of regular cross-community and multi-level cyber exercises in order to test and develop the EU's

	internal and external response to large-scale cyber incidents" (p. 9) • "Further develop[ment of] the Cyber Europe and BlueOLEx exercises" (p. 9) • Exploration of "further exercises on specific segments of the cyber domain, notably a military CERT exercise and an exercise focusing on crisis cooperation amongst EUIBAs" (p. 9) • "Importance of working on developing a common language amongst Member States and with EUIBAs, [...] tailored for discussion at the political level" (p. 10)
3: "promot[ing the EU's] vision of cyberspace"	Vis-à-vis EUIBAs: • Council calls on "the High Representative to review the existing bilateral cyber dialogues and, if necessary, propose to start similar cooperation with additional countries or relevant international organisations" (p. 12) Vis-à-vis Member States: • Council "commits itself to continuous engagement in relevant international organisations especially in the UN First and Third committees related processes" (p. 13) General: • Further support for the "development and operationalisation of confidence-building measures (CBMs) at regional and international level, and further encouraging the use of existing cyber CBMs at the OSCE, including in times of international tensions" (p. 13)
4: "enhanc[ing] cooperation with partner countries and international organisations"	Vis-à-vis EUIBAs: • Council calls on • "the High Representative and the Commission to establish a Cyber capacity building board by Q3 2022" (p. 14) • "the Commission and High Representative to further mobilise [existing financial tools] to support strengthening the resilience of our partners, their capacity to identify and address cyber threats and to investigate and prosecute cybercrimes" (p. 14) • "the High Representative to establish the EU Cyber Diplomacy Network by Q3 2022" (p. 15) • Council "requests the High Representative to present an outreach plan [to promote a global common understanding of the application of international law in cyberspace, the UN framework of responsible State behaviour in cyberspace [and] on the EU and its Members States' position in the ongoing negotiations of a UN Cybercrime Convention] to the Council by the end of 2022" (p. 15) General: • Better connection between the EU Cyber Capacity Building Strategy and the UN norms for responsible state behaviour in cyberspace (p. 14) • "Importance of fully integrating cyber capacity building as part of the EU's offer as a security provider" (p. 14) • "Further strengthen[ed] cyber cooperation with NATO" (p. 16)
5: "prevent[ing], defend[ing] against and respond[ing] to cyber-attacks"	Vis-à-vis Member States and EUIBAs: • Council "invites the Member States and the High Representative, with the support of the Commission, to work towards a revised version of the implementing guidelines of the EU Cyber Diplomacy Toolbox by the end of Q1 2023, notably by exploring additional response measures" (p. 16) Vis-à-vis EUIBAs: • Council "calls upon the High Representative, in cooperation with the

Commission, to identify possible EU joint responses to cyberattacks, including sanctions options, across the spectrum" (p. 18)
- Council invites
  - "the High Representative to develop and submit to the Member States a coherent communication strategy on the use of the EU Cyber Diplomacy Toolbox" (p. 17)
  - "the High Representative together with the Commission to [...] tabl[e] an ambitious proposal for an EU Cyber Defence Policy in 2022" (p. 18)

Vis-à-vis Member States:

- Council "encourages Member States to further develop their own capabilities to conduct cyber defence operations" (p. 18)
- Council "invites Member States to create [...] a MilCERT network [...] as well as a network of military cyber commanders" (p. 19)

General:

- Council "notes the need to strengthen intelligence and information sharing and cooperation between Member States as well as with the EU INTCEN" (p. 17)
- "Importance of [...] exploring the proposal on the possible establishment of a Member States' cyber intelligence working group" (p. 17)

— Strategic Compass

In March 2022, the Council approved the ﬀ Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security. Based on an "EU Threat Analysis," the Compass starts by outlining threats implicating the EU's strategic environment. With respect to cyber and IT security, the Strategic Compass emphasizes that "cyberspace has become a field for strategic competition, at a time of growing dependence on digital technologies" and that the EU "increasingly fac[es] more sophisticated cyberattacks" (p. 12). It notes Russia's "readiness to use the highest level of military force, [...] combined with [...] cyberattacks" (p. 7) with respect to its armed aggression against Ukraine, China's pursuit of "its policies [...] by using cyber tools" (p. 8), and the endangerment of "regional and international peace and security, through [...] cyberattacks" (p. 10) emanating from the Democratic People's Republic of Korea (DPRK). Regarding EU action in the area of security and defense to address the resulting challenges, the Strategic Compass is centered around four work strands under which particular measures are subsumed. The overall objectives of the work strands are to:

- "be able to act rapidly and robustly whenever a crisis erupts, with partners if possible and alone when necessary" (*act*, p. 3);
- "enhance [the EU's] ability to anticipate threats, guarantee secure access to strategic domains and protect our citizens" (*secure*, p. 3);
- "invest more and better in capabilities and innovative technologies, fill strategic gaps and reduce technological and industrial dependencies" (*invest*, p. 4);

- and "strengthen [EU] cooperation with partners to address common threats and challenges" (*partner*, p. 4).

The table below provides an exemplary overview of the measures within the work strands which are of relevance to cybersecurity policy:

Table 30: Objectives and Exemplary EU Actions Specified in the EU's Strategic Compass

Work Strand	Area/Objective of EU Action	Exemplary Actions
1. Act	"Acting together"	• Provision of "associated assets and necessary strategic enablers" such as cyber defense for effective deployment of the "EU Rapid Deployment Capacity" and "develop[ment of] these capabilities where necessary" (p. 14) • Conduct of "regular cyber exercises" to "further strengthen [...] mutual assistance in case of an armed aggression" (p. 20) • Revision of Military Mobility Action Plan, inter alia, to "increas[e] cyber resilience of transport infrastructure and its support systems" (p. 20)
2. Secure	"Strengthening our early warning, intelligence picture and secure communications"	• "Streamlin[ing] security rules and regulations as well as bolster the common approach by the Member States, EU Institutions, bodies and agencies, as well as CSDP missions and operations" through "investments in state-of-the-art European technical equipment, infrastructure and expertise" (p. 21) • Adoption of "additional standards and rules to ensure cybersecurity and security of information" for EUIBAs (p. 21 and 27)
	"Hybrid threats, cyber diplomacy and foreign information manipulation and interference"	• Reinforcement of the EU Cyber Diplomacy Toolbox through the "explor[ation of] additional response measures" (p. 22 and 27)
	"Securing our access to strategic domains"	• Further development of the EU Cyber Defence Policy (p. 23) • Adoption of the Cyber Resilience Act to "increase [...] common approach to cyber infrastructure and standards" (p. 23) • Efforts to set up a "European infrastructure of Security Operations Centres" (p. 23) • Development of the "Union's cyber posture by enhancing [the EU's] ability to prevent cyberattacks [...] and by responding firmly to cyberattacks against the Union, its Institutions and its Member States using all available EU tools" (p. 23) • Strengthening of "cyber intelligence capacities" (p. 23) • Enhancement of cooperation between military CERTs (p. 23)

3. Invest	"Strategic orientations"	• Revision of "capability planning scenarios" by including, inter alia, a scenario on "securing access to strategic domains such as [...] cyber" (p. 31) • Investments in "cyber defence capabilities" as part of a range of "strategic enablers" to "mitigate critical capability shortfalls" (p. 31)
	"Coherent and ambitious capabilities"	• Development and "intensive use of new technologies [in the cyber domain], notably quantum computing, Artificial Intelligence and Big Data, to achieve comparative advantages" (p. 32)
	"Innovation, disruptive technologies and reducing strategic dependencies"	• Operationalization of the ECCC to "develop a strong European cyber industrial and technological ecosystem" (p. 35)
4. Partner	"Multilateral and regional partners"	• Deepened cooperation with NATO, inter alia, on "securing cyberspace" (p. 39) • "Enhance[d] shared awareness and information exchange on [...] cybersecurity" with ASEAN (p. 41)
	"Tailored bilateral partnerships"	• Cooperation, inter alia, on cyber defence with the US (p. 42) • Commitment to "boost[...] cybersecurity" in the Western Balkans (p. 42) • Strengthening of "specific dialogues and cooperation [...] in particular in areas such as [...] cybersecurity" with Ukraine, Georgia, and the Republic of Moldova (p. 42) • Support to "African partners" in "strengthen[ing] their resilience against [...] cyberattacks" (p. 43) • Increased collective efforts toward Latin American countries to "help[...] them counter [...] cyberattacks" (p. 43)

Cyber Diplomacy

— Cyber Diplomacy Toolbox

In its 2017 ﷺ Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, the Council of the EU notes "that measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities and should encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in a long term" (p. 4). The Council further specifies that the framework shall be guided by the following considerations as guiding principles:

- “serv[ing] to protect the integrity and security of the EU, its Member States and their citizens;”
- “tak[ing] into account the broader context of the EU external relations with the State concerned;”
- “provid[ing] for the attainment of the CFSP objectives as set out in the Treaty on the European Union (TEU) and the respective procedures provided for their attainment”;
- “be based on a shared situational awareness agreed among the Member States and correspond to the needs of the concrete situation in hand;”
- “be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity;”
- and “respect[ing] applicable international law and must not violate fundamental rights and freedoms” (p. 4).

To follow through on the objective of establishing such a framework, the Cyber Diplomacy Toolbox, Member States have since approved the implementing guidelines for this Toolbox in ﷺ 2017 and subsequently revised them in ﷺ 2023. Both sets of guidelines reiterate the above-listed guiding principles. A revision of the implementing guidelines was deemed necessary against the backdrop of “a significant corrosion of international security, including in cyberspace” (p. 2, 2023), requiring the EU and its Member States to “step up their ability to strengthen situational awareness, prevent, discourage, deter and respond to malicious cyber activities, ensure solidarity and mutual assistance and enforce the United Nations framework for responsible state behaviour in cyberspace” (p. 3, 2023). As a consequence, the revised guidelines seek to add to the 2017’s “incident-based approach” by setting out “the development of sustained, tailored, coherent and coordinated strategies towards persistent cyber threat actors, to ensure a more strategic, gradual and long-term approach” (p. 11, 2023).

The measures included within the Toolbox are meant to be “complementary to existing and continuous cyber diplomacy engagement to advance conflict prevention, cooperation and stability in cyberspace” (p. 5, 2023) and can be carried out “individually or jointly, in coordination or in parallel, and where appropriate in cooperation with international partners” (p. 10, 2023). The Toolbox may further be “used in tandem with other Union measures” (p. 6, 2023), such as the EU Hybrid Toolbox or the EU Foreign Information Manipulation and Interference Toolbox (p. 22, 2023). With regard to crisis management, “the Cyber Diplomacy Toolbox can be implemented as part of, or in parallel and in complementarity of [EU] crisis management mechanisms” (p. 22, 2023), including, for example, the IPCR mechanism, the EEAS Crisis Management Response Mechanism, or the EEAS Situation Room. The 2023 implementing guidelines underscore the “key importance” of “ongoing and regular exchanges on the cyber threat landscape and thematic briefings in the HWPCI” for developing a “baseline understanding and shared awareness of the cyber threat landscape [which can] serve as the basis for

assessments following a malicious cyber activity or cyber incident" (further specified on p. 12f., 2023).

The Toolbox, inter alia, comprises the following measures:

Table 31: Components of the EU Cyber Diplomacy Toolbox

Category of Measures	Specific Tools
Preventive measures (p. 6, 2017)	• "EU-supported Confidence Building Measures" • "Awareness raising on EU policies" • "EU cyber capacity building in third countries"

Cooperative measures (p. 7, 2017)	• "Cooperation through EU-led political and thematic dialogues or through démarches by the EU Delegations" for either of the following purposes:
	  • "signal[ling] the seriousness of the situation for the EU and its Member States",
	  • "facilitat[ing] the peaceful resolution of an ongoing incident",
	  • "ask[ing] for assistance or cooperation to mitigate the malicious activity",
	  • or "ask[ing] a third country to join in the response to a malicious cyber activity"

Stability measures (p. 7f., 2017)	• "Statements by the High Representative and on behalf of the Council of the EU" [for example, Council of the EU (2022): Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union] • "EU Council conclusions" • "Diplomatic démarches by the EU delegations" • "Signalling through EU-led political and thematic dialogues"
Restrictive measures (p. 9, 2017)	• Sanctions such as "travel bans, arms embargos, freezing funds or economic resources"
Possible EU support to Member States' lawful responses (p. 9f., 2017)	• Upon request, provision of support to "Member States that individually or collectively resort to responses in accordance with international law that are not available within the CFSP"
2023 additions (p. 10, 2023)	The 2023 guidelines identified the following measures, among others [the guidelines refer to a full list contained in a classified separate annex] • "building further global partnerships in view of diplomatic responses" • "raising awareness, notably making use of the publication of advisories" • "coordinated action to counter malicious foreign intelligence activities" • "suspension or cancellation of engagements or dialogues" • exploration the possibility of "us[ing] sectoral sanctions" and "amend[ing] or extend[ing] the EU cyber sanctions regime"

To implement the Toolbox "in response to a large-scale cross border malicious

cyber activity [... or] a situation of an accumulation of malicious cyber activities" (p. 22, 2023), the 2023 guidelines specify a 9-step-process[115]:

Table 32: Implementation of the EU Cyber Diplomacy Toolbox

Step		Specification

1	Start discussions on the use of measures part of the EU Cyber Diplomacy Toolbox (p. 15, 2023)	• Member States or EEAS can
		  • inform Council on "persistent cyber threat, [detection of] a malicious cyber activity or a large-scale cybersecurity incident [...] or a partner's request for support"
		  • "express an interest in exchanging shared situational awareness"
		  • "exploring a joint EU diplomatic response"

2	Exchange of shared situational awareness (p. 15, 2023)	• Upon request, provision of "further specific assessments or briefings" by SIAC or others to HWPCI • Consideration of inviting "geographical working parties [...] to the HWPCI to enhance the understanding on the EU's broader international relations"
3	Exploration of a possible joint EU diplomatic response (p. 15f., 2023)	• "Any Member State or EUIBAs may propose or request to consult the Council for a joint EU diplomatic response" • "request may include a call for a 'strategic response note' [coordinated by the EEAS] that outlines or updates a sustained, tailored, coherent and coordinated strategy towards that particular threat actor or malicious activity" • HWPCI may request EEAS to "outline the possible response options, where necessary by providing an options note"
4	Deliberations on a possible joint EU diplomatic response (p. 16, 2023)	• HWPCI assumes "central role in decision-making as regards a joint EU diplomatic response", operating "under the guidance of the [PSC] and COREPER" • Additional coordination between HWPCI and "other thematic and geographical working parties and EU networks" as necessary
5	Decision-making on the use of EU Cyber Diplomacy Toolbox (p. 16f., 2023)	• Unless IPCR has been activated, "Council decision-making procedures apply" • In case of a decision on restrictive measures, involvement of the respective "competent preparatory bodies within the Council"
6	Implementation of the Cyber Diplomacy Toolbox	• "Member States and the EEAS [...] implement the measures following the guidance provided by the Council for their

115 Different steps and procedures may apply in instances where the IPCR is activated. The 2017 guidelines foresaw a 4-step-process comprised of (1) preparing a decision, (2) attributing a malicious cyber activity, (3) making a decision, and (4) following a decision (pp. 10-16, 2017).

	(p. 17, 2023)	attainment"
7	Cooperation with international partners (p. 17, 2023)	• EU may request "international like-minded partners [...] to support the joint EU diplomatic response to malicious cyber activities or conduct coordinated, and where desirable joint, response" • EU may consider supporting "international like-minded partners in their diplomatic activities", for instance, following "a request for a joint EU diplomatic response [...] by a partner"
8	Evaluation of the impact of the joint EU diplomatic response (p. 17f., 2023)	• Post-implementation: HWPCI "monitor[s] the situation and the effect of the measures" (supported by the EEAS and other EUIBAs) and keeps track of lessons learned
9	Continued discussion about maintaiingn a sustained engagement (p. 18, 2023)	• "Member States may request to revisit the relevant steps of the process"

In relation to attribution[116], the 2023 guidelines note the possibility of pursuing "coordinated political attribution at EU level" (p. 18, 2023) while emphasizing that "political attribution is a sovereign political decision of Member States taken on a case-by-case basis" (p. 18, 2023) and "not all measures require attribution" (p. 18, 2023). The guidelines note seven objectives for carrying out political attributions, among them "expos[ing] the specific malicious cyber activity or specific actor," "promot[ing] the UN framework for responsible state behaviour," and "discourag[ing] future malicious cyber activities" (p. 18, 2023). The guidelines further list ten elements for consideration by states when "discussing the appropriateness of coordinating political attribution, and [...] deciding whether and how to communicate about coordinated attribution, either privately or publicly" (p. 19, 2023). These elements, for instance, include the "ability to influence the behaviour of malicious actors in cyberspace," the "impact on the ongoing work of services such as law enforcement or intelligence services," the "likelihood and impact of a counter-response by any actor" and the "reputation and credibility of the EU" (p. 19, 2023).

The 2023 guidelines further note the importance of employing strategic (public) communication on EU action for attaining the EU's objectives and amplifying the effect of EU responses (p. 20f., 2023) and the added value of further exploring strengthened cooperation with non-EU countries, private sector entities, and

116 The guidelines define attribution "as a practice of assigning a malicious cyber activity to a specific state or non-state actor" (p. 18, 2023).

international organisations (pp. 24-26, 2023). Concerning EU-NATO cooperation[117], the 2023 guidelines stress "possible coordinated responses to malicious cyber activities [... and] seek[ing] potential synergies between the respective crisis management frameworks in the field of cybersecurity," among other fields for inter-institutional collaboration (p. 25, 2023). Once a year, Member States and involved EUIBAs commit to "test[ing their] response to scenarios developed on the basis of regular EU risk assessment" in the framework of an "annual dedicated Cyber Diplomacy Toolbox exercise" (p. 26, 2023).

— Council Conclusions on Malicious Cyber Activities

In its 2018 ⧉⧉ Council conclusions on malicious cyber activities, the Council "firmly condemns the malicious use of information and communications technologies (ICTs), including in Wannacry and NotPetya, which have caused significant damage and economic loss in the EU and beyond" (p. 2). EU Member States further stressed that "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts" (p. 3).

— Council Conclusions on Cyber Diplomacy

In February 2015, the Council adopted ⧉⧉ Council Conclusions on cyber diplomacy. EU Member States agreed that "the further development and implementation of a common and comprehensive EU approach for cyber diplomacy at global level" is "essential and crucial" (p. 4). The Conclusions lay out the following objectives and exemplary measures:

Table 33: Overview of Council Conclusions on Cyber Diplomacy

Objectives	Exemplary Specifications
Promotion and protection of human rights in cyberspace	• Council calls on EU and Member States "to promote and protect human rights and fundamental freedoms in cyberspace" and "actively contribute to the enforcement of international human rights obligations in cyberspace" (p. 5) • Council invites the promotion of implementation and better usage of the "EU Guidelines on the Freedom of Expression online and offline and of the EU Guidelines on Human Rights Defenders" (p. 6)
Norms of behaviour and	• Council "encourages the EU and Member States to focus efforts in a

117 For further information on EU-NATO cooperation, see also Eighth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.

application of existing international law in the field of international security	coherent and coordinated manner and contribute actively to the achievement of a global common understanding on how to apply existing international law in cyberspace and to the development of norms for responsible state behaviour in cyberspace" (p. 7)
Internet Governance	• Council emphasizes Internet Governance as "an integral part of the common and comprehensive EU approach for cyber diplomacy" (p. 8)
Enhancing competitiveness and the prosperity of the EU	• Council "invites the EU and its [Member States] to place specific emphasis on further promoting the EU digital single market and enhancing IT security, promoting digital trust and enabling greater use of ICTs and ICT driven growth" (p. 9)

Cyber capacity building and development	• Council "strongly encourages the EU and its Member States to
	  • develop a coherent and global approach to cyber capacity building" (p. 10) and
	  • "promote the Council of Europe Convention on Cybercrime internationally as the legal framework of reference for international cooperation in fighting cybercrime at a global level and support third countries to accede to the Convention" (p. 11)

Strategic engagement with key partners and international organisations	• Council "invites the EU and its Member States to
	  • ensure that the European activities in cyberspace and national policies, law and initiatives are designed in a way to allow for a coherent approach and avoid duplication" (p. 12),
	  • "share information on their bilateral cyber consultations" (p. 13), and
	  • "maintain close relations with the relevant international organisations where the major cyber developments are taking place" (p. 12)

Sanctions Regime

— Restrictive Measures Against Cyber-Attacks Threatening the Union or Its Member States

The European Union's sanctions regime[118] for "targeted restrictive measures to deter and respond to cyber-attacks[119] with a significant effect which constitute an external threat[120] to the Union[121] or its Member States[122]" (recital (2), Regulation

118 The horizontal cyber sanctions regime is included as one instrument within the EU's Cyber Diplomacy Toolbox.

119 "Cyber-attacks" are defined as "actions [which] are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned", that either involve "access to information systems", "information system interference", "data interference", or "data interception" (Art. 1(3) Council Decision 2019/797 and Regulation 2019/796). The four scenarios mentioned reflect the punishable offenses specified in Directive 2013/40. As part of the Decision's recital, the Council also notes that "targeted restrictive measures should focus on cyber-attacks [...] that are wilfully carried out" to "have a deterrent and dissuasive effect" (recital (8), Decision 2019/797).

2019/796) is based on two components: First, the Council of the EU decides to list particular natural or legal persons (provided for in ⬚ Council Decision 2019/797). Second, EU Member States implement the consequences of that listing within their jurisdiction (as provided for in ⬚ Regulation 2019/796). Sanctioned natural and legal persons are listed in the Council Decision's and Regulation's Annex.

The determination of whether an effect is deemed significant shall be guided by the following factors:

- "the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety;
- the number of natural or legal persons, entities or bodies affected;
- the number of Member States concerned;
- the amount of economic loss caused [...];
- the economic benefit gained by the perpetrator [...];
- the amount or nature of data stolen or the scale of data breaches; or
- the nature of commercially sensitive data accessed" (Art. 3 Decision 2019/797 and Art. 2 Regulation 2019/796).

EU Member States may decide to list:

- (a) natural persons who are responsible for cyber-attacks or attempted cyber-attacks;
- (b) natural persons who provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks;"
- or (c) other natural persons associated with persons of type (a) and (b) (Art. 4(1) Decision 2019/797).

Member States or the High Representative of the Union for Foreign Affairs and Security Policy may propose an initial listing or amend an existing listing. In turn, the Council must unanimously agree on any listing or amendment to it. Apart from specific proposals, the Council shall regularly review the list included in Annex I, at

120 External, in this respect, indicates that the 'cyber attacks' "(a) originate, or are carried out, from outside the Union; (b) use infrastructure outside the Union; (c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or (d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union" (Art. 1(2) Decision 2019/797 and Regulation 2019/796).

121 Threats to the EU may stem from operations "against its institutions, bodies, offices and agencies, its delegations to third countries or to international organisations, its common security and defence policy (CSDP) operations and missions and its special representatives" (Art. 1(5) Decision 2019/797 and Regulation 2019/796). In addition, the sanctions regime also provides for the possibility of using restrictive measures "in response to cyber-attacks with a significant effect against third States or international organisations", if doing so is "deemed necessary to achieve CFSP objectives" (Art. 1(6) Decision 2019/797 and Regulation 2019/796).

122 Threats to Member States may result from the targeting of critical infrastructures, "services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy [...]; transport [...]; banking; financial market infrastructures; health [...]; drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned", "critical State functions", the "storage or processing of classified information", or governmental CERTs (Art. 1(4) Decision 2019/797 and Regulation 2019/796).

least annually. Any listing shall explicitly not be understood to constitute an "attribution of responsibility for cyber-attacks to a third State," as this would remain "a sovereign political decision taken on a case-by-case basis" (recital (9) Decision 2019/797).

The consequences of a listing may be travel restrictions as well as implications for the funds and economic resources of these persons. Specifically, EU Member States shall

- (i) "prevent the entry into, or transit through, their territories" (Art. 4 Decision 2019/797);
- (ii) freeze "all funds and economic resources belonging to, owned, held or controlled by" the listed persons or entities (Art. 5(1) Decision 2019/797);
- and (iii) not make "available directly or indirectly [of funds or economic resources] to or for the[ir] benefit" (Art. 5(2) Decision 2019/797).

Certain exceptions exist to the application of these measures (see further Art. 4(2), (3), (4), (6), (7) and Art. 5(3) and (4) Decision 2019/797 and Art. 4, 5, 6, 7 Regulation 2019/796) that permit derogation from Member States in particular instances.[123] To enforce these measures, Member States must designate competent authorities at the national level. Union-level cooperation shall be ensured so that Member States and the Commission share with each other when any of such measures are taken.

