ACER
European Union Agency for the Cooperation of Energy Regulators

Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

22 July 2021

European Union Agency for the Cooperation of Energy Regulators
Trg Republike 3
1000 Ljubljana, Slovenia

This Document contains the Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows, which the European Union Agency for the Cooperation of Energy Regulators (ACER) has prepared pursuant to Article 59.2(e) of Regulation (EU) 2019/943 and based on the request from the European Commission.

EU reference documents

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

- Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1485

- COMMISSION RECOMMENDATION (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0553

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), available at the following link: https://eur-lex.europa.eu/eli/reg/2019/881/oj

- Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2019%3A158%3ATOC&uri=uriserv%3AOJ.L_.2019.158.01.0001.01.ENG

- Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity, available at the following link: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0943

- Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944

- Smart Grids Task Force - Expert Group 2 – Cybersecurity - Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management, available at the following link: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

- Commission Implementing Decision (EU) 2020/1479 of 14 October 2020 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, available at the following link: https://eur-lex.europa.eu/eli/dec_impl/2020/1479/oj

- Summary of the responses to the targeted stakeholder consultation to set up the priority list, published by the European Commission – DG Energy on July 2020, available at: https://ec.europa.eu/energy/sites/ener/files/summary_for_publication_ares.pdf

- Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2020:18:FIN

- Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020) 823 final): https://op.europa.eu/en/publication-detail/-/publication/561f90d7-8af2-11eb-b85c-01aa75ed71a1/language-en/format-PDF/source-197887699

- Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (COM(2020) 829 final), available at the following link: https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-829-F1-EN-MAIN-PART-1.PDF

- European Commission: Invitation to draft framework guideline on sector-specific rules for cybersecurity aspect of cross-border electricity flows, Reference ARES(2021)653629, 27/01/2021, https://www.acer.europa.eu/Media/News/Documents/2021.01.22%20MK%20585504%20letter%20to%20ACER_cybersecurity_final_22.1.2021%20amended.docx.pdf

Table of Contents

1 General Provisions

1.1 Scope

This Framework Guideline aims at setting out clear and objective principles for the development of a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, pursuant to Article 59, paragraph 2(e) of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (henceforth referred to as the "Electricity Market Regulation").[1] The Electricity Market Regulation provides for the establishment of a network code on sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management (henceforth referred to as the "network code").

In accordance with Article 59(4) of the Electricity Market Regulation, on 28 January 2021 the European Commission invited ACER to draft a Framework Guideline for a network code on cybersecurity, taking into account some high-level objectives [2] and the extensive preparatory work completed so far (e.g. the recommendations of the Smart Grid Task Force Expert Group 2 report[3] and the recommendations of the European Network of Transmission System Operators for Electricity (ENTSO-E) and Distribution System Operator (DSO) associations included in the final report[4]).

This Framework Guideline was subject to public consultation for two months; during this period, ENTSO-E and EU DSO entity were consulted in an open and transparent manner. As a result of the submissions received, several changes were made to improve the draft Framework Guideline.

This Framework Guideline is submitted to the European Commission in accordance with Article 59(6) of the Electricity Market Regulation.

After its submission by ACER to the European Commission, the Framework Guideline will serve as the basis for the development of a proposal for the network code by a specific drafting committee for the cooperation of ENTSO-E and EU DSO entity. The proposal for a network code shall be submitted to ACER within a reasonable period, not exceeding 12 months of the receipt of the Commission's request. ACER shall revise the proposed network code to ensure its compliance with this Framework Guideline and its contribution to market integration, non-discrimination, effective competition, and the efficient functioning of the market. ACER shall submit the revised network code to the Commission within six months of receipt of the proposal, in accordance with Article 59(11) of the Electricity Market Regulation.

1.2 Definitions and acronyms

The following definitions shall apply to this Framework Guideline:

[1] OJ L 158, 14.6.2019, p. 54–124
[2] Objectives for the network code was communicated in the invitation letter from EC to ACER to draft a framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows.
[2] OJ L 158, 14.6.2019, p. 125–199
[3] Smart Grid Task Force Expert Group 2 - Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. Final Report June 2019; at https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf
[4] Final Report 19 February 2021, Recommendations for the European Commission on a Network Code on Cybersecurity - https://ec.europa.eu/energy/sites/default/files/nccs_report_network_code_on_cybersecurity.pdf.

- Definitions in Article 2 of the Electricity Market Regulation.
- Definitions in Article 2 of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (henceforth referred to as the "Electricity Market Directive").[5]

The following definitions are intended to further clarify the provisions of this Framework Guideline and are without prejudice to the definitions to be included in the network code:

- **'Computer Security Incident Response Team (CSIRT)'** refers to a team of IT experts who handle security related incidents. The term CSIRT is normally equivalent to and interchangeable with CERT (Computer Emergency Response Team).

- **'Critical assets'** means the minimum set of assets, including infrastructure, without which cross-border electricity flows cannot be ensured. Asset types include people, products, information and processes which are assessed as essential by an entity.

- **'Critical Business Process'** means a business process which is essential for the supply of electricity from generator to the consumer, one which is operationally so important that it cannot be allowed to be interrupted or fail.

- **'Critical-risk entity'** means an entity which is considered to present a critical risk to suffer and cause a relevant impact to cross-border electricity flows in the event of a cyber-attack impacting its operations.

- **'Critical perimeter'** means the electricity cybersecurity perimeter that includes all critical assets (or those assets owned or operated by critical-risk entities).

- **'Critical service provider'** means a natural or legal person who operates or provides directly or on behalf of an operator any IT and/or OT system, sub-system, service or product, or any of their combinations, that is indispensable to allow efficient cross-border electricity flows with the purpose to store, deliver, produce, aggregate or commercialise electricity to final customers.

- **'Cross-border electricity flow'** means a physical flow of electricity on a transmission network of a Member State that results from the impact of the activity of producers, customers or both, outside that Member State on its transmission network, as defined in point (3) of Article 2 of Regulation 2019/943.

- **'Cyber-attack'** means any attempt with malicious intent to gain access to an information technology environment.[6] A cyber-attack may cause a cyber-incident where damages, disruptions or dysfunctionalities are caused.

- **'Cybersecurity posture'** refers to an organisation's overall cybersecurity status (including procedures, processes, skills, tools and resources) to defend proactively and reactively against cyber-attacks.

[5] OJ L 158, 14.6.2019, p. 125–199
[6] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology - Page 7

- **'Early warning'** means a provision of concrete, valid, reliable information indicating that a cyber-attack may occur which is likely to result in a significant deterioration of the electricity supply situation and at great extent is likely to lead to electricity crisis.[7]

- **'ECRI Caps (ECRICs)'** means the value of the index above/below which an entity, or a group of entities, is considered to be a "high-risk entity"/ "critical-risk entity".

- **'Electricity cybersecurity perimeter'** refers to the cyber systems (hardware or software) that include all assets that belong to the entities concerned by the obligations of the network code, which are designed to either keep intruders out or to keep captives contained within the surrounding boundary. The electricity cybersecurity perimeter may include third parties' dependencies as well as the general regulatory and legal context.

- **'Electricity Cybersecurity Risk-Index(es) (ECRIs)'** means the indexes that synthesise the risk level of an entity or of a group of entities given an impact on cross-border electricity flows in a single or in a set of risk of index(es).

- **'Electricity digital market platform'** means a digital platform for electricity data management and electricity trading.

- **'Information Technology (IT)'** involves information being processed digitally in information technology systems and transferred across communications networks.

- **'High-risk entity'** means an entity which is considered to present a high risk to suffer and cause a relevant impact to cross-border electricity flows in the event of a cyber-attack impacting its operations.

- **'High-risk perimeter'** means the electricity cybersecurity perimeter that includes all critical assets that are owned by a high-risk entity.

- **'Legacy systems'** means obsolete hardware and/or software systems that need to be interconnected and that are used in the context of electricity cross-border flows and cannot be modified or updated to meet minimum cybersecurity requirements. Legacy systems also include hardware and/or software systems that cannot be protected by other means without causing damages, disruptions or dysfunctionalities to electricity cross-border flows operations.