The sanctions regime also has an external dimension, as the Decision formulates the Union's objective to "encourage third States to adopt [similar] restrictive measures" (Art. 9 Council Decision 2019/797).

Cyber Defence

— Council Decision on a European Union Partnership Mission in Moldova

In April 2023, the Council, via its ⬚ Decision 2023/855, decided to establish a European Union Partnership Mission in the Republic of Moldova (EUPM Moldova) as a civilian mission under the umbrella of the CSDP upon request by the Moldovan Prime Minister. The EUPM Moldova predominantly comprises seconded experts of Member States, EUIBAs, or the EEAS. The EUPM Moldova's objective is "enhancing the resilience of the security sector of the Republic of Moldova in the

123 Examples of such grantable exemptions relate to the entry of own nationals (Art. 4 (2) Decision 2019/797) or "on the grounds of urgent humanitarian need" (Art. 4(6) Decision 2019/797).

areas of crisis management and hybrid threats, including cybersecurity" (Art. 2(1)). Of relevance to cybersecurity, the EUPM Moldova's mandate includes the support of crisis management structures and strategic advice "on the development of strategies and policies [...] for enhancing cybersecurity and for the protection of classified information" (Art. 2(2)).

— EU Policy on Cyber Defence

In November 2022, the Commission and the HR/VP put forward a ⧉ Joint Communication on the EU Policy on Cyber Defence with the aim of boosting the EU's cyber defence capabilities to enhance the Union's ability to prevent, detect, defend against, recover from, and deter malicious cyber activities aimed at the EU and its Member States. The Joint Communication builds on the EU Cyber Defence Policy Framework (CDPF) from 2018 (as well as its predecessor from 2014). The 2018 CDPF had for the first time elevated cyberspace to being "the fifth domain of operations" (p. 2). Via its ⧉ Council Conclusions on the EU Policy on Cyber Defence, adopted in May 2023, the Council reacted to the Commission's and HR Joint Communication.

In a general vein, the Council encourages Member States to "further develop their own capabilities to conduct cyber defence operations, including when appropriate proactive defensive measures to protect, detect, defend and deter against cyberattacks" (p. 10) and note "the need to invest in our mutual assistance under Article 42(7) TEU as well as the solidarity clause under Article 222 TFEU" (p. 7). In accordance, the Council regards the EU Policy on Cyber Defence as an enabler for "the EU and its Member States to strengthen their ability to protect, detect, defend and deter, making appropriate use of the whole range of defensive options available to the civilian and military communities for the broader security and defence of the EU, in accordance with international law, including human rights law and international humanitarian law" (p. 3).

The Joint Communication and Council Conclusions are both built on four pillars. Table 34 provides a non-exhaustive overview of specific objectives and exemplary activities and measures as contained in each document:

Table 34: Overview of Joint Communication and Council Conclusions on the EU Policy on Cyber Defence

Pillar	Document	Exemplary Provisions
Act together for a stronger	Joint Communication	(i) Strengthening common situational awareness and coordination within defence community: • Presentation of a proposal for an an EU Cyber Defence

cyber defence		Coordination Centre (EUCDCC) by the HR/VP to "support[…] enhanced situational awareness within the defence community" (p. 4)
		• Further development and strengthening of the EU Cyber Commanders Conference (p. 5)
		• Establishment of an "operational network for milCERTs (MICNET)" with the support of the EDA (p. 5)
		(ii) Enhancing coordination with civilian communities:
		• Cooperation between MICNET and CSIRTs Network in the future (p. 5)
		• Cooperation between the EU Cyber Commanders Conference and EU-CyCLONe (p. 5)
		• "Promot[ion of] the deployment of an EU infrastructure of Security Operation Centres (SOCs)" (p. 6)
		• As part of the Cyber Solidarity Initiative
		  • HR/VP will "explore possibilities for the expansion of the concept of cyber rapid reaction teams (CRRT)" together with the Commission and Member States (p. 7)
		  • "Testing of essential entities operating critical infrastructure for potential vulnerabilities based on EU risk assessments" (p. 7)
		  • "Gradual set-up of an EU-level cyber reserve with services from trusted private providers" (p. 7)
		• New EDA project on cyber defence exercises (CyDef-X, p. 7)
		• HR/VP will "propose […] options for further strengthening the EU Cyber Diplomacy Toolbox"

	Council Conclusions	• Council welcomes
		  • "initiative to further develop the EU Cyber Commanders Conference to be organised by each Presidency of the Council of the EU, with the support of the European Defence Agency (EDA) and participation of the European External Action Service (EEAS)" (p. 5)
		  • "establishment and looks forward to reaching the initial operational capability by mid-2024 of the EU Military Computer Emergency Response Teams Operational Network (MICNET)" (p. 6)
		  • "further development of PESCO CRRTs' capability, national cyber response teams, and, where appropriate, additional incident response capabilities" (p. 7)
		  • "proposal to integrate the proof of concept, if successful as an information coordination centre, from 2025 onwards, into an EU Cyber Defence Coordination Centre (EUCDCC)" (p. 8)
		• Council invites
		  • "EU and its Member States to strengthen their capabilities to defend and secure CSDP missions and operations" (p. 6)
		  • EU-CyCLONe and EU Cyber Commanders Conference "to identify possible ways to cooperate and benefit from a joint military and civilian perspective" (p. 5)

		• "Member States, through their competent authorities, to continue to contribute to EU INTCEN's, EUMS Intelligence Directorate's and Member States work under the Single Intelligence Analysis Capacity (SIAC)" (p. 8)
		• Council encourages
		  • HR/VP and Commission "to reduce complexity in the field of cyber, avoid unnecessary duplication and ensure cooperation and synergies with existing initiatives" (p. 4)
		  • Member States "to further explore and strengthen civil-military national coordination mechanisms" (p. 4)
		  • the EDA "to explore, in close cooperation with Member States and the EEAS, how CyDef-X could further support exercises such as CYBER PHALANX, including on mutual assistance under Article 42(7) TEU and solidarity clause under Article 222 TFEU, as well as with the Commission and ENISA as regards civilian exercises" (p. 9)
		• Council "strongly encourages to create an effective cooperation and coordination mechanism between the two networks at an appropriate time between MICNET and CSIRTs Network" (p. 6)
		• Council calls on HR/VP "to present a concept and roadmap for the establishment of the EUCDCC" (p. 8)

Secure the EU defence ecosystem	Joint Communication	(i) Enhancing the cyber resilience of the defence ecosystem: • "Further development of the EU Operation Wide Area Network" (p. 9) • Support for Member States in the "development of non-legally binding recommendations for the defence community, inspired by the" NIS 2 Directive by the HR/VP (with Commission support) (p. 10) • Reference to Cyber Resilience Act proposal (p. 10) • Development of "risk scenarios for digital infrastructure security" by HR/VP, Commission and NIS Cooperation Group (particularly on "cybersecurity in the energy, telecoms and transport sectors, and space" and "communications infrastructure and networks in the EU", p. 10) • "Measures to improve the robustness and cyber resilience of space infrastructures and related services and to deter and respond to any threats on sensitive space systems and services in the EU" through an EU Space Strategy for Security and Defence (p. 11) • Consideration of an "EU cybersecurity certification scheme for companies providing services to defence industry" (p. 11) (ii) Ensure EU cyber defence interoperability and coherence of standards: • "Develop[ment of] recommendations on a set of EU cyber defence interoperability requirements" by EDA and EUMS (p. 12)
	Council Conclusions	• Council invites

		• EDA, supported by Commission and EEAS, "to assist Member States in developing non-legally binding voluntary recommendations inspired by NIS2 to increase cybersecurity in the defence community" (p. 10)
		• Commission, "in close collaboration with the ECCC, where appropriate, to further support the development of a strong, agile, globally competitive and innovative European cyber defence industrial and technological base, including small- and medium-sized enterprises (SMEs), through further investments, and policy actions" (p. 11)
		• "EDA and the EU Military Staff to work on a set of EU cyber defence interoperability requirements" (p. 11)
		• Council calls for
		  • the timely development of "recommendations based on the mapping of existing tools for secure communication in the cyber domain" by Commission (p. 12)
		  • "risk scenarios to be considered by all relevant actors in risk assessment processes, as well as in the development of cyber exercises" (p. 12)

Invest in cyber defence capabilities	Joint Communication	(i) Develop full-spectrum state-of-the-art cyber defence capabilities: • Consideration of "developing a set of voluntary commitments for the development of national cyber defence capabilities" by Member States (p. 12) • Further support for "responsive operations and cyber operations capabilities" through the EDF (p. 13) • Development of a "cyber domain operations implementation plan" by the EUMS "to provide an overview of the state of play of the implementation of cyber defence capabilities [and] provide support to Member States to better align their efforts and activities" (p. 13) • "Invest[ments] in post-quantum cryptography" (p. 13) • Preparation of "a technology roadmap for critical cyber technologies" (p. 14) (ii) Agile, competitive and innovative European defence industry: • Establishment of "an industry dialogue with the purpose of developing the EU's cyber defence industry" (p. 16) • "In-depth mapping of EU defence industrial manufacturing capabilities" by HR/VP and Commission (p. 16) (iii) EU cyber defence workforce: • Cyber Skills Academy initiative (p. 17) • "Further development of the ESDC Cyber Education, Training, Exercises and Evaluation (ETEE) Platform" (p. 17) • Development of a "cyber defence skills certification framework" by the ESDC (p. 17)

	Council Conclusions	• Council welcomes
		  • "the intention to develop a technology roadmap for critical cyber technologies by the Commission in cooperation with EDA and the ECCC" (p. 14)
		  • "the Cybersecurity Skills Academy initiative, which may also benefit the cyber defence workforce" (p. 15)
		  • "the proposal for a cyber defence skills certification framework" (p. 15)
		• Council "supports the development of a set of voluntary commitments for the further development of national cyber defence capabilities" (p. 13)
		• Council invites
		  • "Member States to exchange information on best practices to develop skilled cybersecurity professionals, leveraging the synergies between military, civilian and law enforcement initiatives" (p. 15)
		  • HR/VP, "in his capacity as Head of the [European Security and Defence College] ESDC to develop [a cyber defence skills certification framework], in cooperation with the EEAS, the Commission and Member States, by leveraging civilian initiatives" (p. 15)
		• Council "encourages the European Cybersecurity Competence Centre (ECCC) and EDA to develop a working arrangement" (p. 14)
		• Council calls on
		  • "Member States and EDA to use the opportunity of the revision of the Capability Development Plan to set a high level of ambition when it comes to the development of collaborative cyber defence at EU level" (p. 13)
		  • "ESDC, with the support and expertise of EDA and ENISA, to consider options for enhancing the exchange of best practices and further synergies between the military and civilian fields regarding training and the development of cyber-specific defence skills" (p. 15)

Partner to address common challenges	Joint Communication	(i) Cooperation with NATO: • Continued exchange "on the military conceptual framework concerning the integration of cyber defence aspects into the planning and conduct of military CSDP missions and operation" (p. 19) • Promotion of "technical and procedural interoperability of cyber defence capabilities" (p. 19) • Accessibility of ESDC training courses for NATO staff (p. 19) • Facilitation of "NATO staff participation in cyber exercises and crisis management exercises with cyber elements" (p. 19) (ii) Cooperation with like-minded partners: • Systematic integration of cyber defence in "existing and future cyber as well as security and defence dialogues" (p. 19)

		• United States (p. 19) • Ukraine (p. 19) (iii) Cyber defence capacity building support for partner countries: • Continued supportive efforts, inter alia, under the European Peace Facility, particularly towards candidate and Neighbourhood countries (p. 20)

	Council Conclusions	• Council "invites the High Representative, also in his capacity as Head of EDA, and the Commission to further strengthen, deepen and expand the partnership in the cyber domain with NATO" (p. 17)
		• Council calls
		  • on HR/VP and Commission "to strengthen and advance its cooperation and explore mutually beneficial and tailored partnerships on cyber defence policies, including on cyber defence capacity building through the European Peace Facility (EPF)" and by including cyber defence "as an item [in] the EU's dialogues and consultations on cyber, to the overall security and defence consultations with partners" (p. 16)
		  • "for links on relevant levels to be established between EU-NATO on training, education, situational awareness, exercises and R&D platforms, and to seek potential synergies between the respective voluntary commitments for the developments of national cyber defence capabilities and the crisis management frameworks, the protection of critical infrastructure, and the enhancement of exchanges of situational awareness, coordinated responses to malicious cyber activities as well as capacity building efforts in third countries" (p. 17)

In July 2023, the Council approved an Implementation Plan for the EU Policy on Cyber Defence, which remains confidential. The Commission and the HR/VP submit an annual report to the Council to "monitor and assess the progress" (p. 22, Joint Communication). of implementing the policy. The Council Conclusions invite Member States to report in this respect from the second quarter of 2024 onwards.

— European Peace Facility

In December 2021, the Council decided on establishing the European Peace Facility (EPF) via ﷺ Council Decision 2021/509. The EPF permits the "financing by Member States of Union actions under the [...] CFSP to preserve peace, prevent conflicts and strengthen international security" (Art. 1(1)). Until 2027, more than 12 billion euros can be spent under the EPF. In particular, EPF actions relate to "common costs of Union operations [... that have] military or defence implications and which [...] cannot be charged to the Union budget" and "assistance measures"

(Art. 1(2)). The latter can be "actions to strengthen the capacities of third States and regional and international organisations relating to military and defence matters" as well as "support to military aspects of peace support operations led by a regional or international organisation or by third States" (Art. 1(2), point (b)). There are exceptions, but the standard way of initiating an EPF action is through the adoption of a Council decision. The management of the EPF rests with its Facility Committee, in which each Member State is represented. A few assistance measures financed under the EPF also include cyber defence components. For instance, EPF assistance measures directed toward Georgia and the Republic of Moldova finance "cyber-defence equipment" (Art. 1(3), point (e), Decision 2023/921 and Art. 1(3), point (d), Decision 2023/920), among other types of equipment. In support of the Ukrainian Armed Forces, an EPF assistance measure funds the delivery of "cyber defence units" (Art. 1(3), point (d), Decision 2021/2135).[124]

— European Union Military Vision and Strategy on Cyberspace as a Domain of Operations

In 2021, the EU Military Committee (EUMC) agreed on a ﷺ "European Union Military Vision and Strategy on Cyberspace as a Domain of Operations". Among the document's objectives are "set[ting] the framework conditions and describ[ing] the ends, ways and means needed to use cyberspace as a domain of operations in support of EU CSDP military operations and missions" and "integrat[ing] cyberspace into all aspects of EU CSDP military operations and missions" (p. 5). The elaborated EU vision on cyberspace as a domain of operations is comprised of three ambitions: the EU

1. "is able to accomplish its objectives in the cyberspace domain as effectively as it does in the other domains in order to execute EU CSDP military operations and missions;"
2. "has effectively integrated cyberspace into EU CSDP military operations and missions planning and conduct, established an effective and consistent cyber resilience and cyber deterrence against potential adversaries, including international cooperation with partners in support of CD [cyber defence] of EU military CSDP;"
3. and "has achieved effective civil-military synergies in EU CSDP" (p. 10).

The document identifies 21 means in terms of capabilities and capacities to put the vision and strategic objectives into action:

Table 35: Means and Exemplary Actions As Specified in the European Union Military Vision and Strategy on Cyberspace as a Domain of Operations

124 See also Council Decisions 2022/1093 and 2022/2352.

Mean	Exemplary Actions
1: Cyberspace Cultural Adoption	• Establishment of "broader acceptance that EU CSDP stakeholders must be prepared to continuously adapt and respond to the evolving cyber threat landscape" (p. 12) • "initiative to anticipate where critical EU vulnerabilities lie" (p. 12)
2: Implementation of Cyberspace Operations (CO) Capabilities	• Establishment of an "EU military CSDP capability coordination and transition instrument to coordinate and expedite the implementation of existing as well as newly researched and developed CO capabilities" (p. 13)
3: Integration of Cyberspace into Advance and Crisis Planning	• Conceptual integration of "cyberspace implications in CSDP crisis response planning, including the establishment of a cyber-threat early warning mechanism" (p. 13)
4: Cyber Defence Management & Evaluation Regime	• Establishment of a "standardized and consistent cyber risk management organization and process, including a systematic assessment of system vulnerabilities, attack vectors and entry points for cyber-attacks and cyber incidents" (p. 13)
5: NIS Directive for the Military Domain	• Improved coordination with ENISA • Needs-based analysis of how implementing particular NIS components can "improve the cyber resilience and responsiveness of EU CSDP military operations and missions" (p. 14)
6: Strong EU Cyberspace Skills Base	• Development of an "EU Cyberspace ETE [Education, Training and Exercise] coordination capability" (p. 15)
7: Information Sharing	• Requirement of a "permanent and federated cyber information sharing and fusion framework, together with applicable processes, procedures and technical capabilities" (p. 15)
8: Cyberspace Situational Awareness and Situational Understanding (CSASU)	• Requirement of a "commonly recognized Cyber Defence Operational Picture (CDOP)" (p. 16) • "emphasis on push instead of pull of information and the ability to quickly assess the impact on the operations/missions and to react accordingly" (p. 16)
9: Cyber Resilience	• Establishment of a "coordinated operation and mission mapping, joint planning and risk management as well as a common recognized CDOP [Cyber Defence Operational Picture]" (p. 16) • "standardized certification of security services and products" (p. 16)
10: Protection and Defence of Military Networks and Systems	• Fostering and effective use of "EU MilCERT cooperation" (p. 17) • Set up and maintenance of "Cyber Rapid Response Teams (CRRTs)" (p. 17)
11: Military Organizational Structures	• Establishment of a "standing and centralized EU military cyber coordination element" (p. 17)
12: Interoperability	• Full compliance of all CSDP networks with the multi-national Federated Mission Networking (FMN) Framework Initiative

13: Cyber Deterrence	• Development and implementation of "improved capabilities and capacities, standardized procedures for detection and investigation as well as effective CD capabilities and mechanisms"
14: Cyber Incident Reporting and Response	• "Combination of a standardized and comprehensive ICT service management and a cooperation framework of static and deployable security operation capabilities across all EU CSDP military operations and missions" (p. 18)
15: Cyberspace Personnel	• Deployment of "sufficient personnel resources for EU CSDP military operations and missions, which understand the implications of cyberspace and take responsibility each in its individual role" (p. 19)
16: Cooperation with International Partners	• "Deepening of the cooperation in cyberspace between the EU and NATO" (p. 19)
17: Military Conceptual Framework	• Development of "new military concepts [...] as part of the EU Conceptual Development Implementation Programme (CDIP)" "when necessary" (p. 19)
18: Civil-Military Cooperation and Harmonization	• Harmonization of "civilian and military elements of cyberspace wherever feasible" (p. 20) • Strengthening of "civil-military synergies in cybersecurity and CD" (p. 20)
19: Collaboration with industry, academia and the cybersecurity Market in EU	• Ensuring "strong collaboration with these significant EU players" (p. 20)
20: Research and Technology	• Leveraging "existing and emerging military Cyber Research Agendas and their Technology Building Blocks" (p. 20)
21: Capability Development	• "Foster[ed] interoperability between the civilian cybersecurity initiatives, and the cyber defence initiatives under the PESCO projects, the European Defence Fund (EDF), the Coordinated Annual Review on Defence (CARD) and the Capability Development Plan (CDP)" (p. 21)

The European Union Military Staff (EUMS) shall regularly report to the EUMC about the implementation of the vision and strategy.

— Permanent Structured Cooperation (PESCO)

In December 2017, the Council decided to establish the Permanent Structured Cooperation (PESCO) via its ﷺ Decision 2017/2315. The PESCO aims to "jointly develop defence capabilities and make them available for EU military operations."[125] Art. 42(6) and Art. 46 of the Treaty of the EU provide PESCO's legal basis. PESCO projects offer participating EU Member States the opportunity to collaboratively plan, develop, and invest in shared capability projects. Relevant

capabilities are identified based on the Capability Development Plan (CDP)[126] and the Coordinated Annual Review on Defence (CARD).[127] Once Member States are involved in particular PESCO projects, resulting commitments are legally binding. Each participating Member State must annually provide co-participating Member States with a National Implementation Plan. The financing of particular PESCO projects may be provided by the European Defence Fund (EDF).[128] Examples of PESCO-projects in the area of cyber defense are:

Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRTs)	The goal of the CRRT project is the development of a cyber capability that could be deployed "as a response to cyber incidents and crises as well as a preventative measure [...] in time of need" (Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: About). The CRRT PESCO project is coordinated by Lithuania, with Belgium, Croatia, Estonia, Netherlands, Poland, Romania, Slovenia, and Denmark as participating Member States. Finland, France, Greece, Italy, and Spain are observers. • ⁂ March 2018: Council Decision establishing the list of projects to be developed under PESCO (2018/340)
Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)	The CTIRISP PESCO project works on the "sharing of cyber threat intelligence through a networked Member State platform" (Permanent Structured Cooperation: Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)). The project is coordinated by Greece, with the further participation of Cyprus, Hungary, Ireland, Italy and Portugal. • ⁂ March 2018: Council Decision establishing the list of projects to be developed under PESCO (2018/340)
Cyber and Information Domain Coordination Center (CIDCC)	The CIDCC project seeks to develop a permanent, multinational military element in which situational pictures from cyber and information space can be compared and evaluated. On that basis, it develops its own analyses and recommendations, which can be introduced in the planning and management of EU operations and missions. The project will be completed in 2026 upon its transfer into a standing European CIDCC. The project is coordinated by Germany, with the participation of France, Netherlands, and Hungary. Belgium, Estonia, Greece, Italy, Austria, Poland, Portugal, Slovakia, Spain, Czech Republic, Cyprus, and Ireland are observers. [For further information see Permanent Structured Cooperation: Cyber and Information Domain Coordination Center (CIDCC) and German Federal Ministry of Defence (2023): Cyber and Information Domain Coordination Centre (CIDCC)] • ⁂ November 2019: Council Decision amending and updating Decision (CFSP) 2018/340 establishing the list of projects to be developed under PESCO (2019/1909)
EU Cyber Academia and	The EU CAIH project seeks to "add value by enhancing the creation of an innovative web of knowledge for cyber defence and cyber security education and training" (Permanent Structured Cooperation: EU Cyber Academia and

125 European Union External Action Service: Permanent Structured Cooperation (PESCO).

126 See further European Defence Agency: Capability Development Plan.

127 See further European Defence Agency: Coordinated Annual Review on Defence.

128 The EDF, established in 2021 until 2027, provides financial assistance to "foster the competitiveness, efficiency and innovation capacity of the European defence technological and industrial base (EDTIB) throughout the Union" (Art. 3(1) Regulation 2021/697). Under the EDF's umbrella, around 8 billion euros can be used to "support collaborative research [in an effort to] boost the performance of future capabilities" and "support the collaborative development of defence products and technologies" (Art. 3(2), Regulation 2021/697). The EDF is implemented by the Commission and works on the basis of annual work programmes that are developed within a dedicated EDF Programme Committee with the support of the EDA and the EEAS.

Innovation Hub (EU CAIH)	Innovation Hub (EU CAIH)). Inter alia, it is envisioned to provide a "coordination point for future cyber education, training and exercises" (ibid.). It is coordinated by Portugal, with the participation of Spain and Romania. • ⁂ November 2019: Council Decision amending and updating Decision (CFSP) 2018/340 establishing the list of projects to be developed under PESCO (2019/1909)
Cyber Ranges Federations (CRF)	The objective of the CRF PESCO project is to "federat[e] existing national Cyber Ranges [1] into a larger cluster with more capacity and unique services" to strengthen the "European Cyber Ranges capability" (Permanent Structured Cooperation: Cyber Ranges Federations (CRF)). The project is coordinated by Estonia, with the participation of Austria, Bulgaria, Finland, France, Italy, Latvia, and Luxembourg. • ⁂ November 2021: Council Decision amending and updating Decision (CFSP) 2018/340 establishing the list of projects to be developed under PESCO (2021/2008) [1] The U.S. National Institute of Standards and Technology (NIST) defines a cyber range as a "Realistic simulation of the internet, systems, applications, and devices in a training environment" (U.S. National Institute of Standards and Technology (2018): Cyber Ranges).

Hybrid Threats and Campaigns

— Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns

EU policies about hybrid threats also, in part, address issues of relevance to cybersecurity. In its 2022 ⁂ Council conclusions on a Framework for a coordinated EU response to hybrid campaigns, the Council stresses that "malicious cyber activities are often a key element of hybrid campaigns" (paragraph 19). With respect to the EU Cyber Diplomacy Toolbox, EU Member States underline "the need for relevant Council bodies, the High Representative and the Commission to encourage cooperation and synergies in the implementation of measures and actions decided on under this Framework [...] when and where appropriate" (paragraph 19).

— Joint Communication "Increasing resilience and bolstering capabilities to address hybrid threats"

Cybersecurity considerations play a role in three areas of action of the Commission's and the HR/VP's 2018 ⁂ Joint Communication "Increasing resilience and bolstering capabilities to address hybrid threats". In the area of situational awareness, the Communication notes the expansion of the EU Hybrid Fusion Cell with "cyber analytical components" by the HR/VP (p. 5). In relation to strategic communication, the Communication highlights the Commission's efforts to "hold high-level events [...] with Member States and relevant stakeholders, [...] to promote

best practices and guidelines on how to prevent, mitigate and respond to cyber-enabled and disinformation threats to elections" (p. 7). The Communication includes a dedicated cybersecurity-related area of action, namely "building resilience and deterrence in the cybersecurity sector" (p. 7). In this context, the Communication, inter alia, underlines close cooperation by the Commission and the HR/VP to "advance the cyber aspects of EU-wide crisis management and response mechanisms" (p. 9). The Communication invites Member States to "continue their work on attribution of cyber-attacks and the practical use of the cyber diplomacy toolbox to step up the political response to cyber-attacks" (p. 9).

— Joint Communication "Joint Framework on Countering Hybrid Threats"

In 2016, the Commission and the High Representative issued a ⁂ Joint Communication "Joint Framework on countering hybrid threats". The Communication describes hybrid threats as a "mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare" (p. 2). Concerning cybersecurity, the Communication, inter alia, addresses the need for enhanced CSIRT cooperation (p. 10), cooperation with industry "to develop and test technologies to better protect users and infrastructures against cyber aspects of hybrid threats" (p. 11), issuing "guidance to smart grid asset owners to improve cybersecurity of their installations" (p. 11), "promot[ing] and facilitat[ing] threat information-sharing platforms and networks" (p. 12) in the financial sector, and "examin[ing] how to respond to hybrid threats, in particular those concerning cyber-attacks across the transport sector" (p. 12).

Development Cooperation and Cyber Capacity-Building

— EU Global Gateway

Via the ⁂ EU Global Gateway (2021), the EU seeks to "channel EU spending on global infrastructure development" in a "security-focused" manner, among other principles (p. 4). To this end, "Global Gateway projects will invest in infrastructure to plug vulnerabilities [...] and build capacity in the face of [...] cyber or hybrid threats" (p. 4).

— Global Europe

In June 2021, the EU established the Neighbourhood, Development and International Cooperation Instrument (Global Europe) until 2027 via ﷺ Regulation 2021/947. The Global Europe Instrument can implement programmes of a geographic or thematic nature and provides funding for rapid response actions (Art. 4(1)). While not representing a particular focus of the instrument, both types of programmes also include cybersecurity considerations:

- *Geographic programmes* shall facilitate "country and multi-country cooperation" in the following regions: the European Neighbourhood [1], Sub-Saharan Africa, the Asia-Pacific, Americas and the Caribbean. In the context of the objective of promoting "inclusive and sustainable economic growth and decent employment," geographical programmes shall, inter alia, "promot[e] accessible, affordable, inclusive, reliable and secure digital connectivity [...and] address[...] cybersecurity, data privacy and other regulatory issues linked to digitalisation" (Annex II). As a contribution to "peace, stability and conflict prevention," activities may also involve "supporting capacity-building in cyber security [and] resilient digital networks" (Annex II). ﷺ Commission Delegated Regulation 2021/1530 supplements the Regulation by designating "specific objectives and priority areas of cooperation" (Art. 1). Cybersecurity-related priority areas of cooperation were identified for the following regions:

Table 36: Cybersecurity-Related Priority Areas of Cooperation of Global Europe Geographic Programmes

Region	Objectives	Cybersecurity-Related Priority Areas of Cooperation
Neighbourhood East	"investing in democracy, good governance, peace and security, the rule of law and justice" (p. 4)	"[...] stepping-up cooperation in countering hybrid threats and disinformation, ensuring cyber security and combating cyber crimes" (p. 4)
	"investing in resilient digital transformation" (p. 5)	"strengthening cyber resilience" (p. 5)
Neighbourhood South	"cooperating on peace and security" (p. 3)	"stepping-up cooperation on [...] addressing cybersecurity, cybercrime and hybrid threats" (p. 3)
The Americas	"digital transformation and innovation" (p. 15)	"Supporting standardisation and policy cooperation addressing cybersecurity [...]" (p. 15)

[1] Annex I specifies what countries the EU considers as 'neighborhood countries'.

- As one of four areas, *thematic programmes* shall center around activities in the area of "peace, stability and conflict prevention," also to support the mitigation of "global and trans-regional [emerging] threats" through "technical and financial assistance". In relation to cybersecurity, such assistance shall enhance "the capacity of law

> enforcement and judicial and civil authorities involved in the fight against [...] cyber-crime" and address "threats to public spaces, critical infrastructure, including [...] cybersecurity" (Annex III).

— Council Conclusions on EU External Cyber Capacity Building Guidelines

The 2018 ﷺ Council Conclusions on EU External Cyber Capacity Building Guidelines[129] underscore that "external cyber capacity building [CCB] initiatives by the EU and its Member States should prioritise addressing cybercrime and increasing cybersecurity in partner countries and regions, with a focus on reforms across the main pillars of cyber resilience, namely by

- supporting an overarching strategic framework,
- promoting legislative reforms and increasing the capacities of the criminal justice system,
- developing and increasing incident management capabilities,
- developing education, professional training and expertise in this field and
- promoting cyber hygiene and awareness as well as a culture of security assessment of digital products, processes and services (p. 8)."

Both the EU and Member States shall draw on the NIS Directive "as inspiration for the development of cybersecurity legislation in partner countries" (p. 9). Furthermore, every external CCB activity shall take into account the "EU's core values and principles for cybersecurity" (p. 7) and build on development cooperation-related lessons learned to elevate their "effectiveness and sustainability (p. 7):

Table 38: Overview of EU External Cyber Capacity Building Guidelines

Values and Principles (p. 7)	Lessons Learned (p. 7f)
• based on "understanding that the existing international law and norms apply in cyberspace," • "rights-based and gender-sensitive by design," • foster "the democratic and efficient multi-stakeholder internet governance model," • encourage "the principles of open access to the internet for all", while "not	• provide for "ownership of the development priorities in relation to cyber resilience by the partner countries," • emphasize "sustainable results through the promotion of broader policy, legal and technical reform processes instead of ad hoc, one-off activities," • encourage partnerships, specifically "the participation of all stakeholders,"

129 The EU funded the development of operational guidance on international cyber capacity building that were published in 2023 and 2018 respectively.

undermin[ing] the integrity of infrastructure, hardware, software and services," • and implement "a shared responsibility approach" between public and private sector bodies, as well as involved citizens	• and assure that every action is guided by "trust, transparency, accountability and shared responsibility"

Support to Other International Organizations

— International Atomic Energy Agency

Through ⁂ Council Decision 2024/656, the Council decided to continue supporting the International Atomic Energy Agency (IAEA) in specific areas guided by three objectives. One of the three objectives aspires to "build[...] capacity to strengthen nuclear security" (Art. 1(3), point (c)). As one of six components under the objective, this also includes "capacity building in computer security" (p. 7) through the provision of "international, regional and national training courses" (p. 8) on cyber and IT security for nuclear security professionals. These trainings shall be conducive to "gaining enhanced information and computer security capabilities at the State and facility levels to support the prevention and detection of, and response to, computer security incidents that have the potential to either directly or indirectly adversely impact nuclear safety and security" (p. 8). Whereas the HR/VP holds the responsibility for the overall implementation of the Decision, the technical implementation rests with the IAEA (Art. 2). This Decision builds upon prior Decisions outlining support actions for the IAEA that have also encompassed issues of cyber and information security (see further ⁂ Council Decision 2013/517 and ⁂ Council Decision 2020/1656).

— Organization for the Prohibition of Chemical Weapons

Through its ⁂ Decision 2021/1026, the Council decided to support the Cyber Security and Resilience and Information Assurance Programme of the Organization for the Prohibition of Chemical Weapons (OPCW) through three types of activities, facilitating the:

- "operationalisation of an enabling environment for ongoing cyber security and resilience efforts within multi-site OPCW operations;"
- "designing of customised solutions for on-premises and cloud-based system integration and configuration with OPCW ICT systems and privileged access management (PAM) solutions;"
- and "initiation and testing of PAM solutions" (Art. 1(2)).

Whereas the HR/VP holds the responsibility for the overall implementation of the

activities, the technical implementation rests with the OPCW's own Technical Secretariat (Art. 2). A bit more than two million euros were dedicated for the realization of the project. The Decision expires on 30 August 2024.

Policy Area 8: Cybersecurity of EU Institutions, Bodies and Agencies

8

Deep Dive: Regulation 2023/2841

⬩⬩ Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (2023/2841)
Link: data.europa.eu/eli/reg/2023/2841/oj
Entry into force: 7 January 2024
Previous legislation: NA
Subsequent documents of relevance: NA
Objective (Art. 1): "achieve a high common level of cybersecurity within Union entities"
Subject matter (Art. 1) "This Regulation lays down measures [...] with regard to: • (a) the establishment by each Union entity of an internal cybersecurity risk-management, governance and control framework [...]; • (b) cybersecurity risk management, reporting and information sharing; • (c) the organisation, functioning and operation of the Interinstitutional Cybersecurity Board [...], as well as the organisation, functioning and operation of [CERT-EU]; • (d) the monitoring of the implementation of this Regulation"
Actors established/regulated by Regulation 2023/2841: • Interinstitutional Cybersecurity Board (IICB, Art. 10-12) [see further Chapter 13] • CERT-EU (Art. 13-18) [see further Chapter 13]
Deep Dive Structure → Cybersecurity Measures → Information-Sharing, Reporting, Incident Response and Management → Compliance → Review

As somewhat an equivalent to the obligations stipulated for essential and important entities in the NIS 2 Directive, Regulation 2023/2841 lays down cybersecurity-related obligations that must be implemented by every EU institution,

body, or agency.[130] According to the Regulation, the "highest level of management of each Union entity shall be responsible for [its] implementation" (Art. 6(5)).

Overviews of the relevant provisions on CERT-EU and the Interinstitutional Cybersecurity Board (IICB) are covered within their actor profiles in Chapter 13.

Cybersecurity Measures

The Regulation foresees that every Union entity[131] must put in place an "internal cybersecurity risk-management, governance and control framework" (Art. 6), conduct "cybersecurity maturity assessments" (Art. 7), undertake "cybersecurity risk management measures" (Art. 8), and develop a "cybersecurity plan" (Art. 9). For each of these measures, the IICB is tasked with drafting guidelines that Union entities "shall take into account" (Art. 5). Before drafting these guidelines, the IICB shall consult ENISA and obtain guidance by CERT-EU.

EUIBAs should establish the **framework** following an "initial cybersecurity review" (Art. 6(1)). The ambit of the framework shall be "the entirety of the unclassified ICT environment of the Union entity concerned, including any on-premises ICT environment, operational technology network, outsourced assets and services in cloud computing environments or hosted by third parties, mobile devices, corporate networks, business networks not connected to the internet and any devices connected to those environments" (Art. 6(2)), for which it shall put in place

- "internal cybersecurity policies, including objectives and priorities, for the security of network and information systems," and
- "roles and responsibilities of the Union entity's staff tasked with ensuring the effective implementation of this Regulation" (Art. 6(3)).

Under this provision, EU entities are also obliged to ensure that "effective mechanisms [are] in place to ensure that an adequate percentage of the ICT budget is spent on cybersecurity" (Art. 6(7)). The framework also includes the designation of a "local cybersecurity officer" (or equivalent) to act as the entities' cybersecurity SPOC, who shall "report directly to the highest level of management on a regular basis on the state of implementation" (Art. 6(8)).

In addition, each Union entity must undertake a **cybersecurity maturity assessment** every two years (Art. 7)[132] and "take appropriate and proportionate technical,

130 Excluded from the Regulation's scope are "network and information systems handling EU classified information" (EUCI) (Art. 2(3)), with the exception that CERT-EU "may provide assistance to Union entities regarding incidents in network and information systems handling EUCI where it is explicitly requested to do so by the Union entities concerned in accordance with their respective procedures" (Art. 13(8)).

131 The Regulation defines Union entities as "Union institutions, bodies, offices and agencies set up by or pursuant to the Treaty on European Union, the Treaty on the Functioning of European Union (TFEU) or the Treaty establishing the European Atomic Energy Community" (Art. 3, point (1)).

operational and organisational **measures** to manage the cybersecurity risks identified" (Art. 8(1)). In effect, the cybersecurity risk-management measures "shall ensure a level of security of network and information systems across the entirety of the ICT environment commensurate to the cybersecurity risks posed" (Art. 8 (1)). The Regulation specifies domains for measures and points out examples for particular measures. Among the domains feature "cybersecurity policy," "policies on cybersecurity risk analysis and information system security," "policy objectives regarding the use of cloud computing services", "organisation of cybersecurity," "supply chain security," or "incident handling" (for a complete list, see Art. 8(2)). Measures taken in these domains should at least comprise, inter alia, the "use of cryptography and encryption," "proactive measures for detection and removal of malware and spyware," or "criteria for secure software development and evaluation" (for a complete list see Art. 8(3)). Building upon the insights gained when carrying out prior measures, EU entities shall each adopt a "cybersecurity plan" that includes, inter alia, the measures taken in accordance with complying with Article 8 as well as the "Union entity's cyber crisis management plan for major incidents" (Art. 9). Subsequently, every entity shall share their plan with the IICB (Art. 3) and, upon request, with the European Parliament and Council (Art. 20(4)).

The following timelines apply for the implementation of each measure:

Who	What	When	Post-Deadline	Legal Basis
IICB (after consultation with ENISA and guidance from CERT-EU)	Issuance of guidelines to Union entities to conduct an initial cybersecurity review and establishing an internal cybersecurity risk-management, governance and control framework, carrying out cybersecurity maturity assessments, taking cybersecurity risk-management measures, and adopting the cybersecurity plan	8 September 2024	-	Art. 5(1)
Each Union entity	Establishment of an internal cybersecurity risk-management, governance and control framework	8 April 2025	Review on a regular basis, at least every four years	Art. 6(1)
Each Union entity	Conduct of cybersecurity maturity assessment	8 July 2025	At least every two years thereafter	Art. 7(1)

132 "Where appropriate, [the cybersecurity maturity assessments shall] be carried out with the assistance of a specialised third party" (Art. 7(2)). management plan for major incidents" (Art. 9). Subsequently, every entity shall share their plan with the IICB (Art. 3) and, upon request, with the European Parliament and Council (Art. 20(4)).

Each Union entity	Enactment of appropriate and proportionate technical, operational and organisational measures to manage the cybersecurity risks identified under the Framework, and to prevent or minimise the impact of incidents	8 September 2025	-	Art. 8(1)
Each Union entity	Approval of cybersecurity plan	8 January 2026	Revision every two years	Art. 9(1)
IICB	Submission of a report [1] on implementation progress and CERT-EU-Member State cooperation → European Parliament and Council [1] This report shall also be used as "an input to the biennial report on the state of cybersecurity in the Union" (Art. 10(14)) to be prepared pursuant to the NIS 2 Directive.	8 January 2025	Annually thereafter	Art. 10(14)

Information-Sharing, Reporting, Incident Response and Management

Voluntarily, EUIBAs can share "information on, incidents, cyber threats, near misses and vulnerabilities" that are impacting them with the CERT-EU (Art. 20(1)). To this end, CERT-EU shall provide for "efficient means of communication, with a high level of traceability, confidentiality and reliability" (Art. 20(1)). The other way around, CERT-EU may also "request Union entities to provide it [without undue delay] with information from their respective ICT system inventories, including information relating to cyber threats, near misses, vulnerabilities, indicators of compromise, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect incidents" (Art. 20(2)).[133] The Regulation further puts in place reporting obligations for EU entities to report when they become subject of a "significant incident" (Art. 21). To determine an incident's significance, the Regulation lists two elements that can give rise to a significant incident:

- (a) the incident "has caused or is capable of causing severe operational disruption to the functioning of, or financial loss to, the Union entity concerned;" or
- (b) the incident "has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage" (Art. 21(1)).

In reporting such an incident to CERT-EU, the following specific timelines apply:

133 Article 20's "sharing obligations do not extend to EUCI [and] information the further distribution of which has been excluded by means of a visible marking, unless the sharing thereof with CERT-EU has been explicitly allowed" (Art. 20(6)).

Table 38: Overview of Regulation 2023/2841's Incident Reporting Obligations

I. Action to be taken by EU entity				
(a) Without undue delay, >24h of "becoming aware" of significant incident	(b) Without undue delay, > 72h of "becoming aware" of significant incident	(c) "Where applicable [...] without undue delay"	(d) Upon request by CERT-EU	(e) <1 month after [I (b)] has been submitted
• Submission of an early warning to CERT-EU. The warning shall "where applicable, [...] indicate that the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-entity or a cross-border impact" (Art. 21(2), point (a)) • Notification of relevant Member State counterparts that a significant incident occurred in its territory (Art. 21(3))	Submission of an incident notification [1] to CERT-EU. Where applicable, the notification shall update information provided in the warning of step (a) and "indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise" (Art. 21(2), point (b))	Communication of the incident to "the users of the network and information systems affected, or of other components of the ICT environment, that are potentially affected by a significant incident or a significant cyber threat" paired with "where appropriate, [the] need to take mitigating measures, any measures or remedies" (Art. 21(5))	Submission of an intermediate report to CERT-EU outlining "relevant status updates" (Art. 21(2), point (c))	Submission of a final report [2] to CERT-EU. If the incident is still ongoing at the time, essential and important entities must submit a progress report instead. In the latter case, a final report must then additionally be provided "within one month of their handling of the incident" (Art. 21(2), point (d) and (e))
[1] An EUIBA's incident notification shall include "any information enabling CERT-EU to determine any cross-entity impact, impact on the hosting Member State or cross-border impact following a significant incident" (Art. 21(4)). [2] The final report shall comprise "(i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; [and] (iv) where applicable, the cross-border or cross-entity impact of the incident" (Art. 21(2), point (d)).				

II. Action to be taken by CERT-EU
No specified timeline

- Issuance of a cybersecurity alert when a "significant incident or significant cyber threat affects a network and information system, or a component of a Union entity's ICT environment that is knowingly connected with another Union entity's ICT environment" (Art. 21(6))

Every quarter, CERT-EU shall provide the IICB, ENISA, EU INTCEN, and the CSIRTs Network with a "summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities" (Art. 21(8)).[134] The Regulation mandates the IICB to "issue guidelines or recommendations further specifying the arrangements for, and format and content of, the reporting pursuant to this Article" by 8 July 2024 (Art. 21(9)).[135]

The Regulation stipulates that the CERT-EU acts as the Union's "cybersecurity information exchange and incident response coordination hub" (Art. 22). This involves facilitation with respect to information-sharing among entities and Member State counterparts and of Union-wide incident response coordination. The latter involves

- "contribution to consistent external communication;"
- "mutual support, such as sharing information relevant to Union entities, or providing assistance, where relevant directly on site;"
- "optimal use of operational resources;"
- and "coordination with other crisis response mechanisms at Union level" (Art. 22(2)).

CERT-EU's role in incident response also extends to support for Union entities in the area of "situational awareness of incidents, cyber threats, vulnerabilities and near misses" (Art. 22(3)) with the close involvement of ENISA. CERT-EU is further tasked with developing "guidelines or recommendations on incident response coordination and cooperation for significant incidents," which are to be agreed upon by the IICB by 8 January 2025 (Art. 22(4)). The IICB is further instructed to prepare a cyber crisis management plan, "in close cooperation with CERT-EU and ENISA," that touches upon the following issues:

- "arrangements concerning coordination and information flow among Union entities for the management of major incidents at operational level;"
- "common standard operating procedures (SOPs);"
- "a common taxonomy of major incident severity and crisis triggering points;"
- "regular exercises;"

134 This report shall also be used for purposes of preparing the biennial report on the state of cybersecurity as provided for pursuant to the NIS 2 Directive (Art. 21(8)).

135 When doing so, the "IICB shall take due regard to relevant implementing acts adopted under the NIS 2 Directive" (Art. 21(9)).

- and "secure communication channels that are to be used" (Art. 23(1)).

The coordination of the management of major incidents among EUIBAs rests with the CERT-EU. To this end, CERT-EU "shall maintain an inventory of the available technical expertise that would be needed for incident response in the event of major incidents"[136] for which EUIBAs need to provide a "list of experts available within their respective organisations detailing their specific technical skills" every year (Art. 23(3) and (4)).

Who	What	When	Legal Basis
CERT-EU	Submission of a report on significant incidents, incidents, cyber threats, near misses and vulnerabilities → IICB, ENISA, EU INTCEN, and CSIRTs Network	Every three months	Art. 21(8)
IICB	Issuance of guidelines or recommendations further specifying the arrangements for, and format and content of, incident reporting	8 July 2024	Art. 21(9)
IICB	Adoption of guidelines or recommendations on incident response coordination and cooperation for significant incidents	8 January 2025	Art. 22(4)

Compliance

In addition to other tasks, the Regulation tasks the IICB to "effectively monitor the implementation of this Regulation and of adopted guidelines, recommendations and calls for action by the Union entities" (Art. 12(1)). In cases of non-compliance, the IICB is, inter alia, empowered to "communicate a reasoned opinion to the Union entity concerned with observed gaps in the implementation of this Regulation," "issue a warning to address identified shortcomings within a specified period," or "issue a recommendation that all Member States and Union entities implement a temporary suspension of data flows to the Union entity concerned" (for a complete list of powers, see further Article 12(2)).

Review

Who	What	When	Post-Deadline	Legal Basis
IICB	Submission of a report on the Regulation's implementation → Commission	8 January 2025	Annually thereafter	Art. 25(1)

136 The Regulation defines 'major incident' as "an incident which causes a level of disruption that exceeds a Union entity's and CERT-EU's capacity to respond to it or which has a significant impact on at least two Union entities" (Art. 3, point (8)).

Commission	Assessment and report on the Regulation's implementation and "experience gained at a strategic and operational level" → European Parliament and Council	8 January 2027	Biannually thereafter	Art. 25(2)
Commission	Evaluation of the Regulation's functioning and submission of a report → European Parliament, Council and European Economic and Social Committee and the Committee of the Regions	By 8 January 2029	-	Art. 25(3)

Rules for Particular EUIBAs

— European External Action Service

In June 2023, the Union's High Representative of the Union for Foreign Affairs and Security Policy adopted a ◆◆ Decision on the security rules for the European External Action Service (EEAS). Scope-wise, the Decision applies "to all EEAS staff and all staff in Union Delegations". The Decision specifies "the general regulatory framework for managing effectively the risks to staff placed under the responsibility of the EEAS [...], to EEAS premises[137], physical assets, information, and visitors" (Art. 1). In relation to cybersecurity, the Decision stipulates that the EEAS shall ensure that a process is in place for reporting security incidents, for which "cyber attacks" are enumerated as a potential scenario (Art. 7 (1)). The Decision also provides for the possibility of carrying out security investigations "in case of cyber-incidents" (Art. 10). The Decision further assigns particular tasks and functions to the EEAS Directorate responsible for headquarters (HQ) security and EEAS information security within the purview of the EEAS Directorate General for Resource Management. For instance, the Directorate is in charge of the "Communication and Information Systems (CIS) and information security for Union Delegations" (Art. 13).

— European Commission

The ◆◆ Commission Decision on the security of communication and information systems in the European Commission (2017) regulates the use of "communication and information systems (CISs)[138] which are owned, procured, managed or

137 The Decision defines EEAS premises as "all EEAS establishments, including buildings, offices, rooms and other areas, as well as areas housing communication and information systems (including those handling EUCI), where the EEAS conducts permanent or temporary activities" (Art. 2, point (d)).