- **'Managed Security Service Provider (MSSP)'** means a provider of SOC services for entities who lack such capabilities themselves and/or prefer to outsource such services.

- **'National Competent Authorities for cybersecurity in Energy (CS-NCAs)'**, in accordance with Article 8 of the NIS Directive, means all national competent authorities with specific competence for the energy sector and responsible for the implementation, monitoring and supervision of cybersecurity in the energy sector at Member State level.

- **'National Competent Authorities for Risk Preparedness (RP-NCAs)'** means all authorities established under Article 3 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (henceforth referred to as the "Risk Preparedness Regulation"[8]).

[7] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC.
[8] OJ L 158, 14.6.2019, p. 1–21

- **'National Regulatory Authorities responsible for the electricity sector (NRAs)'** means all regulatory authorities, in accordance with Article 57(1) of the Electricity Market Directive.

- **'NIS Cooperation Group (NISCG)'**: its mission is to achieve a high common level of security for network and information systems (NIS) in the European Union as described in Article 11 of the NIS Directive[9]. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States. The NIS Cooperation Group is composed of representatives of the EU Member States, the European Commission and the EU Agency for cybersecurity (ENISA).[10]

- **'Operational technology (OT)'** involves the use of computers and data networks to operate physical systems, e.g., electric grid operation.

- **'Originator'** means an entity that initiates an information exchange, sharing or storage event.

- **'Processor'** means an entity that legitimately processes information, independently from its ownership.

- **'Representative'** means any natural or legal person established in the Union explicitly designated to act on behalf of a critical service provider.

- **'Real-time systems'**, in accordance with the IEEE[11] definition, are systems in which its temporal properties are essential for reliability and correctness; the example applications include embedded systems, control systems and monitoring systems. More explanation on real-time requirements in electricity can be found in the Commission Staff Working Document SWD(2019)1240 final accompanying the document Commission Recommendation on cybersecurity in the energy sector.

- **'Risk Impact Matrix (RIM)'** means a matrix used during risk assessment to describe the resulting risk impact level for each risk assessed. By considering one or more *business impact categories* (e.g., Operational, Financial, Legal & Regulatory Compliance, etc.) against the corresponding *potential risk impact rating* (impact level classification) described in the risk impact matrix, the resulting potential risk impact level is determined. The risk matrix is used to increase visibility of potential business risk impacts and assist management decision making related to risk management.

- **'Security Operation Centre (SOC)'** refers to an entity staffed with one or more IT and/or OT experts who perform security related tasks such as log analysis, incident detection, incident handling and security configuration.

- **'System operation regions'** refers to the system operation regions defined in accordance with Article 36 of the Electricity Market Regulation on the geographical scope of regional coordination centres[12].

[9] https://digital-strategy.ec.europa.eu/en/policies/nis-directive
[10] http://www.enisa.europa.eu/
[11] The Institute of Electrical and Electronics Engineers (IEEE) is a professional association for electronic engineering and electrical engineering
[12] Decision No 8/2021 of the European Union Agency for the Cooperation of Energy Regulators of 29 June 2021 on the definition of system operation regions, available at: https://extranet.acer.europa.eu/Official_documents/Acts_of_the_Agency/Individual%20decisions%20Annexes/ACER%20Decision%20No%2008-2021_Annexes/ACER%20Decision%2008-2021%20on%20SOR%20-%20Annex%20I.pdf

1.3 Applicability of the network code

The network code shall apply to the public and private entities listed in Table 1 (henceforth referred to as 'entities') which may affect cross-border electricity flows directly or indirectly. The network code shall set up a clear methodology which allows the CS-NCAs and the NRAs to classify entities on their territory as "critical-risk" or "high-risk" entities (see section 1.5 below). As a general principle, the network code shall not apply to small[13] and micro[14] enterprises, unless explicitly stated otherwise.

Table 1: *Entities to whom the network code for sectoral regulations on cybersecurity aspects of cross-border electricity flows shall apply.*

#	**Entity definition**
1	Electricity undertakings as defined in Article 2(57) of the Electricity Market Directive
2	NEMOs as defined in Article 2(7) and (8) of Electricity Market Regulation
3	Electricity digital market platforms as defined in this Framework Guideline
4	Critical service providers as defined in this Framework Guideline
5	Regional Coordination Centres (RCCs) established pursuant to Article 35 of the Electricity Market Regulation
6	ENTSO-E, the EU DSO entity, ACER and NRAs
7	RP-NCAs, SOCs, CS-NCAs and CSIRTs and ENISA

The proposal for a NIS 2 Directive foresees[15] the possibility for small and micro enterprises to be included in the list of essential/important services when they have a relevance on cybersecurity matters. On this basis, the network code could also apply to those small and micro enterprises that cover specific high-risk or critical roles in the cybersecurity value chain of cross-border electricity flows. Likewise, the network code could also apply to any other additional stakeholder not listed in Table 1, but with relevant cybersecurity impact on the cross-border electricity flow.[16]

Therefore, the network code must provide for the possibility of applying it to small and micro enterprises as well as any additional stakeholders at the initiative of:

i) any entity listed in Table 1, after consulting and having obtained an opinion from the competent NRA(s) and the CS-NCAs;
ii) the CS-NCA jointly with the respective NRA of the concerned Member State; or
iii) the European Commission, following an ACER opinion, after consulting and having obtained an opinion from the competent NRA(s) and the CS-NCAs.

The network code shall define an index to determine objectively if the concerned small or micro enterprise or any additional stakeholder shall be classified either as critical-risk or high-risk entities; the index may take into consideration parameters such as financial turn over, company size in terms of average number of employed staff, impact on cross border electricity flow, etc. The network code shall clearly indicate the conditions to be fulfilled, the method to calculate such index and the thresholds applicable, referred as "size cap".

[13] In the Electricity Market Directive, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.
[14] In the Electricity Market Directive, a micro enterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.
[15] Article 2(2) in COM(2020) 823 final
[16] Such stakeholders may e.g., be large industrial electricity consumers or providers of energy management systems or smart appliances for consumers.

The network code shall establish for all small and micro enterprises below the size cap and not classified as critical-risk entities or as high-risk entities the implementation of basic cyber hygiene requirements in line with the "Review of Cyber Hygiene practices"[17] from the European Union Cybersecurity Agency (ENISA), or with any specific guidance document for energy small and micro enterprises in the energy or electricity sector which ENISA may release in the future.

1.4 Territorial scope and representatives of critical service providers not established in the Union

The network code shall apply to the public and private entities listed in Table 1. The network code shall also apply to critical service providers (Table 1 at point 4) not established in the Union when delivering services to entities in the Union which may affect cross-border electricity flows directly or indirectly.

Where a critical service provider not established in the Union is delivering services to an entity who is in the Union and may affect cross-border electricity flows directly or indirectly, that critical service provider should designate a representative unless the processing is occasional, does not include data processing, is not on a large scale, or is unlikely to result in a risk to entities in the EU. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. The representative should act on behalf of the critical service provider and it should be possible for competent authorities or the CSIRTs to contact the representative. The designation of a representative by the critical service provider shall be without prejudice to legal actions which could be initiated against the critical service provider itself.

1.5 Classification of entities subject to the network code by Electricity Cybersecurity Risk Index

The network code shall allow ENTSO-E and the EU DSO entity, advised by ENISA and ACER and with the assistance of the NRAs and the CS-NCAs, to determine the specific cybersecurity risks exposures of different entities to cross-border electricity flows. This determination shall allow to prioritise the interventions and shall facilitate to the CS-NCA in cooperation with the NRAs the harmonised categorisation of the entities on objective grounds with the purpose to apply proportionate cybersecurity measures. To do so, the network code shall set up a clear methodology which allows the CS-NCAs and the NRAs to classify entities on their territory as "critical-risk" or "high-risk" entities. In particular, this methodology shall:

i) classify objectively the risk level(s) to which each entity is exposed, both in isolation and in correlation with any other entity or group of them to which the entity is connected for the purpose of information and cross-border electricity flow operations, through one or more risk index(es), named Electricity Cybersecurity Risk-Index(es) (ECRIs); and
ii) define one or more ECRI Caps (ECRICs), above/below which an entity or group of them shall be classified as "critical-risk" entity/"high-risk" entity.