138 The Commission Decision defines CISs as "any system enabling the handling of information in electronic form, including all assets required for its operation, as well as infrastructure, organisation, personnel and information resources", also comprising "business

operated by or on behalf of the Commission and all usage of those CISs by the Commission" (Art. 1(1)). The Decision applies to "all Commission departments and Executive Agencies" (Art. 1(3)) and "Members of the Commission, to Commission staff [...], to national experts seconded to the Commission [...], to external service providers and their staff, to trainees and to any individual with access to CIS" (Art. 1(4)). "Overall responsibility for the governance of IT security as a whole within the Commission" rests with the Commission's Corporate Management Board (Art. 5), with the support of the Information Security Steering Board (ISSB), which is entrusted with the "operational responsibility for the governance of IT security as a whole within the Commission" (Art. 6). The Decision lays down "legality, transparency, proportionality and accountability" as IT security principles within the Commission (Art. 3(1)). To this end, the following elements shall be ensured appropriately: authenticity, availability, confidentiality, integrity, non-repudiation, protection of personal data and professional secrecy (Art. 3(3)). The Decision specifies and assigns tasks for the following entities/actors in general and in relation to IT security incident[139] handling:

Table 39: Overview of Tasks and Responsibilities in Relation to IT Security and IT Security Handling Within Commission Decision 2017/46

Entities/ Actors	Definition	Non-exhaustive Examples of Tasks and Responsibilities in Relation to IT Security	Non-exhaustive Examples of Tasks and Responsibilities in Relation to IT Security Incident Handling (Art. 15)
Directorate-General for Human Resources and Security (DG HR)		Art. 6: • "assur[ing] alignment between the IT security policy and the Commission's information security policy" • "establish[ing] a framework for the authorisation of the use of encrypting technologies for the storage and communication of information by CISs" • "perform[ing] IT	• "participat[ing] in IT security incidents crisis management groups and IT security emergency procedures" • "be[ing] in charge of relations with law enforcement and intelligence services" • "perform[ing] forensic analysis regarding cyber-security"

applications, shared IT services, outsourced systems, and end-user devices" (Art. 2, point (5))

139 An IT security incident is defined as "an event that could adversely affect the confidentiality, integrity or availability of a CIS" (Art. 2, point (15)).

	security inspections to assess the compliance of the Commission's CISs with the security policy"	
Directorate-General for Informatics (DG DIGIT) [1] [1] DG DIGIT is called the Directorate-General for Digital Services since November 2023	Art. 7: • "assess[ing[the IT security risk management methods, processes and outcomes of all Commission departments" • "monitor[ing] the IT security risks and IT security measures implemented in CISs" • "request[ing] system owners to take specific IT security measures in order to mitigate IT security risks to Commission's CISs" after consultation with DG HR • "ensur[ing] that system owners, data owners and other roles with IT security responsibilities in Commission departments are made aware of the IT security policy" • "inform[ing] the Directorate-General for Human Resources and Security on specific IT security threats, incidents and exceptions to the Commission's IT security policy notified by the system owners which could have a significant impact on security in the Commission" • "report[ing regularly] on major IT security incidents affecting	• "providing the principal operational IT security incident response capability within the European Commission" • "responsible for handling any IT security incident detected in relation to Commission CISs that are not outsourced systems" • "inform[ing] affected Commission departments about IT security incidents, the relevant LISOs [Local Informatics Security Officers] and, where appropriate, the CERT-EU on a need-to-know basis" • "be[ing] the contact point for the management of the crisis situations by coordinating the IT security incidents crisis management groups" in case of a major IT security incident • "decid[ing] to launch an IT security emergency procedure" in case of an emergency

		the Commission's CIS to the ISSB"	
Commission departments	any Commission Directorate-General or service, or any Cabinet of a Member of the Commission (Art. 2, point (3))	Art. 8: • "appoint[ing] a system owner, who is an official or a temporary agent, for each CIS who will be responsible for IT security of that CIS" • "appoint[ing] a data owner for each data set handled in a CIS", • "designat[ing] a Local Informatics Security Officer (LISO) who can perform the responsibilities independently from system owners and data owners" • "launch[ing] an emergency procedure in case of IT security emergencies" • "hold[ing] ultimate accountability for IT security including the responsibilities of the system owner and data owner" • "launch[ing] an emergency procedure in case of IT security emergencies" • "hold[ing] ultimate accountability for IT security including the responsibilities of the system owner and data owner"	
System owners	the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a CIS (Art. 2, point (33))	Art. 9: • "ensur[ing] the compliance of the CIS with the IT security policy", • "assess[ing] IT security risks and determine the IT security needs for each CIS, in collaboration with	• "immediately notify[ing] their Head of Commission Departments, the Directorate-General for Informatics, the Directorate-General for Human Resources, the LISO and, where

		the data owners and in consultation with" DG DIGIT • "prepar[ing] a security plan, including, where appropriate, details of the assessed risks and any additional security measures required" • "implement[ing] appropriate IT security measures, proportionate to the IT security risks identified" • "manag[ing] and monitor[ing] IT security risks"	appropriate, the data owner of any major IT security incidents, in particular those involving a breach of data confidentiality" • "cooperat[ing] and follow[ing] the instructions of the relevant Commission authorities on incident communication, response and remediation"
Data owners	the individual responsible for ensuring the protection and use of a specific data set handled by a CIS (Art. 2, point (7))	Art. 10: • "defin[ing] the information security needs and inform the relevant system owners of these needs" • "participat[ing] in the CIS risk assessment" • "communicat[ing] IT security incidents"	• "report[ing] all actual or suspected IT security incidents to the relevant IT security incident response team in a timely manner"
Local Informatics Security Officers (LISOs)	the officer who is responsible for IT security liaison for a Commission department (Art. 2, point (26))	Art. 11: • "proactively identify[ing] and inform[ing] system owners, data owners and other roles with IT security responsibilities in Commission department(s) about the IT security policy" • "maintain[ing] an overview of the information security risk management process and of the development and implementation of information system security plans" • "advis[ing] data owners, system owners and heads of Commission	• relevant LISOs "hav[ing] access to IT security incident records concerning the CIS of the Commission department" upon request

		departments on IT-security-related issues"	
Users	any individual who uses functionality provided by a CIS, whether inside or outside the Commission (Art. 2, point (34))	Art. 12: • "comply[ing] with the IT security policy and the instructions issued by the system owner on the use of each CIS" • "communicat[ing] IT security incidents"	• "report[ing] all actual or suspected IT security incidents to the relevant IT helpdesk in a timely manner"

The Commission Decision also instructs the DG DIGIT and DG HR to regularly "exchange information and coordinate the handling of security incidents" (Art. 15(3)). The Commission may draw on CERT–EU to "support the incident handling process when appropriate and for knowledge sharing with other EU institutions and agencies that may be affected" (Art. 15(4)).

Compliance with the outlined provisions and deliverables is mandatory (Art. 14(1)). Non-compliance may, for instance, result in disciplinary action or the imposition of mitigation measures in specified circumstances (Art. 14). The Decision is complemented by Commission Decision 2018/559 laying down implementing rules for Article 6 and Commission Decision 2017/8841 laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15, the latter of which is not publicly available.

The ⬚⬚ Commission Decision on Security in the Commission (2015) "sets out the objectives, basic principles, organisation and responsibilities regarding security at the Commission" (Art. 2(2)). In the Decision's recital, the Commission notes that "the Commission, like other international bodies, faces major threats and challenges in the field of security, in particular as regards terrorism, cyberattacks and political and commercial espionage" (recital (2)). The Decision stipulates that "all Communication and Information Systems ('CIS') used by the Commission shall comply with the Commission's Information Systems Security Policy, as set out in Decision C(2006) 3602, its implementing rules and corresponding security standards" (Art. 10(1)), subsequently repealed by Commission Decision 2017/46. The Decision grants DG HR the power to conduct "security inquiries [..., for instance,] in case of serious cyber-incidents" (Art. 13(1), point (d)) under specified circumstances. In such cases, DG HR and DG DIGIT "shall collaborate closely" (Art. 13 (7)). In this respect, the Decision mandates DG HR to "conduct[...] forensic technical analysis in cooperation with the competent Commission departments in support of the security inquiries [...] related to counterintelligence, data leakage, cyberattacks and information systems security" (Art. 11). Consultations between

DG HR and DG DIGIT on security inquiries shall also extend to examining "when it is appropriate to inform the competent authorities of the host country or any other Member State concerned" (Art. 13(7)), a decision to be ultimately taken by the DG HR. In relation to cybersecurity, the Decision further tasks the DG HR with "implementing security measures aimed at mitigating risks to security and developing and maintaining appropriate CIS to cover its operational needs" (Art. 18(1), point (5)) and "ensur[ing] external liaison [...] with the security authorities of other Union institutions, of agencies and bodies, of the Member States and of third countries in the field of response to cyberattacks with a potential impact on security in the Commission" (Art. 18(2), point (4)).

Who Does What in EU Cybersecurity Policy: Actor Profiles

Table 40 provides an overview of the involved actors per policy area (see Figure 4), ordered by five actor type categories:

1. EU Institutions, Bodies, and Agencies (EUIBAs) and EU-internal Coordination Bodies;
2. EU-Member State Coordination Bodies;
3. Member States;
4. Other Stakeholders;
5. and Bodies with Stakeholder Involvement.

This Chapter includes actor profiles for each actor listed in categories 1, 2, and 5 within dedicated subsections in alphabetical order. The profiles specify an actor's role, mandate, and the activities they engage in with respect to cyber and IT security (policy).[140]

140 This section builds on our continuous work on mapping the institutional cybersecurity policy landscape (see further, Germany's Cybersecurity Architecture).

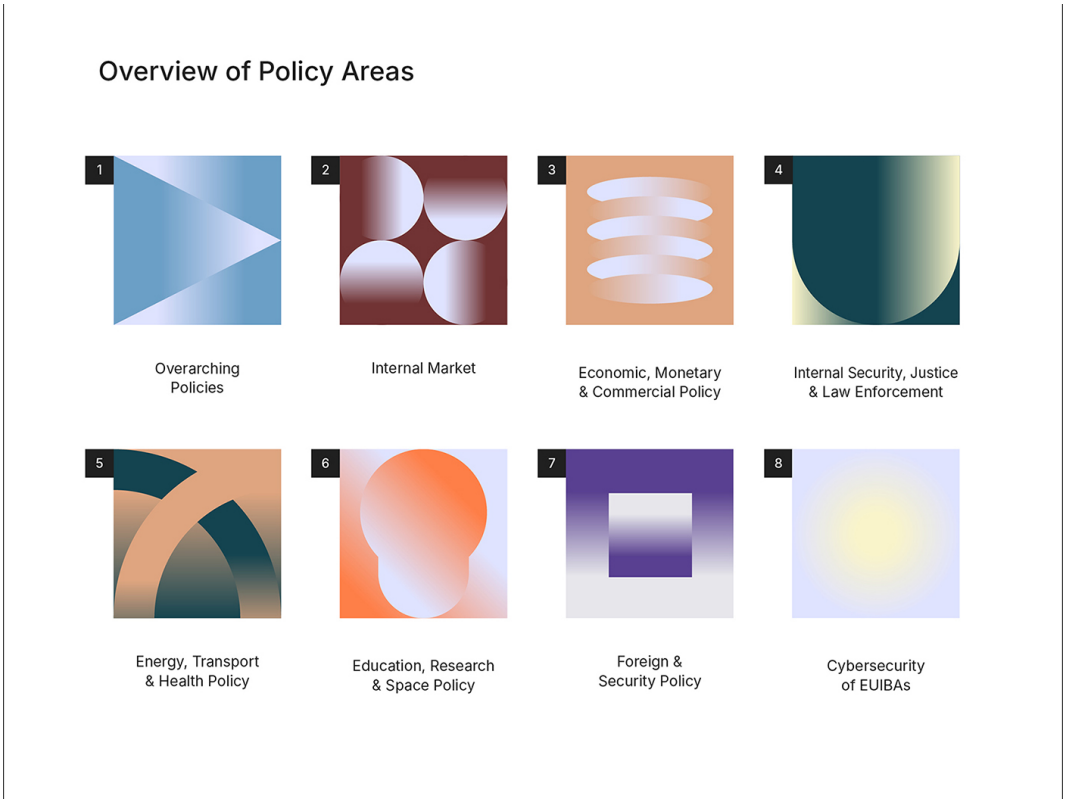


Figure 4: Policy Areas of Compendium

Table 40: Involved Actors Per Policy Area and Actor Type

Actor Type	Policy Areas	Involved Actors (in alphabetical order)
1: EU Institutions, Bodies and Agencies (EUIBAs) and EU-internal Coordination Bodies	All Policy Areas	• Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) • Council of the EU • European Commission • European Data Protection Supervisor (EDPS) • European Parliament • European Union Agency for Cybersecurity (ENISA)
	Policy Areas 2, 6 & 7	• European Cybersecurity Competence Centre (ECCC)

	Policy Area 3	• European Supervisory Authorities (ESAs) incl. Joint Committee
		  • European Banking Authority (EBA)
		  • European Insurance and Occupational Pensions Authority (EIOPA)
		  • European Securities and Markets Authority (ESMA)

		• European Central Bank (ECB)
	Policy Area 4	• European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) • European Union Agency for Criminal Justice Cooperation (Eurojust) • European Union Agency for Law Enforcement Cooperation (Europol) & European Cybercrime Centre (EC3)
	Policy Area 5	• European Union Agency for the Cooperation of Energy Regulators (ACER) • European Union Aviation Safety Agency (EASA)
	Policy Area 6	• European Union Agency for the Space Programme (EUSPA)
	Policy Area 7	• European Defence Agency (EDA) • European External Action Service (EEAS)
	Policy Area 8	• Interinstitutional Cybersecurity Board (IICB)
2: EU-Member State Coordination Bodies	Policy Area 2	• European Cybersecurity Certification Group (ECCG)
	Policy Areas 2, 3, 5, 6 & 7	• NIS Cooperation Group
	Policy Areas 2 & 6	• Computer Security Incident Response Teams Network (CSIRTs Network) • European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)
	Policy Area 4	• Critical Entities Resilience Group (CERG) • European Union Cybercrime Task Force (EUCTF)
3: Member States	All Policy Areas	• Competent and supervisory authorities as designated by Member States pursuant to the various legal acts
	Policy Area 2	• Cyber crisis management authorities • National CSIRTs • National cybersecurity certification authorities and accreditation bodies • Public administration entities

		• Public essential or important entities pursuant to the NIS 2 Directive • Single points of contact on cybersecurity
	Policy Areas 2 & 4	• Public entities identified as critical under the CER Directive
	Policy Area 6	• National Coordination Centres (NCCs)
4: Other Stakeholders	Policy Area 2	Inter alia: • Data controllers and processors • DNS service provider • Economic operators • Gatekeepers • ICT product, service, or process manufacturer/provider seeking certification or having been certified • Manufacturers • Private essential or important entities pursuant to the NIS 2 Directive • Providers of public electronic communications networks or of publicly available electronic communications services • Trust service provider
	Policy Areas 2 & 4	• Private entities identified as critical under the CER Directive
	Policy Area 3	Inter alia: • Crypto-asset service providers • Exporters • Financial entities • Payment service providers
	Policy Area 5	Inter alia: • Energy network operators • Transmission system operators • Particular entities in the civil aviation sector, e.g. airport operators or air carriers
	Policy Area 6	Inter alia: • Academia • Providers of cybersecurity skills trainings
5: Bodies with Stakeholder Involvement	Policy Area 2	• ENISA Advisory Group (ENISA AG) • Stakeholder Cybersecurity Certification Group (SCCG)

EU Institutions

— Council of the European Union (Council)

Website: www.consilium.europa.eu

EU Member States coordinate their policies at the EU level in the Council of the European Union (often just referred to as "Council" to differentiate it from the European Council). Together with the European Parliament, the Council is tasked with "exercis[ing] legislative and budgetary functions" (Art. 16(1) TEU). The Council, which meets at the level of the ministers responsible for their policy area at the national level, convenes in ten thematic configurations – such as Foreign Affairs (FAC), Justice and Home Affairs (JHA), or Economic and Financial Affairs (ECOFIN). The Council is involved in the EU legislative process and may also, in particular circumstances, adopt EU legal acts by itself. The Council is responsible for "defining and implementing" (Art. 26(2) TEU) the EU's Common Foreign and Security Policy (CFSP) based on the decisions and guidelines adopted by the European Council. Once activated, for instance, in the event of an EU-wide crisis emanating from a cybersecurity-related threat, the Council takes over coordination on the EU level through the Integrated Political Crisis Response (IPCR). The Council has established several bodies for coordination and information exchange, as well as the preparation of ministerial meetings. Of cyber and IT security policy relevance are, inter alia, the following:

Subordinate body	Description
Political and Security Committee (PSC)	The PSC is responsible for the EU's CFSP. It usually meets twice a week but gathers more frequently when necessary. The PSC monitors international situation developments and is responsible for the political control and strategic management of crisis management operations. It may be involved in the decision-making process of cyber-related diplomatic actions and the response to large-scale cybersecurity incidents and crises at the EU level. The PSC is composed of Member States' ambassadors in Brussels or representatives of Member States' foreign ministries. [See further Council of the European Union: Political and Security Committee (PSC)]
Horizontal Working Party on Cyber Issues (HWPCI)	The HWPCI, set up in 2016, coordinates the Council's work on cyber policy and respective legal acts. The tasks and objectives of the HWPCI also include harmonizing and unifying approaches to cyber policy issues, improving information sharing on cyber issues between EU Member States, and setting EU cyber priorities and strategic objectives within the EU. The HWPCI may, for example, prepare meetings of the PSC on a case-by-case basis. The HPWCI maintains cooperative relations with the Commission, EEAS, ENISA, Europol, Eurojust, and the EDA. [See further Council of the European Union: Horizontal Working Party on Cyber Issues (Cyber)]
Standing	The COSI works towards strengthening operational measures and coordination

Committee on Operational Cooperation on Internal Security (COSI)	among Member States in relation to the internal security of the EU, for instance, in areas such as law enforcement and judiciary. The COSI includes senior officials from the interior and justice ministries of all EU Member States, representatives of the Commission and the EEAS. Europol, Eurojust and other EUIBAs may be invited to participate as observers. [See further Council of the European Union: Standing Committee on Operational Cooperation on Internal Security (COSI)]

The Council is assisted by the General Secretariat of the Council (GSC), which also comprises a dedicated unit for cybersecurity (GSC.SMART.2.B).

The presidency of the Council and chairmanship of Council bodies rotate biannually among EU Member States. The Council may instruct the Commission to negotiate international agreements, with their conclusion being subject to a decision of the Council based on a Commission proposal. The High Representative of the EU for Foreign Affairs and Security Policy chairs the FAC, and representatives of the EEAS chair the PSC. The Council is represented in the IICB. The NIS Cooperation Group is chaired by the respective Member State holding the Presidency of the Council. Every 18 months, and for the first time by 18 July 2024, EU-CyCLONe reports to the Council about its work. The IICB reports annually (for the first time by 8 January 2025) to the Council on the implementation of Regulation 2023/2841 and CERT-EU-Member State cooperation. The EDA is subordinate to the Council of the EU, to which it reports and from which it receives its guidance. The Council of the EU is involved in the appointment of the EDPS, who can advise it upon request.

Further information:

- Council of the European Union: Council preparatory bodies
- Council of the European Union: Horizontal Working Party on Cyber Issues (Cyber)
- Council of the European Union: The General Secretariat of the Council
- Council of the European Union: Political and Security Committee (PSC)
- Council of the European Union: Standing Committee on Operational Cooperation on Internal Security (COSI)
- Council of the European Union: The Council of the European Union
- Council Implementing Decision on the EU Integrated Political Crisis Response Arrangements (2018/1993)

— European Central Bank (ECB)

Website: www.ecb.europa.eu

As the supervisory authority for the euro area, the European Central Bank (ECB) also assumes responsibility for monitoring and ensuring the operational capability

of financial market infrastructure and system-relevant payment systems by building cyber resilience. To this end, the ECB promotes, among other things, the international exchange of security-related information, identifies best practices, and has established a common European framework for "threat intelligence-based ethical red-teaming" (TIBER-EU) to, inter alia, diagnose strengths and weaknesses. In addition, national central banks in the euro area are required to report significant cybersecurity incidents to the ECB. The ECB also oversees how the national central banks manage relevant risks to their IT systems.

The ECB supervises the national central banks of the euro area. It cooperates with other EU institutions, such as the Commission and the CERT-EU, as well as national cybersecurity authorities. The ECB chairs and provides the Secretariat for the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB).[141] *The ECB is represented in the IICB.*

Further information:

- European Central Bank: Cyber resilience and financial market infrastructures
- European Central Bank: Euro Cyber Resilience Board for pan-European Financial Infrastructures
- European Central Bank: TIBER-EU FRAMEWORK. How to implement the European framework for Threat Intelligence-based Ethical Red Teaming
- European Central Bank: What is cyber resilience?
- European Central Bank: What is TIBER-EU?

— European Commission (EC)

Website: commission.europa.eu

The European Commission plays a strategic and organizational role within EU cybersecurity architecture. With respect to legislation, unless it is specifically precluded, the Commission is the sole actor authorized to propose legislative EU acts for adoption (Art. 17(2) TEU). In addition, it is responsible for keeping track of the implementation status of EU policies and legal acts. The Commission consists of a College of issue area-Commissioners under the political guidance of the Commission President. The Commissioners "are responsible for the implementation

141 The ECRB was created as a forum for exchange and discussion on strategic issues between private and public stakeholders in the financial sector. The ECRB's goals include sharing best practices, raising awareness of cyber resilience, and under- taking joint initiatives. An output of the ECRB is the Cyber Information and Intelligence Sharing Initiative (CIISI-EU), which aims to contribute to the protection of the financial system and its infrastructure against threats from cyberspace, for example, through prevention, identification, and mutual information sharing. ECRB meetings are attended by representatives of the Commission, Europol and ENISA, among others. Among other actors, the ECB, ENISA, and Europol are also involved in the CIISI-EU.

of the political priorities laid down in the President's political guidelines and the Commission Work Programme" and are supported by their "Cabinets and the Commission services."[142] Every Commission acts on the basis of strategic priorities defined at the beginning of its term, which are further specified in dedicated annual Commission work programs. Decision 2017/46 specifies and assigns tasks for the Directorate-General for Digital Services (DG DIGIT) and the Directorate-General for Human Resources and Security (DG HR) (within the purview of the Commissioner for Budget and Administration) in relation to IT security in general and particularly regarding IT security incident handling as outlined in detail in Policy Area 8. In addition, several Commission Directorates-General (DGs) work on cyber/IT security. Among them is the Directorate-General for Communications Networks, Content and Technology (DG CONNECT), within the purview of the Commissioner for the Internal Market, which is responsible for the development and implementation of Commission policies in the areas of the digital economy ("digital single market") and society, as well as research and innovation. To this end, among other things, it works towards "ensur[ing] European leadership and independence in critical digital technologies" and "making Europe a global leader in the data economy and in cybersecurity."[143] DG CONNECT acts as the lead DG for Digital Europe, which provides strategic funding in various fields, including cybersecurity, to promote the digital transformation of society and the economy. In addition, other DGs are responsible for relevant files covered within this compendium which address cybersecurity considerations (for a complete list of files covered within this compendium, see Chapter 4):

Table 41: Overview of Commission DGs and Responsibilities for Cybersecurity-Related Files

Commissioner	DGs and Files
Competition	DG for Competition (COMP) • Digital Markets Act
	DG for Economic and Financial Affairs (ECFIN) • Regulation establishing the Recovery and Resilience Facility
Energy	DG for Energy (ENER) • e.g. Regulation on the internal market for electricity
Financial Services, Financial Stability and Capital Markets Union	DG for Financial Stability, Financial Services and Capital Markets Union (FISMA)

142 European Commission: Governance in the European Commission (C(2020) 4240 final).

143 European Commission: Communications Networks, Content and Technology.

	• e.g. Regulation on digital operational resilience for the financial sector and Regulation on markets in crypto-assets
Health and Food Safety	DG for Health and Food Safety (SANTE) • e.g. Regulation on in vitro diagnostic medical devices
Innovation, Research, Culture, Education and Youth	DG for Research and Innovation (RTD) • Council Decision establishing the Specific Programme implementing Horizon Europe)
Internal Market	DG for Communications Networks, Content and Technology (DG CONNECT) • e.g. NIS 2 Directive, Regulation on ENISA and on information and communications technology cybersecurity certification and Electronic Communications Code
	DG for Defence Industry and Space (DEFIS) • e.g. Regulation establishing the Union Space Programme and the European Union Agency for the Space Programme
	DG for Internal Market, Industry, Entrepreneurship and SMEs (GROW) • e.g. Regulation on machinery and Directive on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment
International Partnerships	DG for International Partnerships (INTPA) • e.g. Regulation establishing Global Europe
Values and Transparency	DG for Justice and Consumers (JUST) • e.g. Regulation on general product safety and General Data Protection Regulation
Home Affairs	DG for Migration and Home Affairs (HOME) • e.g. CER Directive and Directive on attacks against information systems
Trade	DG for Trade (TRADE) • e.g. Regulation setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items
Transport	DG for Mobility and Transport (MOVE) • e.g. Regulation on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency

"Overall responsibility for the governance of IT security as a whole within the Commission" rests with the Commission's Corporate Management Board (CMB)[144]

144 The CMB "provides the highest level of corporate management oversight for operational and administrative issues in the Commission" (Art. 2, point (6) Commission Decision 2017/46).

(Art. 5 Commission Decision 2017/46), with the support of the Information Technology and Cybersecurity Board,[145] which is entrusted with the "operational responsibility for the governance of IT security as a whole within the Commission" (Art. 6 Commission Decision 2017/46).

DG CONNECT is the DG responsible (partner DG) for ENISA and represents the Commission in its Management and Executive Board together with DG DIGIT. CERT-EU is institutionally located within DG DIGIT. The Council of the EU may entrust the Commission with the negotiation of international agreements, the conclusion of which is decided by the Council based on a proposal from the Commission. The EEAS "assist[s] [...] the Commission in the exercise of [its] respective functions in the area of external relations" (Art. 2(2), Regulation 2010/427). Commission services and the EEAS shall regularly consult "on all matters relating to the external action of the Union in the exercise of their respective functions, except on matters covered by the CSDP" (Art. 3(2), Regulation 2010/427). The Commission may draw on CERT–EU to "support the incident handling process when appropriate and for knowledge sharing with other EU institutions and agencies that may be affected" (Art. 15(4) Commission Decision 2017/46). Furthermore, CERT-EU assists the Commission "on the coordinated management of large-scale cybersecurity incidents and crises" (Art. 17(1), Regulation 2023/2841) in the framework of EU-CyCLONe. In relation to their cybersecurity-related tasks, cooperative relations exist with the ACER, the EASA, EC3, the ECB, eu-LISA, and the EUSPA. The Commission provides the secretariat for the IICB, the NIS Cooperation Group and, assisted by ENISA, the ECCG. The Commission is represented in the IICB, the NIS Cooperation Group, and the CERG. Commission representatives chair the CERG and, assisted by ENISA, the ECCG. The Commission participates in EU-CyCLONe and the CSIRTs Network as an observer. It is a member of the EUCTF. The Commission is represented in the ECCC's Governing Board, the EC3's Programme Board, and the EASA's Management Board. Experts from the Commission can attend meetings and participate in the work of the ENISA AG. The SCCG, which it jointly chairs with ENISA, inter alia, supports the Commission in preparing the Union rolling work programme for European cybersecurity certification. The HWPCI lists that it maintains cooperative relations with the Commission. The EDPS can advise the Commission upon request.

Further information:

- European Commission: About the European Commission
- European Commission: Commission Decision on the Corporate Management Board

145 The Information Technology and Cybersecurity Board was formerly called the Information Security Steering Board (ISSB).

- European Commission: Commission work programme
- European Commission: Cybersecurity
- European Commission: Governance in the European Commission (C(2020) 4240 final)
- European Commission Directorate-General for Communications Networks, Content and Technology: Organisation chart
- European Commission Directorate-General for Communications Networks, Content and Technology: Strategic Plan 2020-2024
- EUR-Lex: The European Commission

— European Parliament (EP)

Website: www.europarl.europa.eu

Together with the Council, the European Parliament "exercis[es] legislative and budgetary functions" (Art. 14(1) TEU). In terms of its legislative functions, the European Parliament acts as "equal co-legislator" when legislative acts are adopted according to the ordinary legislative procedure. To exercise its legislative powers, the European Parliament is subdivided into various issue area-specific standing committees, which convene in public sessions once or twice monthly to prepare the Parliament's plenary sessions. Individual committees are, inter alia, responsible for "draw[ing] up, amend[ing] and adopt[ing] legislative proposals" and "consider[ing] Commission and Council proposals."[146] Involved committees on cybersecurity-related legislation contained within this compendium are, for instance, the Industry, Research and Energy Committee (ITRE) for the NIS 2 Directive and the proposed Cyber Resilience Act, the Civil Liberties, Justice and Home Affairs Committee (LIBE) for the CER Directive or the Economic and Monetary Affairs Committee (ECON) for the DORA Regulation. In addition to legislative work, the European Parliament is also empowered to "exercise oversight over other institutions, to monitor the proper use of the EU budget and to ensure the correct implementation of EU law", for instance, by owning the "right to approve and dismiss the European Commission."[147] As part of its supervisory functions, the European Parliament can also set up committees of inquiry, such as the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA).[148] Members of the European Parliament (MEPs) and

146 European Parliament: The Committees of the European Parliament.

147 European Parliament: Supervisory powers.

148 For more information on the PEGA Committee of Inquiry see European Parliament: Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware.

the committees are supported by the European Parliamentary Research Service (EPRS), which, inter alia, maintains an overview of the status quo of legislative initiatives and evaluates the Commission's impact assessments on proposals.

The European Parliament is represented in the IICB. It can request participation in CERG meetings and may be invited to discussions within the NIS Cooperation Group. Every 18 months, and for the first time by 18 July 2024, EU-CyCLONe reports to the European Parliament about its work (Art. 16(7) NIS 2 Directive). The IICB reports annually (for the first time by 8 January 2025) to the European Parliament on the implementation of Regulation 2023/2841 and CERT-EU-Member State cooperation.

Further information:

- European Parliament: Budgetary powers
- European Parliament: European Parliamentary Research Service (EPRS)
- European Parliament: Legislative powers
- European Parliament: Rules of Procedure of the European Parliament
- European Parliament: Supervisory powers
- European Parliament: The Committees of the European Parliament

EU Bodies

— European Union External Action Service (EEAS)

Year of establishment: 2011

Legal basis: ﷺ Council Decision establishing the organisation and functioning of the European External Action Service (2010/427)

Website: www.eeas.europa.eu

The European External Action Service is the "European Union's diplomatic service."[149] It is, inter alia, tasked with "support[ing] the High Representative [HR/VP...] in fulfilling his/her mandate to conduct the Common Foreign and Security Policy ('CFSP') of the European Union" and "in his/her capacity as Vice-President of the Commission for fulfilling within the Commission the responsibilities incumbent on it in external relations, and in coordinating other aspects of the

149 European Union External Action Service: About the European External Action Service.

Union's external action" (Art. 2(1), Regulation 2010/427). In addition to the HR/VP, the EEAS "assist[s] the President of the European Council, the President of the Commission, and the Commission in the exercise of their respective functions in the area of external relations" (Art. 2(2), Regulation 2010/427). The Decision establishing the EEAS further assigns a supporting role vis-à-vis Member States and a coordinating function to it. Specifically, it stipulates that "the EEAS shall support, and work in cooperation with, the diplomatic services of the Member States, as well as with the General Secretariat of the Council and the services of the Commission, in order to ensure consistency between the different areas of the Union's external action and between those areas and its other policies" (Art. 3(1), Regulation 2010/427). From an organizational point of view, the EEAS comprises "a central administration and [...] Union Delegations to third countries and [...] international organisations" (Art. 1(4), Regulation 2010/427). Within the EEAS' Department on Peace, Security and Defence (MD-PSD), a dedicated division deals with "Hybrid Threats & Cyber" (SECDEFPOL.2). As part of the EU Military Staff (EUMS), the EEAS also comprises a division on "Communication and Information Systems & Cyber Defence" (EUMS.E). Furthermore, the EEAS hosts the EU Intelligence and Situation Centre (EU INTCEN) and the EUMS' Intelligence Directorate (EUMS INT). EU INTCEN is a civil analysis unit within the EEAS, that processes intelligence received from Member States and other publicly accessible information. It is made up of an "Intelligence Analysis and Reporting" (INTCEN.1) and "Support/Open Sources Research" (INTCEN.2) Division. Unlike national intelligence services in EU Member States, EU INTCEN, which reports directly to the High Representative for Foreign Affairs and Security Policy, has no independent operational intelligence-gathering capabilities. EU INTCEN products can also be made available to other EU institutions operating within the CFSP, the CSDP, or in the area of counterterrorism. Moreover, the EU's Hybrid Fusion Cell, which "receive[s], analy[zes] and share[s] classified and open source information [...] relating to indicators and warnings concerning hybrid threats," is institutionally located within EU INTCEN.[150] The EUMS INT represents the EU INTCEN's military counterpart. It seeks to support the EUMS by providing "intelligence input" to facilitate early warning, situational awareness, and "crisis response planning and assessment for operations and exercises."[151] Together with the EUMS INT, INTCEN forms the Single Intelligence Analysis Capacity (SIAC) "to deliver joint civilian and military intelligence assessments."[152] The EEAS maintains the "EEAS Crisis Response Mechanism (CRM) [which] is activated upon occurrence of a serious situation or emergency concerning or anyway involving the external

150 European Commission: FAQ: Joint Framework on countering hybrid threats.

151 European Union External Action Service: The European Union Military Staff (EUMS).

152 European Union External Action Service: EEAS Vacancy Notice Contract Agent FGIV – Job title: Intelligence Analyst.

dimension of the EU"[153] and is involved in the implementation of the EU's Cyber Diplomacy Toolbox. At the multilateral level, the EEAS takes part in the discussion within the United Nations (UN) Open-ended Working Group on security of and in the use of information and communications technologies (OEWG) and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC), among other fora.[154] As outlined in detail in policy area 8, Decision 2023/C 263/04 lays down security rules for the EEAS, including provisions on cyber and information security.

The EEAS is managed by the High Representative of the European Union for Foreign Affairs and Security Policy (the HR/VP). The EEAS and Commission entities shall regularly consult "on all matters relating to the external action of the Union in the exercise of their respective functions, except on matters covered by the CSDP" (Art. 3(2), Regulation 2010/427). In particular, the EEAS shall be involved "in the preparatory work and procedures relating to [respective] acts to be prepared by the Commission" (Art. 3(2), Regulation 2010/427). The HR/VP chairs the Council's FAC, EEAS representatives chair the PSC. Together with the EDA, the EEAS forms the secretariat of PESCO. The EEAS is represented in the COSI (Council of the EU). The EEAS participates in the NIS Cooperation Group as an observer. It is represented in the IICB. The Regulation establishing the ECCC provides for cooperative working relations with the EEAS. The EEAS is represented in the EC3's Programme Board. Every quarter, EU INTCEN receives a "summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities" (Art. 21(8) Regulation 2023/2841) from CERT-EU. The HWPCI lists that it maintains cooperative relations with the EEAS.

Further information:

- European Union External Action Service: About the European External Action Service
- European Union External Action Service: Creation of the European External Action Service
- European Union External Action Service: Cybersecurity
- European Union External Action Service: Organisation chart of the EEAS
- European Union External Action Service: The European Union Military Staff (EUMS)

153 For more information on the EEAS CRM see p. 21f. Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises.

154 See further, for instance, Council Decision authorising the opening of negotiations on behalf of the European Union for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes (2022/895) and European Union External Action Service: EU Statement – UN Open-Ended Working Group on ICT: Existing and Potential Threats.

— European Data Protection Supervisor (EDPS)

Year of establishment: 2004

Website: www.edps.europa.eu

The European Data Protection Supervisor and the supervisory authority supporting his or her duties are responsible for ensuring the supervision of and adherence to data protection principles when processing personal data processed by the EU's many institutions. Safeguarding the protection of privacy includes, for example, conducting investigations or processing any submitted complaints. In addition, the EDPS observes and evaluates possible implications for data protection that may arise from new technological developments. The EDPS is appointed for a five-year term and works together with national data protection authorities within EU Member States. In the past, the EDPS also took a stance on, inter alia, the EU's cybersecurity strategy and other legislative proposals, recommendations, and communications of the European Commission from a data-privacy law perspective.

On request, the EDPS can advise the European Commission and the Council of the EU. The Council of the EU is involved in the appointment of the EDPS. The EDPS assumes a supervisory role over the EU agencies Europol and Eurojust regarding their processing of personal data. eu-LISA maintains cooperative relations with the EDPS. The EDPS is represented in the IICB.

Further information:

- European Data Protection Supervisor: About Us
- European Data Protection Supervisor: Cybersecurity
- Example for a Cybersecurity-Related EDPS Opinion: European Data Protection Supervisor: Opinion 23/2022 on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

EU Agencies

— European Union Agency for Criminal Justice Cooperation (Eurojust)

Year of establishment: 2002

Legal basis: ﷺ Regulation on the European Union Agency for Criminal Justice

Cooperation (Eurojust) (2018/1727)

Website: www.eurojust.europa.eu

Eurojust plays a role in combating threats such as cybercrime on an operational level. By promoting information exchange, connecting ongoing investigations, developing criminal law strategies, and enabling joint action,Eurojust is responsible for coordinating case investigations. This coordination is intended to strengthen the investigative capabilities of Member States' law enforcement agencies in the area of cybercrime, the understanding of cybercrime, and the investigative options of both law enforcement and the judiciary. Eurojust regularly publishes reports, such as the annual Cybercrime Judicial Monitor[155] , which provides an overview of legislation and case law at the EU and national level, or occasion-based reports on specific challenges and best practices.

Eurojust works with EC3's specialized advisory groups, networks of heads of cybercrime units, and prosecutors specializing in cybercrime. Cooperative relations, inter alia, exist with the following EUIBAs: Europol, EC3 and eu-LISA. The HWPCI maintains cooperative relations with Eurojust. Together with Europol, Eurojust has published a report on common challenges in the fight against cybercrime in the past. Eurojust is a member of the EUCTF. Eurojust can be invited as an observer to meetings of the COSI (Council of the EU). The EDPS has a supervisory role over Eurojust regarding the lawful processing of personal data. Eurojust is represented on the EC3's Programme Board. Eurojust is part of the eu-LISA's Management Board in an observational capacity and is a member of some of its advisory groups.

Further information:

- European Union Agency for Criminal Justice Cooperation: Cybercrime

— European Union Agency for Cybersecurity (ENISA)

Year of establishment: 2004

Legal basis: ﷺ Regulation on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act, Regulation 2019/881)

Website: www.enisa.europa.eu

155 Past Cybercrime Judicial Monitors can be found here.

ENISA[156], the European Union Agency for Cybersecurity, is tasked with "achieving a high common level of cybersecurity across the Union", "reducing the fragmentation of the internal market," and "approximating Member State laws, regulations and administrative provisions" (Art. 3 Regulation 2019/881). To this end, the Cybersecurity Act assigns to ENISA the following tasks (non-exhaustive):

Table 42: Overview of Tasks Assigned to ENISA

Area	Exemplary Tasks
Development and implementation of Union policy and law (Art. 5 Regulation 2019/881)	• Provision of "independent opinion and analysis as well as carrying out preparatory work" to "assist[…] and advis[e] on the development and review of Union policy and law in the field of cybersecurity and on sector-specific policy and law initiatives" • Issuance of "opinions, guidelines, provi[sion of] advice and best practices" in an assistance effort towards Member States to "implement the Union policy and law regarding cybersecurity consistently" • Support to NIS Cooperation Group activities • Support to Member States "in the implementation of specific cybersecurity aspects of Union policy"
Capacity-building (Art. 6 Regulation 2019/881)	Assistance to Member States with regard to • "efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents [through] knowledge and expertise" • "developing national CSIRTs" • "regularly organising the cybersecurity exercises at Union level" Assistance to Member States and EUIBAs with regard to • "establishing and implementing vulnerability disclosure policies on a voluntary basis" Assistance to EUIBAs with regard to • "improv[ing] the prevention, detection and analysis of cyber threats and incidents and to improve their capabilities to respond to such cyber threats and incidents, in particular through appropriate support for the CERT-EU" • "developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking the progress in their implementation"
Operational cooperation at Union level (Art. 7 Regulation 2019/881)	Vis-à-vis Member States through CSIRTs Network: • "advising on how to improve their capabilities to prevent, detect and respond to incidents and, at the request of one or more Member States, providing advice in relation to a specific cyber threat" • "analysing vulnerabilities and incidents on the basis of publicly available information or information provided voluntarily by Member States for that purpose" Vis-à-vis Union and Member States:

156 Over the course of its establishment, ENISA underwent a name change from the "European Network and Information Security Agency" to "European Union Agency for Cybersecurity". The abbreviation of the original name remained the same after the process.

	• "contribut[ing] to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity", for example, via "ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs network and the technical and political decision-makers at Union level" Vis-à-vis EUIBAs: • "exchang[ing] know-how and best practices" • providing "advice and issuing of guidelines on relevant matters related to cybersecurity"
Market, cybersecurity certification, and standardisation (Art. 8 Regulation 2019/881)	• Preparation of "candidate European cybersecurity certification schemes" • Development and publication of "guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services and ICT processes"
Knowledge and information (Art. 9 Regulation 2019/881)	• Provision of "topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity" • Conduct of "long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents"
Awareness-raising and education (Art. 10 Regulation 2019/881)	• Implementation of "regular outreach campaigns to increase cybersecurity and its visibility in the Union and encourage a broad public debate" together with Member States and EUIBAs
Research and innovation (Art. 11 Regulation 2019/881)	• Provision of advice to EUIBAs and Member States on "research needs and priorities in the field of cybersecurity" • "Contribut[ion] to the strategic research and innovation agenda at Union level in the field of cybersecurity"
International cooperation (Art. 12 Regulation 2019/881)	• Supporting "the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation"

The NIS 2 Directive further tasks ENISA with the development and maintenance of a "European vulnerability database" (Art. 12(2) NIS Directive), upon consultation with the NIS Cooperation Group, and "a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms" (Art. 27(1) NIS 2 Directive). ENISA is responsible for drafting a biannual "report on the state of cybersecurity in the Union" for submission and presentation to the European Parliament (Art. 18 NIS Directive). ENISA is further involved in the drafting of common draft regulatory and

implementing technical standards in the framework of the DORA Regulation. Annually, ENISA publishes a threat landscape report (ENISA Threat Landscape), which identifies and assesses threats from cyberspace. In addition, ENISA organizes regular cybersecurity exercises in various formats, such as the biennial Cyber Europe Exercise together with EU Member States.

DG CONNECT is the DG responsible (parent DG) for ENISA and represents the Commission in ENISA's Management and Executive Board together with DG DIGIT. In fulfilling its mandate, ENISA acts independently (Art. 3(3) Regulation 2019/881). ENISA provides the secretariat of the CSIRTs Network, EU-CyCLONe, and the SCCG. As outlined above, ENISA supports Member States' operational cooperation within the CSIRTs Network. Also, in the framework of EU-CyCLONe, ENISA is assigned a supporting role by facilitating "the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information" (Art. 16(2) NIS 2 Directive). ENISA supports the Commission in providing the ECCG's Secretariat. Member States and the Commission are represented in ENISA's Management Board. ENISA chairs the ENISA AG and co-chairs the SCCG. ENISA is among the members of the IICB. ENISA is tasked with supporting the IICB in setting up an informal group that comprises Union entities' designated local cybersecurity officers. ENISA participates in the NIS Cooperation Group, the EUCTF, and the ECRB. Based on information received by Member State SPOCs, ENISA shall brief the NIS Cooperation Group and the CSIRTs Network every six months concerning "findings on notification" (Art. 23(9) NIS 2 Directive). ENISA and CERT-EU shall maintain a "structured cooperation with ENISA on capacity building, operational cooperation and long-term strategic analyses of cyber threats" (Art. 13(5) Regulation 2023/2841). Every three months, ENISA receives a "summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities" (Art. 21(8) Regulation 2023/2841) from CERT-EU. The ECCC shall "undertake [its] tasks in collaboration with ENISA [...], as appropriate" (Art. 3(2) Regulation 2021/887). ENISA is represented in the ECCC's Governing Board as a permanent observer. In early 2021, ENISA and eu-LISA entered into a three-year joint cooperation plan to strengthen cooperation and exchange knowledge as well as expertise in the field of information security, among other areas for cooperation. EDA, CERT-EU, EC3, and ENISA concluded a Memorandum of Understanding for cooperation and exchange in the field of cybersecurity in 2018. In June 2024, ENISA and the ESAs concluded an MoU for increased cooperation and information-sharing among each other.[157] *The ENISA AG advises ENISA on, among other things, the implementation of its tasks. Upon request,*

157 European Securities and Markets Authority: ESAs and ENISA sign a Memorandum of Understanding to strengthen cooperation and information exchange.

also the SCCG may advise ENISA. Cooperative working relations, inter alia, exist between ENISA and the HWPCI, ACER, Europol, and EUSPA. ENISA is represented on the EC3's Programme Board. The ECCG, in addition to the Commission, may request ENISA to develop new candidate certification schemes. ENISA maintains working arrangements with the U.S. Cybersecurity and Infrastructure Security Agency (CISA)[158] *and Ukrainian authorities*[159] *.*[160]

Further information:

- European Union Agency for Cybersecurity: About ENISA
- European Union Agency for Cybersecurity: International Strategy of the EU Agency for Cybersecurity
- European Union Agency for Cybersecurity: Publications
- European Union Agency for Cybersecurity: ENISA Single Programming Document 2024 - 2026

— European Union Agency for Law Enforcement Cooperation (Europol) & European Cybercrime Centre (EC3)

Year of establishment: 1999 (Europol)/2013 (EC3)

Legal basis: ﷺ Regulation on the European Union Agency for Law Enforcement Cooperation (Europol) (2016/794)

Website: www.europol.europa.eu

Europol is the law enforcement agency of the European Union. It supports the European Commission and EU Member States in prosecuting cybercrime, terrorism, and organized crime. Europol supports Member States in previously initiated investigations and analyzes crime trends in the EU. Europol also cooperates with non-EU member states and international organizations. In the area of cybercrime, Europol is strengthening law enforcement in particular through its European Centre for Cybercrime Prevention (EC3). The EC3 focuses on three areas in combating cybercrime: forensics, expertise and stakeholder management, and operations through dedicated teams. For cyber-dependent crimes, child sexual

158 Commission Decision approving a working arrangement between the European Union Agency for Cybersecurity (ENISA) and the United States Cybersecurity and Infrastructure Security Agency (CISA) in the area of cybersecurity (C (2023) 8553).

159 Commission Decision approving the Working Arrangement between the European Union Agency for Cybersecurity (ENISA) and the National Cybersecurity Coordination Center of Ukraine (NCCC) and the Administration of the State Service of Special Communication and Information Protection of Ukraine (the Administration of SSSCIP) in the area of cybersecurity (C (2023) 4016).

160 The option for ENISA to engage in such international cooperation is provided for in Article 42 of Regulation 2019/881.

exploitation, and payment fraud, the EC3, inter alia,

- "serves as the central hub for criminal information and intelligence";
- "supports operations and investigations by Member States by offering operational analysis, coordination and expertise";
- "provides highly specialised technical and digital forensic support capabilities to investigations and operations";
- and "provides 24/7 operational and technical support to LEAs [law enforcement agencies] for immediate reaction to urgent cyber incidents and/or cyber crises via stand-by duty and the EU Law Enforcement Emergency Response Protocol" (Europol: European Cybercrime Centre - EC3).

The EC3 publishes the Internet Organised Crime Threat Assessment (IOCTA) annually.[161] The EC3 further houses the Joint Cybercrime Action Taskforce (J-CAT)[162], which is tasked with facilitating information-driven and coordinated action against key cybercriminal threats through cross-border investigations and operations by its partners. Upon request, Europol can assist Member State competent authorities "in responding to cyberattacks of suspected criminal origin" (Art. 4(1), point (m)). This assistance may also encompass the "support necessary for competent authorities of the Member States to interact with private parties, in particular by providing the necessary infrastructure for such interaction, for example, when competent authorities of the Member States [...] exchange information with private parties in the context of cyberattacks" (recital (42), Regulation 2022/991). Europol maintains the Secure Information Exchange Network Application (SIENA) for information exchange purposes.

As part of its tasks, Europol shall cooperate with ENISA, particularly "through the exchange of information and provision of analytical support" (Art. 4(1), point (j) Regulation 2016/794). Europol is a member of the EUCTF. It participates in EMPACT, EC3 provides its secretariat. Every six months, Europol and INTCEN jointly produce a threat analysis transmitted to the COSI (Council of the EU), to which Europol can also be invited as an observer. The EDPS has a supervisory role over Europol regarding the lawful processing of personal data. Among the EC3's partners at the EU level are the CERT-EU, Eurojust, ENISA, and the Commission. The HPWCI maintains cooperative relations with Europol. The Regulation establishing the ECCC provides for cooperative working relations with Europol. The EDA, CERT-EU, EC3, and ENISA concluded a Memorandum of Understanding for cooperation and exchange in the field of cybersecurity in 2018. The members of the EC3's Programme Board, inter alia, comprise CERT-EU, the EDA, the EEAS, ENISA, Eurojust, the Commission, and the EUCTF. Europol is a member of eu-LISA's Management Board

161 Past IOCTAs can be found here.

162 For more information on the J-CAT see Europol: Joint Cybercrime Action Taskforce (J-CAT.

in an observational capacity and participates in some of its advisory groups. Europol is among the entities invited to designate a representative to participate in the ENISA AG.