The network code shall foresee the regular revision of the list of "critical-risk"/"high-risk" entities. The lists will be treated as sensitive information and managed jointly and securely by the CS-NCA and the NRA with national security clearances at the Member State level, and ACER and ENISA at the European level. In the event that an NRA has no security clearances at the Member State level, the CS-NCA will grant the NRA relevant access to information on a "need to know" basis. These potential situations shall be described in the Risk Assessment Report.

[17] https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport

For newly established entities or for existing entities providing new services under the classification shown in Table 1, the network code shall establish that their start-up and operations after the first year shall be subject to the execution of an information asset inventory and a risk assessment, as well as their final classification in one of the two categories (high-risk/critical-risk) by the CS-NCA and the NRA within the first initial year. This period may be shortened if deemed appropriate by the CS-NCA and NRA based on the risk assessment.

1.6 Transitional measures for the classification of entities

Within the first six months after the entry into force of the network code, ENTSO-E and the EU DSO entity, advised by ENISA and ACER and with the assistance of the NRAs and the CS-NCAs, shall determine the specific cybersecurity risks exposures of the different entities to cross-border electricity flows, which allows the CS-NCAs and the NRAs to classify all these entities in their territory into a transitional list of “critical-risk”/“high-risk” entities.

The transitional list shall be treated as sensitive information and managed jointly and securely by the CS-NCA and the NRA with national security clearances at the Member State level, and ACER and ENISA at the European level. In the event that an NRA has no security clearances at the Member State level, the CS-NCA will grant the NRA relevant access to information on a “need to know” basis. These potential situations shall be described in the Risk Assessment Report.

The transitional list shall be based on a precautionary principle, so that entities may only gain more responsibilities in the revised list after the end of the transition period, compared to where they stand in the transition list (e.g., no demotion from “critical-risk” to “high-risk” in the revised list).

The transition period shall conclude no later than two years after the entry into force of the network code. Within this two-year period and, based on the integrated top-down and bottom-up cybersecurity risk assessment methodology described in Chapter 3, the CS-NCAs in cooperation with the NRAs, and advised by ENISA and ACER and with the assistance of ENTSO-E and the EU DSO entity, shall revise and update the list of the “critical-risk”/”high-risk” entities. The lists shall be revised at least every two years. The lists shall be treated as sensitive information and managed jointly and securely by the CS-NCA and the NRA with national security clearances at the Member State level and ACER and ENISA at the European level. In the event that an NRA has no security clearances at the Member State level, the CS-NCA will grant the NRA relevant access to information on a “need to know” basis. These potential situations shall be described in the Risk Assessment Report. The transitional list will remain valid until a revised list has been established.

Box 1: List of deliverables chapter 1	
Deliverable	Responsibility
1. Electricity Cybersecurity Risk Index (ECRI), including: - ECRI Caps for defining critical-risk and high-risk entities - An index to determine whether small and micro enterprises shall be defined as high-risk or critical-risk entities	Jointly established by ENTSO-E and the EU DSO entity, and advised by ENISA and ACER and with the assistance of the NRAs and the CS-NCAs
2. Basic cyber hygiene requirements to be implemented by small and micro enterprises listed in Table 1, who are not critical-risk or high-risk entities	Jointly established by ENTSO-E and the EU DSO entity, and advised by ENISA and ACER and with the assistance of the NRAs and the CS-NCAs

3. List of high- and critical-risk entities, including a transitional version of this list	CS-NCAs in cooperation with the NRAs, and advised by ENISA and ACER and with the assistance of ENTSO-E and the EU DSO entity

2 Cybersecurity Electricity Governance

2.1 General principles

The implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (henceforth referred to as the "NIS Directive")[18] has shown the importance, especially in cybersecurity, to establish a solid governance that distinguishes between the strategic and decisional role and the operational roles. In addition, the EU Cybersecurity Act[19] has also stressed the importance of a central support and advisory role for ENISA. In parallel, the proposal for a directive on the resilience of critical entities aims to enhance the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities by increasing the resilience of critical entities providing such services.

As general principles, the network code should complement and be consistent with the two proposed Directives on measures for a high common level of cybersecurity across the Union ("NIS 2 Directive") and the resilience of critical entities. These two main principles shall be reflected in the governance of the cybersecurity for the electricity sector in the network code, providing a role, where possible, to the same actors that have already demonstrated the ability to lead such efforts.

At the same time, the network code shall consider that, to carry out cross-border operations of the electricity system efficiently, there is already a governance that shall be maintained to ensure the reliability of the energy system and should not interfere or jeopardise the objectives already reached through other network codes.

The network code shall limit the creation of its governance to the essential bodies that shall be able to participate in the decisions and operations described in the following chapters, without invalidating the role of EU entities with existing competences in cybersecurity and operation of the electricity system.

To enact this, the network code will need to consider the following:

Article 8 of the NIS Directive established the **"National Competent Authorities for Cybersecurity in Energy (CS-NCAs)"**: the authorities work as a single point of contact, serving the purpose to have an overview also on sectors which the electricity sector is highly dependent on and perform a liaison function to ensure cross-border cooperation of Member State authorities. Therefore, the network code shall not aim to create new national authorities but facilitate the close cooperation between the CS-NCAs and NRAs when there is any need to coordinate, institutionalise and supervise operators involved in the implementation and execution of the network code. Therefore, coordination of all competent authorities within each Member State shall be handled at Member State level, and not raised at EU level when it concerns the first cycle of

[18] OJ L 194, 19.7.2016, p. 1–30
[19] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) - https://eur-lex.europa.eu/eli/reg/2019/881/oj

risk assessment and risk management, as well as when it concerns the monitoring of the implementation of minimum and advanced cybersecurity standards, the monitoring of the security requirements and the close control of the supply chain for the electricity sector involved in cross-border electricity flows;

Article 9 of the NIS Directive established the **"Computer Security Incident Response Teams (CSIRTs)"**. The CSIRTs monitor incidents at Member State level. They can provide early warnings, alerts, announcements and dissemination of information to the relevant stakeholders about risks and incidents, and they can respond to incidents. Nevertheless, they may not possess the knowledge and skills necessary to process information in the context of cross-border electricity flows. Therefore, the CSIRTs shall be supported in their work by a team of specialists in cross-border electricity flows when the cybersecurity issue affects the entities in Table 1.

The network code shall recognise the need for a close collaboration among the CSIRTs network, the National CSIRTs and ENTSO-E, which should in turn cooperate with the EU DSO entity and the RCCs. This cooperation should be clearly defined. The rules for cooperation shall apply to the handling of cross-border electricity incidents with the potential of a cascading effect across the system operation regions. In this case, the network code shall provide clear rules for an escalation and a clear leadership role on decisions regarding the handling of an incident that may need the involvement of all those entities.

The Risk Preparedness Regulation established **National Competent Authorities for Risk Preparedness (RP-NCA)** to carry out risk assessments, prepare risk preparedness plans at the Member State level and participate in the preparation of regional plans that include scenarios related to cybersecurity risks. Therefore, to establish consistency between specific new cybersecurity risks and the cybersecurity scenarios, the network code shall foresee active participation of such entities in cross-border risk assessment and make sure that the methodologies do not overlap.

National Regulatory Authorities in charge of the electricity sector (NRAs) took part to the elaboration of this Framework Guideline and possess specific knowledge of the electricity sector and relevant knowledge of the cybersecurity cross-border risks. Their active participation in cooperation with the CS-NCAs and RP-NCAs foreseen in this network code is essential to classify entities on their territory as "critical-risk" or "high-risk" entities, assess the cost-effectiveness of cybersecurity investments and issue temporal derogations for any entity in Table 1 from the minimum and advanced cybersecurity requirements. The NRAs shall also monitor compliance with the network code, its implementation, inspection and supervise operators involved in the execution of the network code at national level, and reviewing the past performance of network security, quality of supply and reliability rules involved in cross-border electricity flows. Therefore, NRAs may be expected to have or gain the competence to monitor cost-effectiveness through the benchmarking activity as described in chapter 8.2. In addition, NRAs do also have an important role in supporting ACER with monitoring the implementation of the network code and benchmarking costs at EU level.