Further information:

- Europol: Cybercrime
- Europol: EC3 Partners
- Europol: EC3 Programme Board
- Europol: European Cybercrime Centre - EC3
- Europol: Joint Cybercrime Action Taskforce (J-CAT)
- Europol: Secure Information Exchange Network Application (SIENA)

— European Union Agency for the Cooperation of Energy Regulators (ACER)

Year of establishment: 2011

Legal basis: ﷺ Regulation establishing a European Union Agency for the Cooperation of Energy Regulators (2019/942)

Website: www.acer.europa.eu

ACER assists EU Member States' energy regulatory authorities in exercising their regulatory tasks, "coordinat[ing] their action" and "mediat[ing] and settl[ing] disagreements between them" (Art. 1(2), Regulation 2019/942). It is also tasked with contributing to the "establishment of high-quality common regulatory and supervisory practices" (Art. 1(2), Regulation 2019/942). As part of its mandate, ACER also undertakes cybersecurity-related tasks to reinforce "the cybersecurity of Europe's energy system."[163] To this end, ACER "provide[s] expert advice on EU legislation and cyber rules relating to the energy sector," for instance, in relation to the Network Code on Cybersecurity,[164] cooperates and shares information with Member States' energy regulators through "a dedicated cybersecurity task force"[165] and works towards "foster[ing] best practices globally", for instance, in the area of standardization.[166]

163 Agency for the Cooperation of Energy Regulators: ACER and Cybersecurity.

164 For instance, see Agency for the Cooperation of Energy Regulators: ACER Webinar on its Proposal for a Framework Guideline to Establish a Network Code on Cybersecurity.

165 See also Agency for the Cooperation of Energy Regulators: ACER Working Groups and Task Forces.

166 Agency for the Cooperation of Energy Regulators: ACER and Cybersecurity.

ACER works with national energy regulatory authorities and the European Networks of Transmission System Operators for Electricity and for Gas (ENTSO-E, ENTSOG) to "monitor the implementation of the Union-wide network-development plans" regarding "trans-European energy infrastructure" (Art. 11 Regulation 2019/942). In its cybersecurity-related efforts, ACER, inter alia, collaborates with ENISA, DG ENER and the DG JRC within the Commission.

Further information:

- Agency for the Cooperation of Energy Regulators: ACER and Cybersecurity
- Agency for the Cooperation of Energy Regulators: Our Mission

— European Union Agency for the Space Programme (EU-SPA)

Year of establishment: 2004

Legal basis: ﷺ Regulation establishing the Union Space Programme and the European Union Agency for the Space Programme (2021/696)Regulation establishing the Union Space Programme and the European Union Agency for the Space Programme (2021/696)

Website: www.euspa.europa.eu

EUSPA is responsible for implementing the EU Space Programme at the operational level. Among other tasks, it provides "state-of-the-art, safe and secure positioning, navigation and timing services based on Galileo and EGNOS" and fosters "the development of a vibrant European space ecosystem by providing market intelligence, and technical know-how to innovators, academia, start-ups, and SMEs."[167] As the "security gatekeeper of the EU Space Programme", EUSPA is also responsible for the "operational security, security monitoring and the security accreditation of the EU Space Programme."[168] In this respect, it provides "cybersecurity and engineering competence" for all its components and acts as "space security monitoring and operations centre in the EU."[169]

In fulfilling these functions, EUSPA cooperates with the Commission, CERT-EU and ENISA. EUSPA supports the Commission with regard to the EU Space Information

167 European Union Agency for the Space Programme: About EUSPA.

168 European Union Agency for the Space Programme: EU Space and security.

169 European Commission (2023): European Union Space Strategy for Security and Defence.

Sharing and Analysis Centre (EU Space ISAC) and the Euro Quantum Communication Infrastructure (EuroQCI). EUSPA is represented in the IICB.

Further information:

- European Union Agency for the Space Programme: About EUSPA
- European Union Agency for the Space Programme: EU Space and security
- European Union Agency for the Space Programme: Operational security

— European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)

Year of establishment: 2011

Legal basis: ﷺ Regulation on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) (2018/1726)

Website: www.eulisa.europa.eu

eu-LISA manages integrated, large-scale IT systems, that ensure the internal security of the Schengen Area. For instance, these systems allow the exchange of visa data between Schengen Area countries and the determination of responsibility amongst EU countries in the examination of a particular asylum application. eu-LISA further tests new technologies to help create a more modern, effective, and secure border management system in the EU. In developing or managing its IT systems, eu-LISA "shall consult and follow the recommendations of [ENISA] regarding network and information security, where appropriate" (Art. 41(3) Regulation 2018/1726). eu-LISA "shall ensure [...] an appropriate level of data and physical security" (Art. 2, point (g) Regulation 2018/1726), for instance, by

- "adopt[ing] appropriate measures, including security plans, inter alia, to prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or transport of data media, in particular by means of appropriate encryption techniques" and
- making sure that "all system-related operational information circulating in the communication infrastructure [is] encrypted" (Art. 11(3) Regulation 2018/1726).

eu-LISA maintains cooperative relations with the Council of the EU, the Commission, Eurojust, Europol and the EDPS. Eurojust and Europol are also represented on eu-LISA's Management Board as observers and in some of its advisory groups. ENISA and eu-LISA concluded a three-year cooperation plan at the beginning of 2021 to

strengthen the exchange of knowledge and expertise in the field of information security among other areas for cooperation. eu-LISA is among the entities invited to designate a representative to participate in the ENISA AG.

Further information:

- eu-LISA: eu-LISA Security

— European Union Aviation Safety Agency (EASA)

Year of establishment: 2002

Legal basis: ﷺ Regulation on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency (2018/1139)

Website: www.easa.europa.eu

The EASA shall work towards "ensuring the proper functioning and development of civil aviation in the Union" (Art. 75(2), Regulation 2018/1139). To this end, it is, inter alia, tasked with assisting the Commission and Member States, "carry[ing] out, on behalf of Member States, functions and tasks ascribed to them by applicable international conventions, in particular the Chicago Convention" and "promot[ing] Union aviation standards and rules at international level" (Art. 75(2), Regulation 2018/1139). Its mandate also extends to incorporating the consideration of "cyber risks [...] during aircrafts design, development and operation"[170] and subsequent controls thereof. In 2017, the EASA established the European Centre for Cybersecurity in Aviation (ECCSA), a voluntary network among stakeholders in the civil aviation sector, including national aviation authorities. EASA further maintains the European Strategic Cooperation Platform (ESCP) and a Network of Cybersecurity Analysts (NoCA), which comprises Members from the EASA and Member States' aviation authorities.

The EASA is instructed to cooperate with the Commission and Member States "on security matters related to civil aviation, including cyber security, where interdependencies between civil aviation safety and security exist" (Art. 88 1) Regulation 2018/1139). Member States and the Commission are also represented on the EASA's Management Board.

170 European Union Aviation Safety Agency: Cybersecurity Overview.

Further information:

- European Union Aviation Safety Agency: Cybersecurity
- European Union Aviation Safety Agency: European Centre for Cybersecurity in Aviation (ECCSA)
- European Union Aviation Safety Agency: European Strategic Coordination Platform (ESCP)
- European Union Aviation Safety Agency: Network of Cybersecurity Analysts (NoCA)

— European Cybersecurity Competence Centre (ECCC)

Year of establishment: 2021

Legal basis: ﷺ Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (2021/887)

Website: cybersecurity-centre.europa.eu

The European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), located in Bucharest, was established to

- "strengthen [the Union's] leadership and strategic autonomy in the area of cybersecurity by retaining and developing the Union's research, academic, societal, technological and industrial cybersecurity capacities and capabilities necessary to enhance trust and security, including the confidentiality, integrity and accessibility of data, in the Digital Single Market",
- "support Union technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software in the Union",
- "increase the global competitiveness of the Union's cybersecurity industry, ensure high cybersecurity standards throughout the Union and turn cybersecurity into a competitive advantage for other Union industries" (Art. 3(1) Regulation 2021/887),

by "promoting research, innovation and deployment in the area of cybersecurity" (Art. 4(1) Regulation 2021/887). To this end, the ECCC is, inter alia, mandated to "establish[...] strategic recommendations for research, innovation and deployment in cybersecurity" and "implementing actions under relevant Union funding programmes" (Art. 4(3), Regulation 2021/887). To fulfill its missions, the ECCC engages in two sets of activities, further specified below:

Strategic Tasks	Implementation Tasks

Art. 5 (2)	Art. 5 (3)
Among others, for instance, • "developing and monitoring the implementation of the Agenda" • "ensuring synergies between and cooperation with relevant Union institutions, bodies, offices and agencies, in particular ENISA" • "providing expert cybersecurity industrial, technology and research advice to Member States at their request, including with regard to the procurement and deployment of technologies" • "facilitating collaboration and the sharing of expertise among all relevant stakeholders"	Among others, for instance, • "coordinating and administrating the work of the Network and the Community in order to fulfil the [ECCC's] mission […], in particular by supporting cybersecurity start-ups, SMEs, microenterprises, associations and civic technology projects in the Union and facilitating their access to expertise, funding, investment and markets" • "establishing and implementing the annual work programme […] for the cybersecurity parts of" Digital Europe Programme, Horizon Europe joint actions and others as provided for • "carrying out or enabling the deployment of ICT infrastructure and facilitating the acquisition of such infrastructure, for the benefit of society, industry and the public sector, at the request of Member States, research communities and operators of essential services"

The ECCC is responsible for implementing the call for proposals for cybersecurity projects within the Horizon Europe cluster Civil Security for Society as outlined in the 2023-2024 work programme. Regulation 2021/887 establishes the ECCC until 31 December 2029.

The ECCC "shall carry out [its strategic and implementation tasks] in close cooperation with the Network" (Art. 5(4), Regulation 2021/887) and shall "undertake [its] tasks in collaboration with ENISA and the Community, as appropriate" (Art. 3(2), Regulation 2021/887). The ECCC "shall [further] cooperate with relevant" EUIBAs, among them the EEAS, EC3, the EDA, the DG JRC, European Research Executive Agency, the European Research Council Executive Agency, the European Health and Digital Executive Agency, in order to "ensure consistency and complementarity while avoiding any duplication of effort" (Art. 10(1), Regulation 2021/887). The ECCC and the EDA shall work towards formalizing their cooperative relationship through a working arrangement to "facilitate information sharing among respective staffs on respectively civil, dual use and defence technology priorities."[171] *Member States and the Commission are represented on the ECCC's Governing Board. ENISA is represented in the Board through a permanent observer. The ECCC is represented in the IICB. The ECCC is supported by a Strategic Advisory Group*

171 Council of the European Union: Council Conclusions on the EU Policy on Cyber Defence (9618/23).

consisting of Cybersecurity Competence Community Member representatives from entities other than EUIBAs.

Further information:

- European Cybersecurity Competence Centre and Network: About Us
- European Cybersecurity Competence Centre and Network (2023): Strategic Agenda

— European Defence Agency (EDA)

Year of establishment: 2004

Legal basis: ** Council Decision defining the statute, seat and operational rules of the European Defence Agency (2015/1835)

Website: eda.europa.eu

The European Defence Agency supports all EU Member States "in developing their capabilities to improve cyber resilience."[172] Specifically, the EDA supports, among other things, the creation of a risk management model for cybersecurity in the context of military capability supply chains, the establishment of the Cyber Ranges Federation project, the development of specific capabilities for Advanced Persistent Threat (APT) detection, and cyber situational awareness. The EDA informs Member States annually "on the landscape of emerging technologies, including those applicable to cyber defence."[173] The EDA is responsible for the management of the Military Computer Emergency Response Team Operational Network (MICNET), which was established in 2013.

The EDA is subordinate to the Council of the EU, to which it reports and from which it receives its guidance. The High Representative of the EU for Foreign Affairs and Security Policy also assumes the role of EDA head. The Steering Board of the EDA meets at the level of the Member States' defense ministers. Together with the EEAS, the EDA jointly manages all secretarial functions for the PESCO.[174] *The EDA is represented on the Steering Board of the PESCO project CIDCC and the EC3 Programme Board. The EDA signed a Memorandum of Understanding with ENISA, the EC3, and CERT-EU, intending to develop a cooperation framework among the*

172 European Defence Agency: Cyber.

173 European Commission: EU Policy on Cyber Defence (JOIN(2022) 49 final).

174 For a description of all PESCO projects with a cybersecurity-related component see a respective explanation in the section on cyber defence within Policy Area 7.

entities. The EDA and the ECCC shall work towards formalizing their cooperative relationship through a working arrangement to "facilitate information sharing among respective staffs on respectively civil, dual use and defence technology priorities."[175]

Further information:

- European Defence Agency: Cyber
- European Defence Agency: Cyber defence R&T - CapTech Cyber
- European Defence Agency: EDA-led network of cyber defence teams starts with 18 EU countries

— European Supervisory Authorities (ESAs)

Year of establishment: 2011

Legal basis:

- ﷺ Regulation establishing a European Supervisory Authority (European Banking Authority) (1093/2010)
- ﷺ Regulation establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority) (1094/2010)
- ﷺ Regulation establishing a European Supervisory Authority (European Securities and Markets Authority) (1095/2010)

Website: www.eba.europa.eu | www.eiopa.europa.eu | www.esma.europa.eu

Together, the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA) form the so-called European Supervisory Authorities (ESAs) tasked with financial supervision. As part of the mandate of each entity, their respective legal bases, among others, stipulate that the ESAs shall promote "an effective bilateral and multilateral exchange of information between competent authorities, pertaining to all relevant issues, including cyber security and cyber-attacks" (Art. 29(1), point (b), Regulations 1093/2010, 1094/2010, and 1095/2010). The ESAs cooperate and coordinate their work through a Joint Committee, for which cybersecurity constitutes one of its priorities (Art. 54(2), Regulations 1093/2010, 1094/2010 and 1095/2010).

The ESAs "may participate in the activities of the [NIS] Cooperation Group for matters that concern their supervisory activities in relation to financial entities" and

175 Council of the European Union: Council Conclusions on the EU Policy on Cyber Defence (9618/23).

"may request to be invited to participate in the activities of the [NIS] Cooperation Group for matters in relation to essential or important entities [...] that have also been designated as critical ICT third-party service providers" within the DORA Regulation (Art. 47(1) Regulation 2022/2554). The DORA Regulation provides for the establishment of an Oversight Forum as a subcommittee of the Joint Committee to support the Lead Overseer and Joint Committee in the area of ICT third-party risk. In the context of the DORA Regulation, the ESAs are involved in the drafting of common draft regulatory and implementing technical standards DORA (see further DORA Deep Dive) and shall report annually on major ICT-related incidents through its Joint Committee. In June 2024, ENISA and the ESAs concluded an MoU for increased cooperation and information-sharing among each other.[176]

EU Interinstitutional Services

— Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU)

Year of establishment: 2011

Legal basis: ﷺ Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (2023/2841)[177]

Website: cert.europa.eu

CERT-EU is the computer emergency response team for Union entities. Concerning the entities' unclassified networks[178] , it acts as "their cybersecurity information exchange and incident response coordination hub" and contributes to the "prevent[ion], detect[ion], handl[ing], mitigat[ion], respon[se] to and recover[y] from incidents" (Art. 13(1) Regulation 2023/2841). To this end, CERT-EU is tasked with "collect[ing], manag[ing], analy[zing] and shar[ing] information with the Union entities on cyber threats, vulnerabilities and incidents in unclassified ICT infrastructure" and "coordinat[ing][179] responses to incidents at interinstitutional

176 European Securities and Markets Authority: ESAs and ENISA sign a Memorandum of Understanding to strengthen cooperation and information exchange.

177 Concerning CERT-EU, it is important to note that "the provisions of [...] Regulation [2023/2841] prevail over the provisions of the [2018] Interinstitutional arrangement on the organisation and operation of CERT-EU" (recital (18), Regulation 2023/2841).

178 CERT-EU's scope of action may only involve the provision of assistance towards EUIBAs "regarding incidents in network and information systems handling EUCI where it is explicitly requested to do so by the Union entities concerned in accordance with their respective procedures" (Art. 13(8) Regulation 2023/2841).

179 For instance, CERT-EU assumes an incident response coordination function in relation to "contributi[ng] to consistent external communication", "mutual support [...] or providing assistance", the "optimal use of operational resources" and the "coordination with other crisis response mechanisms at Union level" (Art. 22(2) Regulation 2023/2841), where relevant together with ENISA.

and Union entity level" (Art. 13(2) Regulation 2023/2841). It supports Union entities, inter alia, by assisting with the (coordinated) implementation of Regulation 2023/2841 and notifying the IICB on any related challenges, providing CSIRT baseline services, and "coordinat[ing] the management of major incidents" (Art. 13(3) Regulation 2023/2841). In relation to its support for implementing Regulation 2023/2841, CERT-EU is empowered to "issu[e] (a) calls for action describing urgent security measures that Union entities are urged to take within a set timeframe; (b) proposals to the IICB for guidelines addressed to all or a subset of the Union entities; [or] (c) [...] for recommendations addressed to individual Union entities" (Art. 14(1) Regulation 2023/2841).[180] In line with the requirements set out in NIS 2, CERT-EU assumes the function of CVD coordinator for all EU entities. CERT-EU also offers additional chargeable services to Union entities, such as "a proactive scanning of the network and information systems of the Union entity concerned to detect vulnerabilities with a potential significant impact" (Art. 13(6) Regulation 2023/2841 lists all of these services). CERT-EU houses six teams working on forensics and operational response to cyber events; cyber threat intelligence; offensive security; DevSecOps, cooperative relationships; and security consultation. CERT-EU also publishes security advisories, security guidance, and other threat-intelligence-related reports, such as a monthly "Cyber Security Brief" on its website.

Institutionally, CERT-EU is located within DG DIGIT. However, its status is that of an "autonomous interinstitutional service provider for all Union entities" (Art. 16(1) Regulation 2023/2841). The IICB "supervis[es] the implementation of general priorities and objectives by CERT-EU and provid[es] strategic direction to CERT-EU" (Art. 10(2), point (b), Regulation 2023/2841). Upon approval by the IICB, the Commission appoints the head of CERT-EU. He or she must regularly report to the IICB's chair and provide annual reports "on the activities and performance of CERT-EU during the reference period" (Art. 15(5) Regulation 2023/2841) addressed to both the IICB and its chair. CERT-EU's head may participate in IICB discussions as an observer. Regulation 2023/2841 puts in place reporting obligations for EUIBAs when facing a significant incident, of which they shall notify CERT-EU. CERT-EU assists the Commission "on the coordinated management of large-scale cybersecurity incidents and crises" (Art. 17(1) Regulation 2023/2841) in the framework of EU-CyCLONe. CERT-EU is a member of the CSIRTs Network. CERT-EU shall maintain a "structured cooperation with ENISA on capacity building, operational cooperation and long-term strategic analyses of cyber threats" (Art. 13(5) Regulation 2023/2841). CERT-EU may "cooperate or exchange information" (Art. 13(5) Regulation 2023/2841) with the EC3. Regulation 2023/2841 also allows the CERT-EU to "cooperate and exchange

180 Art. 14(2) provides examples for guidelines and recommendations that may be issued by CERT-EU to that end.

information" with the EC3 (Europol). A Memorandum of Understanding for cooperation and exchange in the field of cybersecurity was concluded between EDA, EC3, ENISA, and CERT-EU. Apart from cooperation at the Union level, CERT-EU "shall, without undue delay, cooperate and exchange information with Member State counterparts, [...] with regard to incidents, cyber threats, vulnerabilities, near misses, possible countermeasures as well as best practices and on all matters relevant for improving the protection of the ICT environments of Union entities" (Art. 17(1) Regulation 2023/2841), also within the framework of the CSIRTs Network. This exchange of information with Member State authorities shall also specifically extend to situations where CERT-EU "becomes aware of a significant incident occurring within the territory of a Member State", which shall be notified to the respective Member State "without delay" (Art. 17(2) Regulation 2023/2841). CERT-EU is among the entities invited to designate a representative for participation in the ENISA AG. CERT-EU is represented on the EC3 Programme Board. In fulfilling its functions, EUSPA, inter alia, cooperates with CERT-EU.

Further information:

- CERT-EU: About Us
- CERT-EU: Publications

EU-internal Coordination Bodies

— Interinstitutional Cybersecurity Board (IICB)

Year of establishment: 2024

Legal basis: ﷺ Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (2023/2841)

The IICB was established through Regulation 2023/2841, laying down cybersecurity obligations for every EU entity. Its mandate is twofold: first, it shall observe and contribute to the implementation of these obligations by Union entities, and second, with respect to CERT-EU, it assumes supervisory functions and "provid[es...] strategic direction" (Art. 10(2), point (b) Regulation 2023/2841) to it. Relating to the former, it shall develop a "multiannual strategy on raising the level of cybersecurity in the Union entities" (Art. 11, point (c) Regulation 2023/2841), to be updated at least every five years. To ensure compliance with the regulation, it can, in cases of perceived contravention, for instance, issue warnings, recommend an audit, or advise that "all Member States and Union entities

implement a temporary suspension of data flows to the Union entity concerned" (Art. 12(2), point (g) Regulation 2023/2842). Every year, the IICB shall provide the European Parliament and the Council of the EU with a report on the "progress made with the implementation of [...] Regulation [2023/2841] and specifying in particular the extent of cooperation of CERT-EU with Member State counterparts" (Art. 10(4), Regulation 2023/2842).[181] The IICB convenes at least three times annually. CERT-EU or any IICB member may request an additional meeting. The Board can set up designated technical advisory groups to assume particular functions. The IICB is responsible for monitoring and ensuring the compliance of EUIBAs with Regulation 2023/2841.

Members of the IICB are one representative each by the European Parliament, the European Council, the Council of the EU, the Commission, the EU's Court of Justice, the ECB, the Court of Auditors, EEAS, the European Economic and Social Committee, European Committee of the Regions, the European Investment Bank, the ECCC, ENISA, the EDPS, and the European Union Agency for the Space Programme. In addition, it comprises three representatives to be assigned by the EU Agencies Network[182] *(EUAN) to "represent the interests of the bodies, offices and agencies of the Union [other than those previously mentioned] that run their own ICT environment" (Art. 10(3), point (b), Regulation 2023/2841). As observers, the head of CERT-EU, as well as the Chairs of the NIS Cooperation Group, the CSIRTs Network, and EU-CyCLONe may participate in IICB discussions. The Commission provides the IICB's secretariat. With the support of ENISA, the IICB shall contribute to setting up an informal group that comprises Union entities' designated local cybersecurity officers. The appointment of the Head of the CERT-EU by the Commission depends on a prior approval by at least two-thirds of the IICB members. On an annual basis, and for the first time by 8 January 2025, the IICB submits a progress report on the implementation of Regulation 2023/2841 and CERT-EU-Member State cooperation to the Council and European Parliament. Every three months, CERT-EU provides the IICB with a "summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities" (Art. 21 (8) Regulation 2023/2841).*

181 The Regulation further specifies that this report "shall constitute an input to the biennial report on the state of cybersecurity in the Union" (Art. 10(14), Regulation 2023/2841) to be adopted by ENISA under the NIS 2 Directive.

182 The EUAN seeks to enhance collaboration between EU agencies. As one of its sub-networks, the EUAN comprises an ICT Advisory Committee of the EU Agencies, the ICTAC. The ICTAC, which meets twice a year, aims to serve as a forum to exchange best practices, experience, and knowledge. It provides a mechanism to develop common positions and aims to contribute to cooperation among themselves, for example, by sharing resources and best practices in the development, maintenance, or deployment of new ICT systems. From the actors covered within this compendium, ACER, EASA, EBA, EIOPA, ENISA, ESMA, eu-LISA, Eurojust, Europol, EUSPA and the ECCC are members of the EUAN. The EDA participates as an observer. For further information see EU Agencies Network: Our role, governance and strategy and EU Agencies Network: 2024-2025 Work Programme of the EU Agencies Network.

EU-Member State Coordination Bodies

— Computer Security Incident Response Teams Network (CSIRTs Network)

Year of establishment: 2016

Legal basis: ﷺ Directive on measures for a high common level of cybersecurity across the Union (NIS 2, Directive 2022/2555)

Website: csirtsnetwork.eu

The CSIRTs Network was established through both NIS Directives and aims to contribute to existing, trusted operational cooperation between Member States. It provides a forum for cooperation and developing a coordinated response to cross-border cybersecurity incidents. The NIS 2 Directive assigns to it the following tasks (non-exhaustive):

- exchanging
  - information on "CSIRTs' capabilities",
  - "relevant information about incidents, near misses, cyber threats, risks and vulnerabilities",
  - "information with regard to cybersecurity publications and recommendations",
  - "information in relation to [a particular] incident and associated cyber threats, risks and vulnerabilities" ("at the request of a member of the CSIRTs network potentially affected by an incident")
- "facilitat[ing] the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs",
- "at the request of a member of the CSIRTs network, discuss[ing] and, where possible, implement[in] a coordinated response to an incident that has been identified within the jurisdiction of that Member State",
- "provid[ing] Member States with assistance in addressing cross-border incidents",
- "cooperat[ing], exchang[ing] best practices and provid[ing] assistance to the CSIRTs designated as [CVD coordinators] with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State" (Art. 15(3) NIS 2 Directive).

The CSIRTs Network consists of representatives of the designated national CSIRTs and CERT-EU. The Commission participates in the network as an observer. ENISA acts as its secretariat and is further tasked with "actively provid[ing] assistance for the cooperation among the CSIRTs" (Art. 15(2) NIS 2 Directive). The CSIRTs Network receives its strategic guidance from the NIS Cooperation Group. The CSIRTs Network and EU-CyCLONe shall cooperate closely based on respective procedural arrangements.

Every two years (for the first time by 17 January 2025), the CSIRTs Network shall report to the NIS Cooperation Group on the "progress made with regard to [...] operational cooperation" (Art. 15(4) NIS 2 Directive). The Chair of the CSIRTs Network may participate in IICB discussions as an observer. The CSIRTs Network shall receive a "summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities" (Art. 21(8) Regulation 2023/2841) by CERT-EU every three months. Twice a year, ENISA shares with the CSIRTs Network its notification-related findings (Art. 23(9) NIS 2 Directive). When Member States determine that a reported vulnerability "could have a significant impact on entities in more than one Member State," the national CVD coordinators shall interact with their counterparts in other EU Member States within the framework of the CSIRTs Network (Art. 12(1) NIS 2 Directive).

Further information:

- CSIRTs Network: CSIRTs Network Members
- European Union Agency for Cybersecurity: CSIRTs Network

— Critical Entities Resilience Group (CERG)

Year of establishment: 2023

Legal basis: ﷺ Directive on the resilience of critical infrastructures (CER Directive, Directive 2022/2557)

The CER Directive establishes the Critical Entities Resilience Group (CERG) to "support the Commission and facilitate cooperation among Member States and the exchange of information on issues relating to this Directive" (Art. 19(1) CER Directive). The CER Directive assigns to it the following tasks (non-exhaustive):

- "supporting the Commission in assisting Member States in reinforcing their capacity to contribute to ensuring the resilience of critical entities;"
- "facilitating the exchange of best practices with regard to the identification of critical entities by the Member States;"
- "exchanging best practices related to the notification of incidents;"
- "exchanging information and best practices on innovation, research and development relating to the resilience of critical entities" (Art. 19(3) CER Directive).

The CERG operates on a system of biennial work programs, with the first to be adopted by 17 January 2025 (Art. 19(4) CER Directive). The Commission is empowered to "adopt implementing acts laying down procedural arrangements necessary for the functioning of the Critical Entities Resilience Group" (Art. 19(6)

CER Directive). The Commission is further mandated to provide the CERG with a summary report on information received by Member States on their national strategies on the resilience of critical entities and risk assessments at least every four years (for the first time by 17 January 2027).

Representatives of EU Member States and the Commission take part in the CERG. The CERG is chaired by the Commission's representative. External stakeholders can participate when relevant. The European Parliament can request participation, upon which the Commission may invite experts of the European Parliament to attend the Group's meetings. At least once a year, the CERG shall convene with the NIS Cooperation Group for a joint meeting.

— European Cyber Crisis Liaison Organisation Network (EU-CyCLONE)

Year of establishment: Launched in 2020, formally established in 2023

Legal basis: ﷺ Directive on measures for a high common level of cybersecurity across the Union (NIS 2, Directive 2022/2555)

The idea for a European Cyber Crisis Liaison Organisation Network (CyCLONe) was first introduced within the European Commission's Blueprint for a coordinated reaction to large, transnational cybersecurity incidents and crises. Its establishment has been formalized through the NIS 2 Directive. Among EU-CyCLONe's objectives are to "support the coordinated management of large-scale cybersecurity incidents and crises at operational level" (Art. 16(1) NIS 2 Directive). The NIS 2 Directive assigns to it the following tasks:

- "increas[ing] the level of preparedness of the management of large-scale cybersecurity incidents and crises;"
- "develop[ing] a shared situational awareness for large-scale cybersecurity incidents and crises;"
- "assess[ing] the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;"
- "coordinat[ing] the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;" and
- "discuss[ing], upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans" (Art. 16(3) NIS 2 Directive).

In the past, various exercises have taken place in the framework of EU-CyCLONe (CySOPex and BlueOLEx).

EU-CyCLONe comprises the cyber crisis management authorities (designated as such under Art. 9 NIS 2 Directive, the Cyber Crises Liaison Organisations (CyCLOs)) of all

EU Member States and the Commission in an observational capacity. The Commission may only actively take part in EU-CyCLONe's deliberations when "a potential or ongoing large-scale cybersecurity incident [occurs that] has or is likely to have a significant impact on services and activities" (Art. 16(2) NIS 2 Directive). A Member State representative of the respective current EU presidency chairs EU-CyCLONe. ENISA acts as the network's secretariat and it is tasked with "support[ing] the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information" (Art. 16(2) NIS 2 Directive). Additionally, ENISA also facilitates "the organisation of exercises for CyCLONe members, such as CySOPex (played by officers) and BlueOLEx (played by executives)."[183] *CERT-EU assists the Commission in relation to "the coordinated management of large-scale cybersecurity incidents and crises" (Art. 17(1) Regulation 2023/2841) in the framework of EU-CyCLONe. EU-CyCLONe receives strategic guidance from the NIS Cooperation Group. EU-CyCLONe and the CSIRTs Network shall cooperate closely on the basis of respective procedural arrangements (Art. 16 6) NIS 2 Directive). The network shall report regularly to the NIS Cooperation Group on "the management of large-scale cybersecurity incidents and crises, as well as trends, focusing in particular on their impact on essential and important entities" (Art. 16(5) NIS 2 Directive). Additionally, every 18 months and for the first time by 18 July 2024, EU-CyCLONe must report to the European Parliament and the Council about its work (Art. 16(7) NIS 2 Directive). The Chair of EU-CyCLONe may participate in IICB discussions as an observer. Member States must submit to EU-CyCLONe "relevant information relating to [...] their national large-scale cybersecurity incident and crisis response plans" at the maximum three months after their adoption (Art. 9(5) NIS 2 Directive).*

Further information:

- European Union Agency for Cybersecurity: EU CyCLONe

— European Cybersecurity Certification Group (ECCG)

Year of establishment: 2019

Legal basis: ** Regulation on ENISA and on information and communications technology cybersecurity certification (2019/881)

The European Cybersecurity Certification Group (ECCG) was established with the

183 ENISA: EU CyCLONe.

2019 Cybersecurity Act. It is tasked, inter alia, with carrying out the following activities:

- "advis[ing] and assist[ing] the Commission in its work to ensure the consistent implementation and application of" the Cybersecurity Certification Framework;
- "assist[ing], advis[ing] and cooperat[ing] with ENISA in relation to the preparation of a candidate scheme;"
- "adopt[ing] an opinion on candidate schemes prepared by ENISA;"
- "request[ing] ENISA to prepare candidate schemes;"
- "adopt[ing] opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;"
- "facilitat[ing] the cooperation between national cybersecurity certification authorities;"
- and "facilitat[ing] the alignment of European cybersecurity certification schemes with internationally recognised standards" (Art. 62(4), Regulation 2019/881).

The ECCG comprises "representatives of national cybersecurity certification authorities or representatives of other relevant national authorities" (Art. 62(2) Regulation 2019/881), with the Member States being represented by a maximum of one member. The Commission, assisted by ENISA, chairs the ECCG and provides its Secretariat. The ECCG cooperates with the SCCG.

Further information:

- European Commission: The European Cybersecurity Certification Group

— European Union Cybercrime Task Force (EUCTF)

Year of establishment: 2010

The European Union Cybercrime Task Force (EUCTF) seeks to "develop and promote a harmonised approach within the European Union to the criminal misuse of information and communication technology and the fight against cybercrime."[184] Functioning as a network, the EUCTF meets two times annually to "identify, discuss and prioritise the key challenges and actions."[185]

Europol, the European Commission, and Member States jointly set up the EUCTF. Its members are the National Cybercrime Units of the Member States and a few associated

184 Europol: European Union Cybercrime Task Force.

185 Ibid.

non-EU countries, as well as representatives of the Commission, Eurojust, and Europol. EC3 provides its secretariat. The ECTF is a member of EC3's Programme Board.

Further information:

- Europol: European Union Cybercrime Task Force

— NIS Cooperation Group

Year of establishment: 2016

Legal basis: ﷺ Directive on measures for a high common level of cybersecurity across the Union (NIS 2, Directive 2022/2555)

Website: digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

The first Directive on Security of Network and Information Systems (NIS Directive) put in place a Cooperation Group, whose establishment has been renewed through its successor, the NIS 2 Directive. The NIS Cooperation Group seeks to facilitate strategic cooperation and the exchange of information between Member States. Its tasks comprise the provision of guidance to national competent authorities "in relation to the transposition and implementation" of the NIS 2 Directive as well as the "development and implementation of policies on coordinated vulnerability disclosure" (Art. 14(4) NIS 2 Directive). The NIS 2 Directive assigns to it the following further tasks (non-exhaustive):

- "exchang[ing] best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications as well as the identification of essential and important entities;"
- "exchang[ing] advice and cooperat[ing] with the Commission on emerging cybersecurity policy initiatives and the overall consistency of sector-specific cybersecurity requirements;"
- "exchang[ing] views on the implementation of sector-specific Union legal acts that contain provisions on cybersecurity;"
- "discuss[ing] and carry[ing] out on a regular basis an assessment of the state of play of cyber threats or incidents, such as ransomware;"
- "carry[ing] out coordinated security risk assessments of critical supply chains;"
- "contribut[ing] to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the competent authorities or the CSIRTs;"
- "exchang[ing] views on the policy on follow-up actions following large-scale cybersecurity incidents and crises on the basis of lessons learned of the CSIRTs

network and EU-CyCLONe" (Art. 14(4) NIS 2 Directive).

The NIS Cooperation meets regularly[186] and operates on a system of biennial work programs. It acts based on consensus and can set up subgroups to work on specific questions related to its work. As part of its mandate, the NIS Cooperation Group can develop and publish non-binding guidelines and documents.[187] The Commission is empowered to "adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group" (Art. 14(8) NIS 2 Directive).[188]

The NIS Cooperation Group consists of representatives of Member States, the European Commission (acting as the secretariat), and ENISA. The EEAS participates in an observational capacity. The NIS Cooperation Group is chaired by the respective Member State holding the Presidency of the Council of the European Union. For instance, when they concern their "supervisory activities in relation to financial entities" (Art. 47(1) DORA Regulation), the European supervisory authorities and designated national competent authorities under the DORA Regulation may participate in NIS Cooperation Group activities. In addition, representatives of the European Parliament or other "relevant stakeholders" may be invited. The Group "provide[s] strategic guidance to the CSIRTs Network and EU-CyCLONe on specific emerging issues" (Art. 14(4), point (l) NIS 2 Directive). It can request the former to provide it with a "technical report on selected topics" (Art. 14(6) NIS 2 Directive). ENISA shares its notification-related findings twice a year with the NIS Cooperation Group (Art. 23(9) NIS 2 Directive). EU-CyCLONe shall report regularly to the NIS Cooperation Group on "the management of large-scale cybersecurity incidents and crises, as well as trends, focusing in particular on their impact on essential and important entities" (Art. 16(5) NIS 2 Directive). Every two years, for the first time by 17 January 2025, the CSIRTs Network shall report to the NIS Cooperation Group on the "progress made with regard to [...] operational cooperation" (Art. 15(4) NIS 2 Directive). At least once a year, the NIS Cooperation Group shall convene with the Critical Entities Resilience Group for a joint meeting. The Chair of the NIS Cooperation Group may participate in IICB discussions as an observer. The NIS 2 Directive provides for the Cooperation Group to "carry out [Union level] coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains" (Art. 22(1) NIS 2 Directive) based on (non-) technical risk considerations with the support of ENISA and the Commission. ENISA shall consult

186 The agendas of NIS Cooperation Group meetings can be found here. Member States also cooperate in the framework of the NIS Cooperation Group within dedicated workstreams, for instance, on 5G Cybersecurity or Energy. A full list of workstreams is not publicly available.

187 Past outputs of the NIS Cooperation Group can be found here. For instance, in January 2020, the NIS Cooperation Group published the EU Toolbox of risk mitigating measures in relation to the cybersecurity of 5G networks.

188 The respective Commission Implementing Decision currently in force predates the entry into force of the NIS 2 Directive.

the NIS Cooperation Group in developing and maintaining the European vulnerability database as stipulated in the NIS 2 Directive.

Further information:

- Commission Implementing Decision laying down procedural arrangements necessary for the functioning of the Cooperation Group (2017/179)
- European Commission: NIS Cooperation Group meetings agendas
- European Commission: NIS Cooperation Group Publications

Bodies With Stakeholder Involvement

— ENISA Advisory Group (ENISA AG)

Year of establishment: 2019

Legal basis: ﷺ Regulation on ENISA and on information and communications technology cybersecurity certification (2019/881)

The ENISA AG was established with the 2019 Cybersecurity Act. It is tasked with "advis[ing] ENISA in respect of the performance of ENISA's tasks" (Art. 21(5) Regulation 2019/881) in all areas except for cybersecurity certification. Its advisory function particularly relates to consulting the ENISA "Executive Director on the drawing up of a proposal for ENISA's annual work programme, and on ensuring communication with the relevant stakeholders on issues related to the annual work programme" (Art. 21(5) Regulation 2019/881).

The Group comprises a maximum of 33 "recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, SMEs, operators of essential services, consumer groups, academic experts in the field of cybersecurity, and representatives of competent authorities notified in accordance with [the Electronic Communications Code], of European standardisation organisations, as well as of law enforcement and data protection supervisory authorities" (Art. 21(1) Regulation 2019/881) and is chaired by ENISA's Executive Director or a designated alternate. Members of the AG serve a term of two and a half years. Experts from the Commission and Member States can attend meetings and participate in the work of the AG. The Executive Director of ENISA can invite representatives of other entities to participate in meetings without the right to vote. In addition to the 33 appointed stakeholder members, BEREC, Europol/EC3, eu-LISA, and CERT-EU, among other institutions, were invited to nominate representatives for the 2023–2025 term of ENISA AG. [189]

Further information:

- European Union Agency for Cybersecurity: Advisory Group (AG)
- European Union Agency for Cybersecurity: Decision No 2020/2 of the Management Board of the European Union Agency for Cybersecurity (ENISA) of 3 February 2020 on the Establishment and Operation of the Advisory Group

— Stakeholder Cybersecurity Certification Group (SCCG)

Year of establishment: 2019

Legal basis: ﷺ Regulation on ENISA and on information and communications technology cybersecurity certification (2019/881)

Upon the Cybersecurity Act's entry into force, a cybersecurity certification stakeholder group was established. The SCCG is tasked with

- "advis[ing] the Commission on strategic issues regarding the European cybersecurity certification framework" and "upon request, advis[ing] ENISA on general and strategic matters concerning ENISA's tasks relating to market, cybersecurity certification, and standardisation;"
- "assist[ing] the Commission in the preparation of the Union rolling work programme" for European cybersecurity certification;
- "issu[ing] an opinion on the Union rolling work programme;"
- and "in urgent cases, provid[ing] advice to the Commission and the ECCG on the need for additional certification schemes not included in the Union rolling work programme" (Art. 22(3) Regulation 2019/881).

The SCCG comprises representatives of European stakeholders, who are appointed by the Commission based on a proposal by ENISA. Representatives of the European Commission and ENISA jointly chair the SCCG. ENISA provides its Secretariat. The ECCG cooperates with the SCCG.

Further information:

- European Commission: Stakeholder Cybersecurity Certification Group

189 European Union Agency for Cybersecurity: Decision No 2023/02 of the Management Board of the European Union Agency For Cybersecurity (ENISA) Setting Up An Advisory Group for the Period 2023-2025.

Outlook: EU Cybersecurity Policies on the Horizon

In addition to the legal acts already covered within this compendium, a number of EU legislative and non-legislative initiatives of cybersecurity relevance have been announced, entered into force after May 2024, or can be expected to be adopted in due course.

Tables 43 and 44 keep track of these initiatives respectively (as of June 17, 2024):

Table 43: Status Quo of Initiatives for Legislative Acts of Cybersecurity Relevance as of June 17, 2024

Legislative Initiative	Policy Area	Status	Resources
Regulation on measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (Cyber Solidarity Act)	Overarching Policies	Close to adoption	• Link to Legislative Observatory entry • Link to Legislative Train entry • Text adopted by EP
Amendment of Cybersecurity Act on managed security services	Internal Market	Close to adoption	• Link to Legislative Observatory entry • Link to Legislative Train entry • Text adopted by EP
Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)	Internal Market	Close to adoption	• Link to Legislative Observatory entry • Link to Legislative Train entry • Text adopted by EP
Regulation on laying down harmonised rules on Artificial Intelligence (Artificial	Internal Market	Adopted, awaiting	• Link to Legislative

Intelligence Act)		publication in the EU's Official Journal	Observatory entry • Link to Legislative Train entry • Text adopted by EP
Revised Product Liability Directive	Internal Market	Close to adoption	• Link to Legislative Observatory entry • Link to Legislative Train entry • Text adopted by EP
Revision of the foreign direct investment (FDI) screening regulation	Economic, Monetary and Commercial Policy	Announced	• Link to Legislative Train entry
EU Space Law	Education, Research and Space Policy	Announced	• Link to Legislative Train entry
Information Security Regulation for EUIBAs	Cybersecurity of EUIBAs	Announced	• Link to Legislative Observatory entry

Table 44: Status Quo of Initiatives for Non-Legislative Acts of Cybersecurity Relevance as of June 17, 2024

Legal Basis	Delegated/Implementing Act	Status	Resources
DORA	Regulatory Technical Standards specifying the criteria for classification of ICT-related incidents	Awaiting publication	• Link to Register entry
	Regulatory Technical Standards specifying criteria regarding ICT risk management	Awaiting publication	• Link to Register entry
	Regulations specifying criteria (policy) for the critical ICT third-party service providers in the financial sector	Awaiting publication	• Link to Register entry
	Delegated regulation specifying fees for the critical ICT third-party service providers in the financial	Published, in force from June 19, 2024	• Commission Delegated

	sector	onwards	Regulation 2024/1505 • Link to Register entry
	Delegated regulation on further specifying the criticality criteria for critical ICT 3rd party service providers	Published, in force from June 19, 2024 onwards	• Commission Delegated Regulation 2024/1502 • Link to Register entry
	Implementing regulation laying down templates for a register of information of ICT contracts	Planned	• Link to Register entry
Regulation on the internal market for electricity	Network Code for cybersecurity aspects of cross-border electricity flows	Adopted, in force from June 13, 2024 onwards	• Commission Delegated Regulation 2024/1366
NIS 2 Directive	Rules specifying the obligations laid down in Articles 21(5) and 23(11) of the NIS 2 Directive	Planned	• Link to Register entry
Regulation 2019/2144	Protection of vehicles against cyberattacks	Planned	• Link to Register entry

Annex I: Where to Find Information on EU Cybersecurity Policy

Actor	Link & Description of Resource
EU Publications Office	eur-lex.europa.eu • Legal acts and policies in all official EU languages • Overview of amendments to a legal act and provision of consolidated versions of legal acts • Relevant document information such as dates of effect, dates of transposition, responsible bodies, legal bases, “all documents based on this document”, “all delegated/implementing acts based on this document” and “all documents mentioning this document” • Procedural information indicating the steps of procedure and the type of the competence conferred on the EU for the particular act • Information on national transposition measures • Document summaries, see also eur-lex.europa.eu/browse/summaries.html and eur-lex.europa.eu/summary/glossary.html for a glossary of summaries
European	oeil.secure.europarl.europa.eu

Parliament	• "European Parliament's database for monitoring the EU decision-making process," including, for instance, information on key events, involved Committees and the Committee responsible, (shadow) rapporteurs, relevant Council meetings, responsible Commission Directorate-Generals, a document gateway and for purposes of transparency, an overview of meetings with interest representatives published in line with the Rules of Procedure
	www.europarl.europa.eu/legislative-train • European Parliament "Legislative Train" permits "monitor[ing] the progress of legislative files during the current and past European Parliament term"
	www.europarl.europa.eu/thinktank • Briefings and other analyses of the European Parliamentary Research Service (EPRS)
Council	www.consilium.europa.eu/en/documents-publications/public-register • Public register of Council documents
	www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-cyber-issues • HWPCI-related documents such as meeting agendas and unclassified files
	consilium-europa.libguides.com/cybersecurity • "Cybersecurity Library Guide" providing an overview of books, articles, databases, websites, podcasts, videos and EU publications
	www.consilium.europa.eu/en/documents-publications/library/library-blog/think-tank-review • "Think Tank Review" providing "a monthly selection of EU-related papers published by think tanks across the world"
Commission	ec.europa.eu/transparency/documents-register • Register of Commission Documents, including "various types of Commission documents such as proposals, impact assessments, communications, delegated and implementing acts and other Commission decisions, agendas and minutes of meetings held by the College of Commissioners"
	webgate.ec.europa.eu/regdel • Register of delegated and implementing acts (for instance, any NIS 2-related delegated and implementing acts can be tracked here)
	digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies • European Commission website on "Cybersecurity Policies"
	digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group • Website of the NIS Cooperation Group containing, inter alia, agendas and outputs of the Group
EEAS	www.europa.eu/public-register • Public document register containing HR/VP and EEAS documents
ENISA	www.enisa.europa.eu/publications • Publications from the European Union Agency for Cybersecurity

	certification.enisa.europa.eu • ENISA website on EU Cybersecurity Certification
CERT-EU	cert.europa.eu/publications/threat-intelligence • Threat intelligence-related publications, such as monthly “Cyber Briefs” providing an overview of cybersecurity-related developments based on open-source information

Annex II: List of Definitions Used Within EU Cybersecurity Policies

Term	Definition	Source
assurance level	a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned	Art. 2, point (21) Regulation 2019/881
attribution	a practice of assigning a malicious cyber activity to a specific state or non-state actor	p. 18, 2023 Implementing Guidelines of EU Cyber Diplomacy Toolbox
communication and information system (CIS)	any system enabling the handling of information in electronic form, including all assets required for its operation, as well as infrastructure, organisation, personnel and information resources. This definition includes business applications, shared IT services, outsourced systems, and end-user devices	Art. 2, point (5) Commission Decision 2017/46
	any system enabling the handling of information in electronic form, including all assets required for its operation, as well as the infrastructure, organisation, personnel and information resources	Art. 1, point (3) Decision 2015/443
computer data	a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function	Art. 2, point (b) Directive 2013/40
connected product	an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user	Art. 2, point (5) Regulation 2023/2854
critical infrastructure	an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the	Art. 2, point (4) Directive 2022/2557

	provision of an essential service	
	an asset, network, system or part thereof which is essential for the maintenance of vital societal functions, the health, safety, security, economic or social well-being of people, and the disruption, breach or destruction of which would have a significant impact in a Member State or in the Union as a result of the failure to maintain those functions	Art. 2, point (4) Regulation 2021/ 1149
cyber attacks	actions [which] are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned", that either involve "access to information systems", "information system interference", "data interference", or "data interception"	Art. 1(3), Council Decision 2019/ 797 and Regulation 2019/ 796
cyber defence	one of the cybersecurity dimensions (mostly seen as the military dimension, but comprising both military and civilian approaches). It may also be considered as measures to defend critical systems and information in order to achieve cybersecurity. Cyber defence comprises all technical and non-technical measures to improve resilience of ICT-based systems (such as CIS, C2 and any weapon or sensor systems) supporting MS' defence and national security interests, and to prevent, detect, react to and recover from a Cyber Attack on these systems	p. 25, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations
cyber deterrence	cyber deterrence in the context of EU military CSDP is the ability to persuade continuously any cyber attacker that targeting EU CSDP military operations and missions in or through cyberspace will cost the attacker more than the gains expected. It encompasses all measures along the full spectrum of EU CSDP instruments	p. 25, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations
cyber resilience	the ability to continuously deliver the intended outcome despite adverse cyber events, in particular the capacity of an organization to face events (incident or attack), resist a failure or cyberattack and recover its previous condition after the incident	p. 26, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations
cyber threat	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	Basis: Art. 2, point (8) Regulation 2019/ 881
		Referenced by Art. 3, point (11) Regulation 2023/ 2841; Art. 3, point (12) Regulation 2022/ 2554; Art. 2, point (4) Regulation 2021/ 887; and Art. 6, point (10) Directive 2022/