Finally, the **Electricity Coordination Group (ECG)**, established pursuant to the "Commission Decision of 15 November 2012 setting up the Electricity Coordination Group" [20] has among its tasks to "serve as a platform for the exchange of information and coordination of electricity policy measures having a cross-border impact". Thus, the ECG shall be informed periodically on the establishment and implementation of the network code.

[20] OJ C 353, 17.11.2012, p. 2–4

Box 2: List of deliverables chapter 2	
Deliverable	Responsibility
1. Periodically inform ECG on the establishment and implementation of the network code	ACER

3 Cybersecurity risk assessment for cross-border electricity flows

The objective of the cybersecurity Cross-Border Risk Assessment is to identify risk scenarios for the operational reliability of the electricity systems that, through a cyber-attack, can generate adverse events that impede the regular circulation of cross-border electricity flows and/or the regular distribution of electricity to a relevant part of the consumer audience.[21]

The risk assessment methodology will provide the rules for the definition of the ECRIs and ECRICs as described in chapter 1.5 which, together with the distinction of critical-risk/ high-risk entities, will allow to identify the stakeholders subject to minimum or advanced cybersecurity requirements.

The cybersecurity risk assessment shall focus on assessing cyber risks that may impact cross-border operations and safety. In particular for electricity systems, this focus should be put on vulnerabilities that affect the real-time aspects of electricity flows, the cascading effects of electricity incidents and the real-time nature of systems operating the grid. Financial, reputational, and legal cybersecurity risks which are unlikely to impact cross-border electricity flows, shall not be assessed.

3.1. Integrated top-down and bottom-up cybersecurity risk assessment methodology for cross-border electricity flows

Currently there are two main approaches for conducting a cross-border risk assessment, which complement each other:

- A top-down cybersecurity risk assessment (see section 3.2) starts at the highest conceptual level and works down to the details. It is faster and with a high-level scope, addressing general and common risk scenarios. Thus, the top-down approach may be effective for cybersecurity governance and to guide security-related decisions.

- A bottom-up cybersecurity risk assessment (see section 3.3.) begins down with the details and works its way up to the highest conceptual level. It is more detailed, addresses specific scenarios and takes time, but is effective in identifying risk where there is diversity between the assessed entities. During the bottom-up risk assessment, risks are identified at entity and Member State level, and the more severe risks at these levels are carried over to the higher levels, ending up at regional level.

The network code shall apply an integrated top-down and bottom-up cybersecurity risk assessment methodology and ensure their complementarity, governance and flexibility.

The risk assessment shall be integrated at regional and pan-European level as illustrated in Figure 1 below. This means that results of both top-down and bottom-up assessments, when finalised, shall be merged to close gaps resulting from weaknesses in each of the assessments. As a result, the Cross-Border Electricity Cybersecurity Risk Assessment Report (see chapter 7) will summarise risks combined from the two assessments.

[21] Chapter 8 of the SGTF EG2 / Cybersecurity Report of June 2019

The integrated risk assessment shall provide the necessary information for risk governance, including identification and mitigation of risks connected to legacy systems, identification of high-risk and critical-risk entities, prioritisation of actions for supply chain security and design cybersecurity exercises. The governance shall be based on information from both the top-down and bottom-up risk assessments. As the top-down approach as described in chapter 3.2, can be executed faster than bottom-up, it shall therefore be used as a basis for risk governance in the transitional period described in chapters 1.6 and 3.5.

Chapter 3.3 describes the entities responsible for conducting the risk assessment at the different levels illustrated in Figure 1. ENTSO-E shall, with the contribution from the EU DSO entity and the RCCs, be responsible for the implementation of the integrated risk assessment methodology, including both top-down and bottom-up approaches. Every second year, the full integrated risk assessment shall be revised and updated considering experience gained in recent and past attacks, new assets subject to new threats and vulnerabilities of the electricity system that could disrupt cross-border electricity flows.

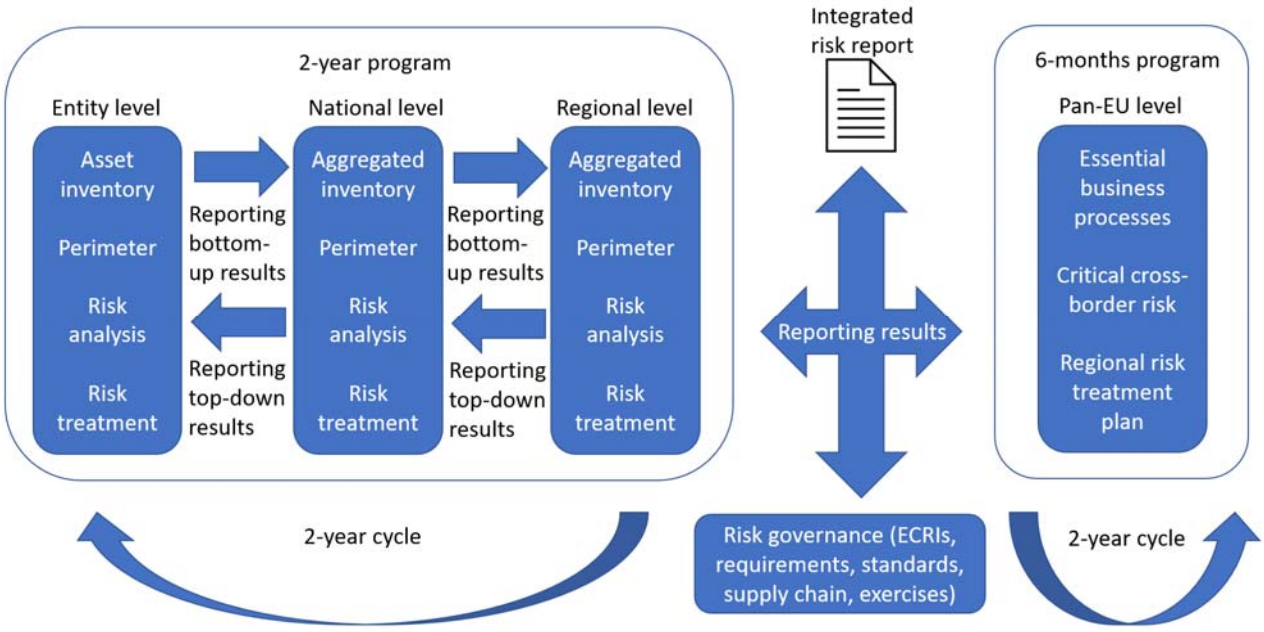

***Figure 1**: Topology of the integrated top-down and bottom-up cybersecurity risk assessment methodology.*

3.2. Top-down cybersecurity risk assessment methodology

The primary objective of the top-down risk assessment shall be to identify high consequence events, identifying how main potential scenarios[22] could materialise through a cyber-attack and then provide guidance through appropriate security controls on how best to defend each Critical Business Process identified against a cyber-attack under a regional risk treatment plan. The risk treatment plan shall be used as base for minimum and advanced cybersecurity requirements for entities listed in Table 1.

[22] The ENTSO-E Continental Europe Operation Handbook (Appendix 3: Operational Security) states that to ensure the safety of the electricity grid, protection must be provided against four main phenomena which may deeply disturb the system or initiate a large-scale incident, namely: (1) Cascade tripping, (2) Voltage collapse, (3) Frequency collapse, (4) Loss of synchronism.

The top-down risk assessment shall also take as input the results of the Regional (level 3) risk assessments and the National (level 2) risk assessments which will identify national cyber risk concerns from the bottom-up approach.

The network code shall ask ENTSO-E and the EU DSO entity to establish a top-down risk assessment working group (the "Working Group"), which shall represent the interests of all critical-risk and high-risk entities. ENTSO-E and the EU DSO entity shall be responsible for properly operating such Working Group and providing appropriate resources to assess cross-border electricity flow cyber risks. The Working Group shall:

i) Identify Critical Business Processes which could pose critical operational and safety issues to the resilience of cross border electricity flows;
ii) maintain a Risk Impact Matrix (RIM) together with appropriate operational limit thresholds for the purposes of cross-border electricity flow cyber risk evaluation purposes;
iii) perform a top-down risk assessment on every Critical Business Process identified, using internationally recognised techniques such as Business Impact Analysis (BIA) together with the Smart Grid Architecture Methodology (SGAM) model to perform threat modelling and derive appropriate security controls.

ENTSO-E in collaboration with the EU DSO entity and the RCCs shall maintain a Regional cyber risk treatment plan, which shall be complementary to the Cross-Border Electricity Cybersecurity Risk Assessment Report, and which shall provide:

i) a description of mandatory and/or advisory–only functional security controls providing adequate protection (assurance) against cyber-attacks;
ii) a description of advisory-only, non-functional security requirements, such as quality, assurance level and compliance to national or international standards.

ACER, in cooperation with ENISA, and assisted by the CS-NCAs, the NRAs and the RP-NCAs shall issue opinions on:

i) the selection of Critical Business Processes and their criticality under cyber risk process and asset identification;
ii) the Critical Business Process cyber risk impact severity ratings;
iii) the content of the Risk Impact Matrix and associated thresholds, which are the assumptions for evaluating cyber risk;
iv) the mandatory functional and non-functional security controls.

ENTSO-E and the EU DSO entity shall periodically review every two years the Cyber risk list and Cyber risk treatment plan and amend it according to ACER's opinions and any changes in overall cyber risks.

3.3. Bottom-up cybersecurity risk assessment methodology

The integration of the bottom-up approach in the network code must be aligned with the provisions of Articles 5 to 7 of the Risk Preparedness Regulation for the identification and updating of risk preparedness plans at entity, Member State and regional levels. The network code shall set rules to carry out a risk assessment at these three levels:

3.3.1. First level of risk assessment (entity level)

The first level of risk assessment shall, at least, include the following four steps:

1) **Step 1: Asset inventory:** The network code shall set rules to clearly identify in a harmonised way individual assets and create asset inventories. These rules shall apply to critical-risk and high-risk entities. These entities shall identify assets that may affect cross-border electricity flows directly or indirectly. The network code shall also provide specific mechanisms for the identification and treatment of the legacy systems that will not be able to reach a sufficient minimum level of cybersecurity, the protection and/or replacement of which shall be considered carefully in a broader context and with a long-term perspective.

2) **Step 2: Electricity cybersecurity perimeter:** The network code shall define the methodologies and tools to define an electricity cybersecurity perimeter. ENTSO-E shall, in cooperation with the EU DSO entity, establish clear rules and harmonised templates for implementation of the electricity cybersecurity perimeter. These templates shall be used on a voluntary basis at entity level but shall be compulsory to use at Member State level.

3) **Step 3: Risk analysis:** A risk analysis shall be conducted based on assets inventoried in the previous step. At the entity level, the analysis is performed by the entity. At Member State level, national authorities are responsible; at the regional level, ENTSO-E is responsible in cooperation with the EU DSO entity.

4) **Step 4: Risk treatment:** All critical-risk and high-risk entities shall establish a risk treatment plan to reduce risks identified during the risk analysis. Member State level risk treatment plans shall also be established. National rules on risk acceptance level may be applied for treating risks identified through assessments at entity and Member State levels. If such rules are not present, entities may choose their preferred risk acceptance level for internal risk treatment[23] and submit it to their NRA and CS-NCA and RP-NCA.

The ongoing mutations of cybersecurity threats that may affect cross-border electricity flows will require the network code to provide a mechanism to set a dynamic scope for the asset inventory and for the definition of the cybersecurity perimeter, which shall be reviewed at least once every two years by NRAs, CS-NCAs and RP-NCAs. This means that the scope of application of the cybersecurity risk assessment of cross-border electricity flows shall be periodically reviewed considering experience gained in recent and past cyberattacks, new assets subject to new cyberattacks and vulnerabilities of the electricity system that could disrupt cross-border electricity flows.

3.3.2. Second level of risk assessment (Member State level)

The second level of risk assessment consists of Member State level scenarios that may potentially escalate to a trans-national cybersecurity incident or attack. In general, CS-NCAs, RP-NCAs and NRAs shall be responsible for aggregating assets inventoried and risks analysed in the first level of risk assessment and report to the regional level. Except from the aggregation, the methodology shall be identical to the first level of risk assessment.

3.3.3. Third level of risk assessment (regional level)

Built on the risk assessments performed and consolidated on the previous two levels, ENTSO-E, in cooperation with the EU DSO entity and the RCCs, shall assess which scenarios would likely disturb or impede the regular execution of cross-border electricity flows at regional level. ENTSO-

[23] Risk treatment measures for harmonising cybersecurity cross-border will be decided on the third level of risk assessment, and therefore single entities and Member States may design their own risk treatment plans to reduce entity specific and national risks due to own preferences.

E and the EU DSO entity may also, to the extent they find reasonable, include other stakeholders listed in Table 1 in the risk assessment. The third level of risk assessment shall aggregate assets inventoried and risks analysed in the second level of risk assessment. Except from the aggregation, the methodology shall be similar to the one used for the first level of risk assessment.

3.4. Governance of integrated top-down and bottom-up cybersecurity risk assessment methodology for cross-border electricity flows

The network code shall provide for the following specific governance that allows all relevant stakeholders to appropriately participate in the network code implementation activities:

3.4.1. For the development of the definition and review of the scope of activities at each level of cybersecurity risk assessment:

1. ENTSO-E in cooperation with the EU DSO entity shall be responsible for drafting the definition and revision of the scope of activities of the first level of cybersecurity risk assessment. All critical-risk and high-risk entities, through their own representatives and/or associations, shall be consulted and shall actively participate in the definition and revision of the scope of activities of the first level of the risk assessment,
2. ENTSO-E, in cooperation with the EU DSO entity, shall be responsible for drafting the definition and revision of the scope of activities of the second level of cybersecurity risk assessment. All Member States, through their CS-NCAs, in cooperation with the NRAs and the RP-NCAs, shall be consulted and shall actively participate in the definition and revision of the scope of activities of the second level of cybersecurity risk assessment,
3. ENTSO-E, in cooperation with the EU DSO entity and the RCCs, shall be responsible for drafting the definition and revision of the scope of activities of the third level of cybersecurity risk assessment,
4. ENTSO-E, in cooperation with the EU DSO entity, shall be responsible for drafting the definition and revision of the scope of activities of the pan-EU level of cybersecurity risk assessment,
5. The ECG, ACER and ENISA, shall be informed and consulted on the activities for each level,
6. ENTSO-E, in cooperation with the EU DSO entity shall accordingly revise the scope of activities for each level.

3.4.2. For the development of cybersecurity risk assessment methodologies, as well as the establishment of standards, methodologies and tools for the execution of the cybersecurity risk assessment of cross-border electricity flows:

7. All critical-risk and high-risk entities, through their own representatives and/or associations, shall be consulted on the draft methodologies,
8. The ECG, ACER and ENISA, shall be informed and consulted,
9. ENTSO-E, in cooperation with the EU DSO entity shall accordingly revise the risk assessment methodologies and tools.

3.4.3. For the purposes of executing the Cross-Border Cybersecurity Risk Assessment at each level:

10. For the execution of the cybersecurity Cross-Border Risk Assessment for the first level, each critical-risk and high-risk entity shall execute the risk assessment based on scopes of activities of the first level of cybersecurity risk assessment, set at point 1. Results shall be provided for further escalation to the CS-NCAs, in cooperation with the NRAs and with the RP-NCAs for further escalation.

11. For the execution of the cybersecurity Cross-Border Risk Assessment for the second level, all Member States, through their CS-NCAs in cooperation with the NRAs and the RP-NCAs, shall organise the risk assessment based on scopes of activities of the second level of cybersecurity risk assessment, set at point 2. Critical-risk and high-risk entities with prominent roles shall be invited to advise in the execution of the risk assessment. Relevant results shall be provided to ENTSO-E and the EU DSO entity for further escalation.
12. For the execution of the cybersecurity Cross-Border Risk Assessment for the third level, ENTSO-E, in cooperation with the EU DSO entity and the RCCs, after receiving all necessary information as result of the risk assessment at point 11, shall execute the risk assessment based on scopes of activities of the third level of cybersecurity risk assessment, set at point 3.
13. For the execution of the cybersecurity Cross-Border Risk Assessment for the pan-EU level, ENTSO-E, in cooperation with the EU DSO entity and the RCCs, shall execute the risk assessment based on scopes at point 4.