		2555
cyber-attack	a malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset	Art. 3, point (14) Regulation 2022/2554
cyber-surveillance items	dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems	Art. 2, point (20), Regulation 2021/821
cybercrime	either crimes whose commission necessarily involves information and communications technology systems (ICT systems), either as tools for committing the crime or as the primary targets of the crime (cyber-dependent crimes), or traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other ICT systems (cyber-enabled crimes)	Art. 2, point (5) Regulation 2021/1149
cybersecurity	the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats	Basis: Art. 2, point (1) Regulation 2019/881
		Referenced by Art. 3, point (4) Regulation 2023/2841; Art. 2, point (1) Regulation 2021/887; and Art. 6, point (3) Directive 2022/2555
cybersecurity communities	collaborative civilian, law enforcement, diplomacy and defence groups representing both Member States and relevant EU institutions, bodies and agencies which exchange information in pursuit of shared goals, interests and missions in relation to cybersecurity	p. 7, Commission Recommendation 2021/1086
cybersecurity products, services and processes	commercial and non-commercial ICT products, services or processes with the specific purpose of protecting network and information systems or ensuring the confidentiality, integrity and accessibility of data that are processed or stored in network and information systems, as well as the cybersecurity of the users of such systems and other persons affected by cyber threats	Art. 2, point (3) Regulation 2021/887
cybersecurity risk	the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident	Basis: Art. 6, point (9) Directive 2022/2555
		Referenced by: Art. 3, point (14) Regulation 2023/2841

cyberspace	the virtual global and common domain within the information environment consisting of all interconnected and interdependent networks of global, organisational and national information infrastructure, based on the Internet and telecommunications networks, to be extended by other networks, computer systems and embedded processors, and containing also stand-alone systems and networks	p. 25, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations
cyberspace domain of operations	the global operational domain cutting through and being a substrate of all others, encompassing all cyberspace related information, information operations and strategic communications, and consisting of all interconnected information technology, communication networks, and included systems, which process, store or transmit information, separated or independent	p. 25, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations
cyberspace operations	operation aimed to retain freedom of manoeuvre in cyberspace / in the cyber domain to accomplish operational objectives, deny freedom of action to adversaries, and enable other operational activities	p. 25, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations
cyberspace situational awareness and situational understanding	the level of perception and understanding of all environmental elements and events, with respect to time or space and the projection of their status after some variable has changed, that allow making rational decisions and actions in cyberspace	p. 26, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations
data interception	intercepting, by technical means, non-public transmissions of digital data to, from or within an information system, including electromagnetic emissions from an information system carrying such digital data	Art. 2, point (d) Council Decision 2019/797 and Art. 1(7), point (d) Council Regulation 2019/796
data interference	deleting, damaging, deteriorating, altering or suppressing digital data on an information system, or rendering such data inaccessible; it also includes theft of data, funds, economic resources or intellectual property	Art. 2, point (c) Council Decision 2019/797 and Art. 1(7), point (c) Council Regulation 2019/796
digital operational resilience	the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions	Art. 3, point (1) Regulation 2022/2554
electronic communications	a transmission system, whether or not based on a permanent infrastructure or centralised	Art. 3, point (25) Regulation 2018/

network	administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed	1725 and Art. 2, point (1) Directive 2018/ 1972
electronic identification	the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person	Art. 3, point (1), Regulation 910/ 2014
electronic identification scheme	a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons	Art. 3, point (4), Regulation 910/ 2014
essential service	a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment	Art. 2, point (5) Directive 2022/ 2557
EU Cybersecurity Incident and Crisis Response Plan	a compilation of roles, modalities and procedures leading to the completion of the EU Cybersecurity Crisis Response Framework described in point (1) of the Commission Recommendation of 13 September 2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (‘Blueprint’)	p. 7, Commission Recommendation 2021/1086
EU Cybersecurity Rapid Reaction team	a team composed of recognised cybersecurity experts, drawn notably from the CSIRTs of the Member States, with support from ENISA, CERT-EU and Europol, which is ready to remotely assist participants impacted by large-scale incidents and crises	p. 7, Commission Recommendation 2021/1086
European cybersecurity certificate	a document issued by a relevant body, attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme	Art. 2, point (11) Regulation 2019/ 881
European cybersecurity certification scheme	a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes	Art. 2, point (9) Regulation 2019/ 881
ICT asset	a software or hardware asset in the network and information systems used by the financial entity	Art. 3, point (7) Regulation 2022/ 2554
ICT process	a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service	Basis: Art. 2, point (14) Regulation 2019/ 881

		Referenced by Art. 6, point (14) Directive 2022/2555
ICT product	an element or a group of elements of a network or information system	Basis: Art. 2, point (12) Regulation 2019/881
		Referenced by Art. 6, point (12) Directive 2022/2555
ICT risk	any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment	Art. 3, point (5) Regulation 2022/2554
ICT service	a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems	Basis: Art. 2, point (13) Regulation 2019/881
		Referenced by Art. 6, point (13) Directive 2022/2555
ICT services	digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services	Art. 3, point (21) Regulation 2022/2554
ICT third-party risk	an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements	Art. 3, point (18) Regulation 2022/2554
ICT-related incident	a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity	Art. 3, point (8) Regulation 2022/2554
incident	an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems	Basis: Art. 6, point (6) Directive 2022/2555
		Referenced by Art. 3, point (7) Regulation 2023/2841

	an event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service, including when it affects the national systems that safeguard the rule of law	Art. 2, point (3) Directive 2022/2557
	any event having an actual adverse effect on the security of network and information systems	Basis: Art. 4, point (7) Directive 2016/1148
		Referenced by Art. 2, point (6) Regulation 2019/881
incident handling	any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident	Basis: Art. 6, point (8) Directive 2022/2555
		Referenced by Art. 3, point (10), Regulation 2023/2841
	all procedures supporting the detection, analysis and containment of an incident and the response thereto	Basis: Art. 4, point (8) Directive 2016/1148
		Referenced by Art. 2, point (7) Regulation 2019/881
information asset	a collection of information, either tangible or intangible, that is worth protecting	Art. 3, point (6) Regulation 2022/2554
information assurance	also defined as protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats	p. 26, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations
information security policy	a set of information security objectives, which are or have to be established, implemented and checked. It comprises, but is not limited to, Decisions 2015/444 and 2015/443	Art. 2, point (10) Commission Decision 2017/46
information system interference	hindering or interrupting the functioning of an information system by inputting digital data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible	Art. 2, point (b) Council Decision 2019/797 and Art. 1(7), point (b) Council Regulation 2019/796
information system(s)	a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed,	Art. 2, point (a) Directive 2013/40

	retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance	
	a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes digital data, as well as digital data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance	Art. 2, point (a) Council Decision 2019/797 and Art. 1(7), point (a) Council Regulation 2019/796
integrated EU cybersecurity situation report	a report gathering input from participants in the Joint Cyber Unit, building on the EU Cybersecurity Technical Situation Report defined under Article 7(6) of Regulation (EU) 2019/881	p. 7, Commission Recommendation 2021/1086
IT security (or security of CIS)	the preservation of confidentiality, integrity and availability of CISs and the data sets that they process	Art. 2, point (13) Commission Decision 2017/46
IT security guidelines	consist of recommended but voluntary measures that help support IT security standards or serve as a reference when no applicable standard is in place	Art. 2, point (14) Commission Decision 2017/46
IT security incident	an event that could adversely affect the confidentiality, integrity or availability of a CIS	Art. 2, point (15) Commission Decision 2017/46
IT security measure	a technical or organisational measure aimed at mitigating IT security risks	Art. 2, point (16) Commission Decision 2017/46
IT security need	a precise and unambiguous definition of the levels of confidentiality, integrity and availability associated with a piece of information or an IT system with a view to determining the level of protection required	Art. 2, point (17) Commission Decision 2017/46
IT security objective	a statement of intent to counter specified threats and/or satisfy specified organisational security requirements or assumptions	Art. 2, point (18) Commission Decision 2017/46
IT security plan	the documentation of the IT security measures required to meet the IT security needs of a CIS	Art. 2, point (19) Commission Decision 2017/46
IT security policy	a set of IT security objectives, which are or have to be established, implemented and checked. It comprises this decision and its implementing rules	Art. 2, point (20) Commission Decision 2017/46
IT security requirement	a formalised IT security need through a predefined process	Art. 2, point (21) Commission Decision 2017/46
IT security risk	an effect that an IT security threat might induce on a CIS by exploiting a vulnerability. As such, an IT security risk is characterised by two factors: (1) uncertainty, i.e. the likelihood of an IT security threat to cause an unwanted event; and (2) impact, i.e. the consequences that such an unwanted event may have on a CIS	Art. 2, point (22) Commission Decision 2017/46
IT security threat	a factor that can potentially lead to an unwanted	Art. 2, point (25)

	event which may result in harm to a CIS. Such threats may be accidental or deliberate and are characterised by threatening elements, potential targets and attack methods	Commission Decision 2017/46
large-scale cybersecurity incident	an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States	Basis: Art. 6, point (7) Directive 2022/2555
		Referenced by Art. 3, point (9) Regulation 2023/2841
large-scale incident	an incident as defined under Article 4(7) of Directive (EU) 2016/1148 [= any event having an actual adverse effect on the security of network and information systems] with a significant impact in at least two Member States	p. 7, Commission Recommendation 2021/1086
legacy ICT system	an ICT system that has reached the end of its lifecycle (end-of-life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity	Art. 3, point (3) Regulation 2022/2554
major ICT-related incident	an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity	Art. 3, point (10) Regulation 2022/2554
major incident	an incident which causes a level of disruption that exceeds a Union entity's and CERT-EU's capacity to respond to it or which has a significant impact on at least two Union entities	Art. 3, point (8) Regulation 2023/2841
major operational or security payment-related incident	an operational or security payment-related incident that has a high adverse impact on the payment-related services provided	Art. 3, point (11) Regulation 2022/2554
major threat to security	a threat to security that can reasonably be expected to lead to loss of life, serious injury or harm, significant damage to property, compromise of highly sensitive information, disruption of IT systems or of essential operational capacities of the Commission	Art. 1, point (17) Decision 2015/443
managed security service provider	a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management	Art. 6, point (40) Directive 2022/2555
managed service provider	an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely	Art. 6, point (39) Directive 2022/2555
market	the activities carried out and measures taken by	Art. 3, point (23)

surveillance	market surveillance authorities to ensure that products comply with the requirements set out in this Regulation	Regulation 2023/988
national cybersecurity certification scheme	a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme	Art. 2, point (10) Regulation 2019/881
national cybersecurity strategy	a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State	Art. 6, point (4) Regulation 2022/2555
near miss	an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise	Basis: Art. 6, point (5) Directive 2022/2555 Referenced by Art. 3, point (6) Regulation 2023/2841
network and information system	(a) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance [1] While Regulations 2021/887 and 2019/881 refer to Art. 4, point (1) Directive 2016/1148 (NIS Directive) instead of Art. 6, point (1) Directive 2022/2555 (NIS 2 Directive) for the definition of 'network and information system', the actual definitions used in both Directives are similar in wordings.	Basis: Art. 6, point (1) Directive 2022/2555 Referenced by Art. 3, point (2) Regulation 2023/2841 and Art. 3, point (2) Regulation 2022/2554, as well as Art. 2, point (2) Regulation 2021/887 and Art. 2, point (2) Regulation 2019/881 [1]
operating system	a system software that controls the basic functions of the hardware or software and enables software applications to run on it	Art. 2, point (10) Regulation 2022/1925
operational or security payment-related incident	a single event or a series of linked events unplanned by the financial entities referred to in Article 2(1), points (a) to (d), whether ICT-related or not, that has an adverse impact on the availability, authenticity, integrity or confidentiality of payment-related data, or on the payment-related services provided by the financial entity	Art. 3, point (9) Regulation 2022/2554
personal data	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the	Art. 4, point (1) Regulation 2016/679

	physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	
processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction	Art. 4, point (2) Regulation 2016/679
product	any item, whether or not it is interconnected to other items, supplied or made available, whether for consideration or not, including in the context of providing a service, which is intended for consumers or is likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them	Art. 3, point (1) Regulation 2023/988
radio equipment	an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination	Art. 2(1), point (1) Directive 2014/53
resilience	a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident	Art. 2, point (2) Directive 2022/2557
	the ability to face economic, social and environmental shocks or persistent structural changes in a fair, sustainable and inclusive way	Art. 2, point (5) Regulation 2021/241
risk	the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident	Art. 6, point (9) Directive 2022/2555 and Art. 2, point (6) Directive 2022/2557
	the combination of the probability of an occurrence of a hazard causing harm and the degree of severity of that harm	Art. 3, point (4) Regulation 2023/988
	the combination of the probability of occurrence of harm and the severity of that harm	Art. 2, point (23) Regulation 2017/745
risk assessment	the overall process for determining the nature and extent of a risk by identifying and analysing potential relevant threats, vulnerabilities and hazards which could lead to an incident and by evaluating the potential loss or disruption of the provision of an essential service caused by that incident	Art. 2, point (7) Directive 2022/2557
safe product	any product which, under normal or reasonably foreseeable conditions of use, including the actual duration of use, does not present any risk or only	Art. 3, point (2) Regulation 2023/988

	the minimum risks compatible with the product's use, considered acceptable and consistent with a high level of protection of the health and safety of consumers	
security in the Commission	the security of persons, assets and information in the Commission, and in particular the physical integrity of persons and assets, the integrity, confidentiality and availability of information and communication and information systems, as well as the unobstructed functioning of Commission operations	Art. 1, point (12) Decision 2015/ 443
security incident	an event having an actual adverse effect on the security of electronic communications networks or services	Art. 2, point (42) Directive 2018/ 1972
security of network and information systems	the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems	Basis: Art. 6, point (2) Directive 2022/ 2555 Referenced by Art. 3, point (3) Regulation 2023/ 2841 and Art. 3, point (4) Regulation 2022/ 2554
security of networks and services	the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services	Art. 2, point (21) Directive 2018/ 1972
serious risk	a risk which, based on a risk assessment and taking into account the normal and foreseeable use of the product, is considered to require rapid intervention by the market surveillance authorities, including cases where the effects of the risk are not immediate	Art. 3, point (5) Regulation 2023/ 988
significance of a disruption	In order to determine the significance of a disruption, the following parameters shall, in particular, be taken into account: (a) the number and proportion of users affected by the disruption; (b) the duration of the disruption; (c) the geographical area affected by the disruption, taking into account whether the area is geographically isolated.	Art. 15(1), Directive 2022/ 2557
significance of the impact of a security incident	in order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account: (a) the number of users affected by the security incident; (b) the duration of the security incident; (c) the geographical spread of the area affected by	Art. 40(2), Directive 2018/ 1972

	the security incident; (d) the extent to which the functioning of the network or service is affected; (e) the extent of impact on economic and societal activities.	
significant cyber threat	a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage	Basis: Art. 6, point (11) Directive 2022/2555 Referenced by Art. 3, point (12) Regulation 2023/2841
	a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident	Art. 3, point (13) Regulation 2022/2554
	financial entities shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.	Art. 18(2), Regulation 2022/2554
significant effect of a cyber attack	The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include any of the following: (a) the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety; (b) the number of natural or legal persons, entities or bodies affected; (c) the number of Member States concerned; (d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property; (e) the economic benefit gained by the perpetrator, for himself or for others; (f) the amount or nature of data stolen or the scale of data breaches; or (g) the nature of commercially sensitive data accessed.	Art. 3, Decision 2019/797 and Art. 2, Regulation 2019/796
significant disruptive effect	When determining the significance of a disruptive effect [...], Member States shall take into account the following criteria: (a) the number of users relying on the essential service provided by the entity concerned; (b) the extent to which other sectors and subsectors as set out in the Annex depend on the essential service in question; (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population; (d) the entity's market share in the market for the essential service or essential services concerned; (e) the geographic area that could be affected by an incident, including any cross-border impact, taking	Art. 7(1), Directive 2022/2557

	into account the vulnerability associated with the degree of isolation of certain types of geographic areas, such as insular regions, remote regions or mountainous areas; (f) the importance of the entity in maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of that essential service.	
significant incident	an incident shall be considered to be significant if: (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.	Art. 23(3), Directive 2022/2555
	an incident shall be considered to be significant if: (a) it has caused or is capable of causing severe operational disruption to the functioning of, or financial loss to, the Union entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.	Art. 21(1), Regulation 2023/2841
software application	any digital product or service that runs on an operating system	Art. 2, point (15) Regulation 2022/1925
threat intelligence	information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making and to enable relevant and sufficient understanding in order to mitigate the impact of an ICT-related incident or of a cyber threat, including the technical details of a cyber-attack, those responsible for the attack and their modus operandi and motivations	Art. 3, point (15) Regulation 2022/2554
threat-led penetration testing (TLPT)	a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems	Art. 3, point (17) Regulation 2022/2554
vulnerability	a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat	Basis: Art. 6, point (15) Directive 2022/2555
		Referenced by Art. 3, point (13) Regulation 2023/2841
	a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited	Art. 3, point (16) Regulation 2022/2554

Annex III: List of Abbreviations Used in Compendium

Abbreviation	Full Name
ACER	European Union Agency for the Cooperation of Energy Regulators
AFSJ	Area of freedom, security and justice
APT	Advanced Persistent Threat
BEREC	Body of European Regulators for Electronic Communications
CARD	Coordinated Annual Review on Defence
CBMs	Confidence-building measures
CCB	Cyber capacity-building
CD	Cyber Defence
CDOP	Cyber Defence Operational Picture
CDP	Capability Development Plan
CDPF	Cyber Defence Policy Framework
CER Directive	Critical Entities Resilience Directive
CERG	Critical Entities Resilience Group
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CFSP	Common Foreign and Security Policy
CIDCC	Cyber and Information Domain Coordination Centre
CIISI-EU	Cyber Information and Intelligence Sharing Initiative
CIS	Communication and Information Systems
COREPER	Committee of the Permanent Representatives of the Governments of the Member States to the European Union
COSI	Standing Committee on Operational Cooperation on Internal Security
CRA	Cyber Resilience Act
CRF	Cyber Ranges Federations
CRRT	Cyber Rapid Response Teams and Mutual Assistance in Cyber Security
CSDP	Common Security and Defence Policy
CSIRTs	Computer Security Incident Response Teams

CSIRTs Network	Computer Security Incident Response Teams Network
CTI	Cyber Threat Intelligence
CTIRISP	Cyber Threats and Incident Response Information Sharing Platform
CVD	Coordinated Vulnerability Disclosure
CyCLOs	Cyber Crises Liaison Organisations
DG	Directorate-General
DG COMP	Directorate-General for Competition
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DG DEFIS	Directorate-General for Defence Industry and Space
DG DIGIT	Directorate-General for Digital Services
DG ECFIN	Directorate-General for Economic and Financial Affairs
DG ENER	Directorate-General for Energy
DG FISMA	Directorate-General for Financial Stability, Financial Services and Capital Markets Union
DG GROW	Directorate General for Internal Market, Industry, Entrepreneurship and SMEs
DG HOME	Directorate-General for Migration and Home Affairs
DG HR	Directorate-General for Human Resources and Security
DG INTPA	Directorate-General for International Partnerships
DG JRC	Joint Research Centre
DG JUST	Directorate-General for Justice and Consumers
DG MOVE	Directorate-General for Mobility and Transport
DG RTD	Directorate-General for Research and Innovation
DG SANTE	Directorate-General for Health and Food Safety
DG TRADE	Directorate-General for Trade
DNS	Domain Name System
DORA	Digital Operational Resilience Act
e-CODEX	e-Justice Communication via Online Data Exchange
EASA	European Union Aviation Safety Agency
EBA	European Banking Authority
EC	European Commission
EC3	European Cybercrime Centre
ECB	European Central Bank

ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ECCSA	European Centre for Cybersecurity in Aviation
ECOFIN	Economic and Financial Affairs Council
ECRB	Euro Cyber Resilience Board for pan-European Financial Infrastructures
ECSF	European Cyber Skills Competence Framework
EDA	European Defence Agency
EDF	European Defence Fund
EDPS	European Data Protection Supervisor
EDTIB	European Defence Technological and Industrial Base
EEAS	European External Action Service
EGNOS	European Geostationary Navigation Overlay Service
eIDAS Regulation	Regulation on electronic identification and trust services
EIOPA	European Insurance and Occupational Pensions Authority
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENISA	European Union Agency for Cybersecurity
ENISA AG	ENISA Advisory Group
ENTSO-E	European Network of Transmission System Operators for Electricity
ENTSOG	European Network of Transmission System Operators for Gas
EP	European Parliament
EPF	European Peace Facility
ESAs	European Supervisory Authorities
ESDC	European Security and Defence College
ESMA	European Securities and Markets Authority
ESRB	European Systemic Risk Board
ETIAS	European Travel Information and Authorisation System
ETSI	European Telecommunications Standards Institute
EU	European Union
EU CAIH	EU Cyber Academia and Innovation Hub
EU DSO Entity	European Distribution System Operators Entity
EU INTCEN	European Union Intelligence and Situation Centre
EU SOCTA	European Union Serious and Organised Crime Threat Assessment

EU Space ISAC	EU Space Information Sharing and Analysis Centre
EU-CyCLONe	European Cyber Crises 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
EUAN	EU Agencies Network
EUCDCC	EU Cyber Defence Coordination Centre
EUCI	EU classified information
EUCTF	European Union Cybercrime Task Force
EUIBAs	EU Institutions, Bodies, and Agencies
EUMC	EU Military Committee
EUMS	European Union Military Staff
EUMS INT	European Union Military Staff Intelligence Directorate
EUPM Moldova	European Union Partnership Mission Moldova
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EuroQCI	European Quantum Communication Infrastructure
EUSPA	European Union Agency for the Space Programme
FAC	Foreign Affairs Council
FDI	Foreign direct investments
FMN	Federated Mission Networking
GDPR	General Data Protection Regulation
GNSS	Global navigation satellite system
GOVSATCOM	European Union Governmental Satellite Communications
GSC	General Secretariat of the Council
HR/VP	High Representative of the Union for Foreign Affairs and Security Policy / Vice President of the Commission
HWPCI	Horizontal Working Party on Cyber Issues
IAEA	International Atomic Energy Agency
ICT	Information and communication technologies
ICTAC	ICT Advisory Committee of the EU Agencies
IEP	Internet Exchange Point
IICB	Interinstitutional Cybersecurity Board
IOCTA	Internet Online Crime Threat Assessment

IoT	Internet of Things
IPCR	Integrated Political Crisis Response
ISAA	Integrated Situational Awareness and Analysis
ISF	Internal Security Fund
ISMS	Information security management systems
ISSB	Information Security Steering Board
IT	Information technology
ITRE	Committee on Industry, Research and Energy
J-CAT	Joint Cybercrime Action Taskforce
JC	ESA Joint Committee
JCU	Joint Cyber Unit
JHA	Justice and Home Affairs Council
JITs	Joint Investigation Teams
JON	Joint Oversight Network
LEAs	Law enforcement agencies
LIBE	Committee on Civil Liberties, Justice and Home Affairs
LISO	Local Informatics Security Officer
MiCA	Markets in Crypto-Assets Regulation
MICNET	Military Computer Emergency Response Team Operational Network
MilCERT	Military Computer Emergency Response Team
MLA	Mutual Legal Assistance
MSP	Managed service provider
NCC	National Coordination Centre
NEC	National EMPACT coordinator
NIS	Directive concerning measures for a high common level of security of network and information systems across the Union (2016)
NIS 2	Directive on measures for a high common level of cybersecurity across the Union (2022)
NoCA	Network of Cybersecurity Analysts
PEGA	Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware
PESCO	Permanent Structured Cooperation
PoA	Programme of Action
PSC	Political and Security Committee

QCI	Quantum communication infrastructure
R&D	Research and development
RED	Radio Equipment Directive
RRF	Recovery and Resilience Facility
RTS	Regulatory technical standards
SCCG	Stakeholder Cybersecurity Certification Group
SIAC	Single Intelligence Analysis Capacity
SIENA	Secure Information Exchange Network Application
SMEs	Small and medium-sized enterprises
SOCs	Security Operation Centres
SOP	Standard Operating Procedures
SPOC	Single Point of Contact
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TIBER-EU	European framework for Threat Intelligence-based Ethical Red Teaming
TLPT	Threat-led penetration testing

Acknowledgements

The author would like to thank Jasen Ho for research support, particularly on EU legal acts and policies in the areas of energy, transport, health, education and research policy, as well as Sven Herpig and Luisa Seeling for their support with this publication.

Concept and Supervision Infographics, Backend Curation: Alina Siebert
Backend Curation Support: Martha Rahel Reinicke
Design Infographics: Jan Klöthe

Author

Christina Rupp
Senior Policy Researcher Cybersecurity and Resilience
crupp@interface-eu.org
+49308145037880

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
Ebertstraße 2
D-10117 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com