3.4.4. To report the results of the cybersecurity risk assessment:

14. The results of the integrated top-down and bottom-up cybersecurity risk assessment shall be consolidated in a Cross-Border Electricity Cybersecurity Risk Assessment Report (see chapter 8.3) that shall be provided by ENTSO-E in cooperation with the EU DSO entity to the NIS Coordination Group for further analysis, particularly to identify crucial interdependencies with other sectors where an additional level of harmonisation may be needed.
15. The Cross-Border Electricity Cybersecurity Risk Assessment Report shall assess and certify the improved state of the cybersecurity posture of the electricity sector. It shall be prepared by ENTSO-E in cooperation with the EU DSO entity and with contribution from critical-risk and high-risk entities through their own representatives and/or associations. It shall be submitted to the European Commission and to ACER for their opinion.
16. The Cross-Border Electricity Cybersecurity Risk Assessment Report shall include Critical Business Processes which shall act as the reference for compliance and product assurance activities. The network code shall set the structure and general content of the risk assessment report (see also 8.3 for the overall description), which at least shall contain the following information:
    i) Under cyber risk process and asset identification:
        - Name and high-level description of the Critical Business Process together with a description of the identified cross-border electricity flow cyber risk and the consequences of a successful cyber-attack causing disruption to that Critical Business Process.
        - The underlying IT or OT systems and components (asset inventory) which support that Critical Business Process using the Smart Grid Architecture Methodology (SGAM) model.
        - A mapping to a Functional Process Area.
    ii) Under cyber risk impact identification: the Business Impact Analysis evaluation cyber risk Severity Ratings in terms of Confidentiality (unauthorised access), Integrity (unauthorised modification) and Availability (unplanned outage).
17. Within three months of receipt the report at point 15, ACER shall provide the European Commission with its opinion after consulting ENISA and the ECG.
18. Within three months of receipt of ACER's opinion, the European Commission shall deliver an opinion on the Cross-Border Electricity Cybersecurity Risk Assessment Report.
19. Within three months of receipt of the opinion from the European Commission, ENTSO-E and the EU DSO entity shall accordingly review the final version of the Cross-Border Electricity Cybersecurity Risk Assessment Report.

20. The report shall be subject to the rules of protection of exchange of information (see chapter 7). For this reason, the report may be released in a sanitised public version without those annexes that, for the nature of their confidentiality, may be released on “need-to-know basis”. A full and confidential version shall be distributed on “need-to-know basis”, only to NISCG members, to ACER, to ENISA and to the European Commission. Before the release of the public sanitised version, the NIS Coordination Group shall provide its approval.
21. ENTSO-E and the EU DSO entity are responsible for the compilation and the release of the report in line with the rules defined above.

3.5. Transitional Risk assessment methodology

The network code shall provide that the existing methodologies for the transition period shall be used for cross-border risk assessment purposes until the final methodology is defined and delivered during the first two years after the entry into force of the network code. As the top-down approach can be executed faster than the bottom-up one, it shall therefore be used as a basis for risk governance to deliver the transitional list described in chapter 1.6 within the first six months after the entry into force of the network code. Likewise, after defining a suitable scope of activities, the risk assessment methodologies described and/or further developed in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and ISO/IEC 27019 can provide solid foundation for conducting a cybersecurity risk assessment for the first level. For the second and third levels, after defining the proper scope, the risk assessment methodologies described and/or further developed in ISO/IEC 27005 and ISO 31000 can provide the basis for conducting a cybersecurity risk assessment for cross-border electricity flows no later than two years after the adoption of the network code**.**

Box 3: List of deliverables chapter 3	
Deliverable	Responsibility
1. Cross-border electricity cybersecurity risk assessment report, to be reviewed every 2 years	ENTSO-E and the EU DSO entity, with contributions from critical-risk and high-risk entities through their own representatives and/or associations, and after the opinion of ACER and the European Commission, and approval of the NIS coordination group.

4 Common Electricity Cybersecurity Framework

To ensure a common electricity cybersecurity level across borders, the network code shall establish a set of minimum cybersecurity requirements that shall be mandatory for both high-risk and critical-risk entities. In addition, the network code shall establish a set of advanced cybersecurity requirements only for critical-risk entities. These two sets of requirements shall be the basis of the common electricity cybersecurity framework. The content of this common electricity cybersecurity framework shall be based on mandatory functional and non-functional security controls identified in the risk assessment as described in chapter 3.2, obligations listed in Table 2 and electricity requirements and standards that are commonly applied for cybersecurity in the EU.

In order to preserve investments and security plans already in place in Member States and to give direction for the common electricity cybersecurity framework, the network code shall ask ENTSO-E and the EU DSO entity, advised by ACER and ENISA, to provide an **Electricity Requirements and Standards Mapping Matrix (ERSMM).** The ERSMM shall map requirements of the common electricity cybersecurity framework to requirements of selected legislative frameworks and

internationally recognised standards. The selection shall be based on whether implementation of the framework or standard will likely result in compliance with all or most requirements in the forthcoming common electricity cybersecurity framework. The aim of the ERSMM is to avoid double work on implementing cybersecurity requirements. Requirements from international standards and national legislations may overlap with the common cybersecurity framework, and in such cases, the ERSMM may be used to track conformity with requirements in the common electricity cybersecurity framework.

When the common electricity cybersecurity framework has been established, compliance with requirements in the framework shall be verifiable by a third party. The third party shall be accredited through an accreditation model and considered as a conformity assessment body in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council. Verification by the third party may follow one of the following three paths:

1. **Verification through third party certification or statement of applicability:** Standards covering cybersecurity requirements equivalent to the common electricity cybersecurity framework shall be listed in the ERSMM and may be used for verification through certification or a statement of applicability from a conformity assessment body.
2. **Verified peer review process:** Industry experts on electricity cybersecurity may establish a template of controls covering cybersecurity requirements equivalent to the common electricity cybersecurity framework. If a conformity assessment body has verified that the template sufficiently covers the requirements in the common electricity cybersecurity framework, the template may be registered in the ERSMM and used for peer review. The process shall be overlooked by NRAs and/or CS-NCAs and the frequency of reviews shall be reported to ACER by each NRA annually if peer review is in use in the Member State.
3. **Verified framework of legal obligations:** National legal obligations that impose to entities the implementation of cybersecurity requirements equivalent to the common electricity cybersecurity framework shall be listed in the ERSMM and may be used for verification through inspection and supervision by authorities in the Member States. A conformity assessment body shall verify that the requirements in the legal framework sufficiently cover the requirements in the common electricity cybersecurity framework. In addition, the NRA shall, on an annual basis, report the frequency of inspections to ACER.

Figure 2 illustrates the three paths to demonstrate implementation of the common electricity cybersecurity framework.

***Figure 2**: Three tracks to demonstrate the implementation of minimum and advanced cybersecurity requirements of the common electricity cybersecurity framework.*

The minimum and advanced cybersecurity requirements of the common electricity cybersecurity framework shall, as a minimum, cover the areas presented in Table 2.

Table 2: *Cybersecurity areas the network code shall address, mapped to entities who shall be subject to requirements in the listed cybersecurity areas. V = Compulsory, V* = Implicit but not enforced*

Cybersecurity areas	Small[24] and Micro Enterprises	Minimum Requirements (High-risk entities	Advanced Requirements (Critical-risk entities)
1. Basic Cybersecurity Hygiene requirements (see last paragraph of Chapter 1.3).	✓	✓*	✓*
2. Obligation to compile an asset inventory and to define the internal electricity cybersecurity perimeter.		✓	✓
3. The assets potential impact on cross-border electricity flows shall be described in the inventory.		✓	✓
4. Obligation to perform a cybersecurity risk assessment and establish a risk treatment plan		✓	✓
5. Take part to a cross-border cybersecurity Risk assessment for electricity cross-border flows.			✓
6. Obligation to implement requirements from the common electricity cybersecurity framework, including functional and non-functional cybersecurity controls.		✓	✓
7. Verification of the implementation of advanced requirements from the common electricity cybersecurity framework, including functional and non-functional cybersecurity controls.			✓
8. Obligation to take part and contribute to the information sharing and dissemination system for the electricity cybersecurity cross-border flows and monitoring, benchmarking and additional reporting obligations.		✓	✓
9. Obligation to establish incident handling and crisis management procedures.		✓	✓
10. Obligation to set procedures in case of a disruption to cross-border electricity flows.			✓
11. Obligations related to Supply Chain Security.		✓	✓
12. Advanced supply chain security in form of product verification.			✓
13. Obligation to conduct internal cybersecurity exercises on a regular basis.		✓	✓
14. Participation in national and regional electricity cybersecurity exercises.			✓

Within a period of three months from the entry into force of the network code and in the absence of a common electricity cybersecurity framework, ENTSO-E and the EU DSO entity, advised by ENISA and ACER and with the assistance of the NRAs and the CS-NCAs, shall prepare a

[24] In this context, Small and Micro Enterprises below the Size Cap defined at chapter 1.3 and not classified as either high-risk entity or critical-risk entity.

transitional list of prominent International standards and national legislation on electricity cybersecurity to be implemented by entities in preparation for the implementation of the common electricity cybersecurity framework. The transitional list shall be published on the website of ENTSO-E and the EU DSO entity and shall be made accessible to all potential stakeholders.

4.1 Governance for the definition of minimum and advanced cybersecurity requirements, and for the ERSMM

For the purpose of establishing the minimum and advanced cybersecurity requirements (the common electricity cybersecurity framework), the following specific governance shall be followed:

1. ENTSO-E and the EU DSO entity jointly shall establish the common electricity cybersecurity framework and transmit it to ENISA for their opinion and then to ACER for their opinion.

2. All entities listed in Table 1 shall be consulted and shall have the chance to actively participate in updating the minimum and advanced cybersecurity requirements.

For the purposes of establishing the ERSMM, the following specific governance shall be followed:

3. All entities shall be consulted and shall have the chance to actively participate in the process of choosing international standards, national legislation and peer review templates to be included in the ERSMM as well as whether they cover minimum or advanced cybersecurity requirements.

4. ENTSO-E and the EU DSO entity shall jointly consolidate the list of international standards, national legislation and peer review templates, to add to the ERSMM.

5. ACER, with guidance from ENISA, shall provide an opinion on the drafted ERSMM resulting from point 4 above.

6. Within three months of receipt of ACER's opinion, the European Commission shall deliver an opinion on the common electricity cybersecurity framework and the draft for ERSMM.
7. Within three months of receipt of the opinion from the European Commission, ENTSO-E and the EU DSO entity shall accordingly review the final version of the common electricity cybersecurity framework and ERSMM.

The network code shall foresee a reasonable implementation timeline for the common electricity cybersecurity framework following the adoption of the list of requirements described above. Further, the network code shall ensure that the verification processes for the requirements of the common electricity cybersecurity framework is established within 24 months.

The network code shall grant the NRAs and CS-NCAs the right to issue **derogations of a maximum two years for any entity in Table 1 from the minimum and advanced cybersecurity requirements** when:

A. The cost of the implementation of the cybersecurity requirements of Table 2, may exceed the benefits, and when the requirements may generate cybersecurity risks.
B. A cybersecurity plan already exists in the concerned entity, and the cybersecurity plan covers at least 80% of the cybersecurity requirements. This shall be verified by a conformity assessment body.

C. The results of the risk assessment of the entity do not show any direct or indirect impact on cross-border electricity flows.

The list of the derogations resulting from the conditions at points A, B and C, shall be added to the "Cross-Border Electricity Cybersecurity Risk Assessment Report" as an annex, and kept regularly updated jointly by ENTSO-E and the EU DSO entity.

4.2 Supply Chain Security including advanced requirements to product verification

The network code shall encourage the high-risk / critical-risk entities, among all risk assessment and risk management tasks, to manage cybersecurity risks concerning their supply chain. It therefore shall define specific requirements for the supply chain security to ensure that the asset owners, and/or those who operate the assets on behalf of the owners, can control the whole asset supply chain from the design of the product/system along the entire process to install, configure and operate/maintain the system. The control of the supply chain shall focus on the following points:

i) The risk assessment in chapter 3 shall also take into consideration a severe and unexpected corruption of the supply chain, the unavailability of products/systems/services from the supply chain and the possibility that an attack may be initiated by an actor that takes part in the supply chain. Those risks shall lead to set clear rules for the acquisition of system and services, and the diversification of the supply sources, where possible.
ii) The selection of systems with security by design, and security embedded in all the processes during system design and production phase. Secure processes for design and production of systems shall provide assurance of traceability of security operations in each phase of the lifecycle and until the delivery of the system to the production.
iii) The careful selection of critical-risk vendors and critical service providers that apply security rules to the delivery of their systems and products and that can clearly show their capability to fulfil the same security requirements as the high-risk / critical-risk entity. The selection of critical vendors and service providers shall also ensure that the commercial relationships are based on mutual trust, but that the critical-risk / high-risk entity will always have control over the systems and services provided. This will contribute to the harmonisation of the sector, also in the case of outsourcing of systems and services.

All the above points can be implemented by setting up clear procurement templates and procurement protocols in line with relevant procurement rules. Templates and protocols for procurement may also be used to assess if existing contracts are in line with the need to further enhance the control of the supply chain underlying cross-border electricity flows.

The advanced requirements applicable to critical-risk entities shall encourage the following product verification rules:

iv) Concerning products and systems, in the absence of specific European Cybersecurity verification schemes that may cover the systems in use in the context of cross-border electricity flows, the high-risk / critical-risk entities may rely on national schemes, especially if such schemes provide the possibility to be certified by an accredited third party. This shall be considered under the condition that all critical service providers have equal access to both the schemes and the verification capabilities, without negative impact on the acquisition of more secure electricity systems. The network code shall promote the use of cybersecurity verification under the existing schemes and under the European Cybersecurity Certification schemes, providing a fast track to those products/services/systems that have been verified, and therefore, can assure a certain level of security of the supply chain. The network code shall anyway foresee a transitional phase that, starting from international standards and/or National Schemes, will converge in the European Cybersecurity Certification schemes, once suitable schemes are available[25].

In the context of the EU Cybersecurity Certification Framework, the network code may task ENTSO-E and the EU DSO entity, in cooperation with ENISA, to develop a sector-specific guideline on EU products/services/systems verification schemes. The guideline could for instance define what cyber threats should be considered or what types of tests should be performed. Cybersecurity verification shall be made mandatory at latest by 2027.

To prevent that an inappropriate exchange of information concerning critical assets/systems/processes may constitute a risk for the entire electricity system, the network code shall, to the extent possible, set clear rules to require confidentiality and traceability of information exchanges between the critical-risk / high-risk entities and all actors in the supply chain. The rules to require confidentiality and traceability of information exchanges between the critical-risk / high-risk entities shall be applicable also to the communication related to risks between SOCs and CSIRTs of the critical-risk / high-risk entities. The network code may consider appropriate penalties for the infringement that, in case of disclosure of information related to the cybersecurity of cross-border electricity flows, shall be proportionate with the generated level of risk for the grid.

The network code may impose rules for the roll-out of new systems that may be classified as critical systems for cross-border electricity flows or for the systems that take part to the execution of any critical process in the scope of cross-border electricity flows. In the absence of a certification scheme, the roll-out of such new systems shall be subject to penetration testing, whose aim is to identify the conditions under which the system (a single device or the entire branch of the system of which it will be part of may become unstable or unusable due to specific cybersecurity and non-cybersecurity conditions or due to known or emerging vulnerabilities. Critical-risk entities shall be responsible for having penetration tests executed and also document actions performed to reduce risks identified during penetration testing. The penetration testing may be executed by the critical-risk entity, by authorities, by commercial or academic organisations or any other entity the critical-risk entity may find suitable for the task.

Finally, the following additional measures may be considered to further secure the supply chain for cross-border electricity flows:

i) The network code may establish rules for the integration of cybersecurity requirements into tender specifications, setting clear obligations to allow the selection of only those products that comply with current security requirements at point 6 of Table 2.
   - The use of cybersecurity requirements in Request for Information, Requests for Proposals and their further agreements.

[25] From EU cybersecurity certification framework perspective there is a possibility to create a specific annex for ICT products used in the context of cross-border electricity flows under the EU cybersecurity certification scheme.

- The use of vendor due diligence.
- The reliance on cybersecurity certified systems and on vendors that have followed a specific clearance process.
- Procure multiple vendors with interoperability between processes to avoid dependence on a single vendor and vendor lock-in.

ii) The network code may consider obligations for full lifetime support with regular security updates to critical assets and systems. When in these cases lifetime support cannot be reasonably guaranteed, mandatory plans for replacement should be established from the moment this end-of-life support is identified.

iii) The network code may set provisions to impede or limit attempts of supply chain tracking and supply chain infiltration both in the systems development and in the systems operations.

iv) The network code shall promote the secure termination or transition of contracts having relevance for the development and operations of critical assets, especially in case of significant cyber-attacks having an impact on cross-border electricity flows, for which the negligence of the vendor can be demonstrated by the lack of application of known security rules and by international standards.

4.3 Cybersecurity inspections

The network code shall ensure that the measures applied for supervision or enforcement imposed on critical-risk entity and high-risk entity are effective, proportionate and dissuasive, considering the circumstances of each individual case.

The network code shall ensure that CS-NCAs and/or NRAs, where exercising their supervisory tasks, have the power to subject critical-risk and high-risk entities to:

a) on-site individual and coordinated multi-site joint inspections and off-site supervision, including random checks, especially following a cybersecurity incident, or when the network of CSIRTs will signal an imminent risk related to cybersecurity of critical systems, processes, operations that take part to the cross-border electricity flows;
b) random security audits aimed to verify the conformity on risk assessments and of their results;
c) requests of information necessary to assess the cybersecurity measures adopted by a critical-risk / high-risk entity, including documented cybersecurity policies, as well as compliance with minimum or advanced requirements.

Box 4: List of deliverables chapter 4	
Deliverable	Responsibility
1. A Common Electricity Cybersecurity Framework, including: -A minimum set of cybersecurity requirements -A set of advanced cybersecurity requirements	Jointly established by ENTSO-E and the EU DSO entity, to be submitted to ENISA for their opinion and then ACER for their opinion
2. An Electricity Requirements/Standards Mapping Matrix (ERSMM)	ENTSO-E and the EU DSO entity, advised by ACER and ENISA
3. A transitional list of national regulations of electricity cybersecurity and EU/International standards	ENTSO-E and the EU DSO entity, advised by ENISA and ACER and with the assistance of the NRAs and the CS-NCAs
4. A list of the temporary derogations from the minimum and advanced cybersecurity requirements	ENTSO-E and the EU DSO entity

5. Procurement templates and procurement protocols	To be defined by the network code
6. A sector-specific guideline on EU products/services/systems certification schemes	ENTSO-E and the EU-DSO entity, in cooperation with ENISA
7. Monitoring of cost-efficiency of the cybersecurity verification schemes	ACER and ENISA
8. Rules to require confidentiality and traceability of information exchanges between the critical-risk / high-risk entities and all actors in the supply chain	ENTSO-E and the EU DSO entity
9. Rules for the roll-out of new systems that may be classified as critical systems for cross-border electricity flows or for the systems that take part to the execution of any critical process in the scope of cross border electricity flows	ENTSO-E and the EU DSO entity
10. Rules for the integration of cybersecurity requirements into tender specifications, life-time support, limiting supply chain tracking and promote secure termination	ENTSO-E and the EU DSO entity

5 Essential information flows, Incident and Crisis Management

5.1 Data Collection, Sanitisation and Dissemination

The network code shall establish an information collection and sharing system to further support all the critical-risk / high-risk entities in the EU with key security-related information for operations of cross border electricity flows, such as near real-time reporting of cybersecurity incidents, early warnings related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system. There shall also be a possibility for small and micro enterprises to participate in the information collection and sharing system on a voluntary basis, and small and micro enterprises shall be encouraged to participate. The network code may apply own rules connected to the participation of small and micro enterprises. Such rules shall aim to reduce cybersecurity risk following participation of small and micro enterprises as these may not be subject to the common electricity cybersecurity framework and therefore may have a lower cybersecurity standard than the high-risk and critical-risk entities.

The information collection and sharing system for the cross-border electricity flows shall foresee data collection from all critical-risk / high-risk entities, sanitisation and anonymisation of information and the prompt dissemination within 24 hours of a reportable cybersecurity incident to all relevant high-risk and critical-risk entities participating in the system. Proper sanitisation and anonymisation is especially important in case of information that may allow to identify a critical-risk / high-risk entity and may impact security or reputation of anyone part of the information sharing system. The information sharing system shall play a key role in effective and timely sharing of security-related information between critical-risk / high-risk entities, thus enhancing protection from current threats and risks, and allowing them to proactively act on imminent risks. The system to be established through the network code shall complement the information gathering and dissemination flows of the existing CSIRTs Network[26] established through Article 12 of the NIS Directive.

[26] The CSIRTs Network, under the NIS Directive, is a network composed of EU Member States appointed CSIRTs. ENISA has the role of secretariat and actively supports incident coordination upon request.

The network code shall require all critical-risk entities to actively participate and contribute to the information collection and sharing network. To ensure they benefit from such participation, critical-risk entities shall establish a SOC or access SOC services through a MSSP. Depending on the definition of the ECRIs & ECRICs, high-risk entities may also be required to participate and contribute to the information collection and sharing network and establish a SOC or access SOC services through a MSSP. High-risk entities not required to participate and contribute to the information collection and sharing network shall still be required to establish basic services with at least weekly review of logs, notifications and alerts.

A main objective of requiring SOC activities is to make critical-risk / high-risk entities capable of detecting malicious activities to alert other critical-risk / high-risk entities, and to be able to react when alerted to malicious activities of other critical-risk / high-risk entities with minimal delay and with the appropriate combination of cybersecurity and operational skills. The SOC services of critical-risk / high-risk entities shall include at least the following:

i) Monitoring and management of cybersecurity devices and general systems within the critical-risk / high-risk entity;
ii) Intrusion detection, vulnerability scanning (software and configuration) and verification of general cyber hygiene within the critical-risk / high-risk entity;
iii) Participating in a European information-sharing (threat intelligence) program through national SOC networks established by the network code, including cooperation with sector CSIRT and/or national CSIRT and sharing of data about important attacks and vulnerabilities discovered;
iv) Analysing and if needed reacting properly to data received through the information sharing (threat intelligence) program established by the network code;
v) General cybersecurity incident response and participation in crisis management within the critical-risk / high-risk entity.
vi) Take part in the strategic initiative of the new EU cybersecurity strategy to build a network of SOCs across the EU and provide support for the improvement of existing SOCs and the establishment of new ones.
vii) Optional use of Artificial Intelligence enabled services.

SOC activities and services may be shared by more critical-risk / high-risk entities as this will increase efficiency and may provide a viable way to slowly contribute to the creation of additional capacity in terms of human resources and skills. Furthermore, it shall be considered that the terms SOC, MSSP and CSIRT may be used interchangeably or combined in different ways by critical-risk / high-risk entities. The network code shall allow critical-risk / high-risk entities to choose how to organise their SOCs or MSSPs and what terms to use, provided they meet the functional requirements of the network code.

Built on the CSIRT Network already established through the NIS directive, the network code shall establish national information sharing networks following the mesh topology as illustrated in Figure 3. The national information sharing mesh networks shall be composed of SOCs and MSSPs of critical-risk / high-risk entities, national CSIRTs and national Energy Sector CSIRT (where present) or similar. The national CSIRTs and Energy Sector CISRTs of the states that have them, shall also be connected in a similar EU mesh, as illustrated in Figure 3. The organisation in mesh topology ensures rapid exchange of information within networks, first at Member State level, and when information is sanitised and cleared by a national CSIRT, fast sharing at EU level.

Appointed CSIRTs are responsible for data collection, sanitisation and dissemination at Member State level, with a focus on Operators of Essential Services. Further information available at https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

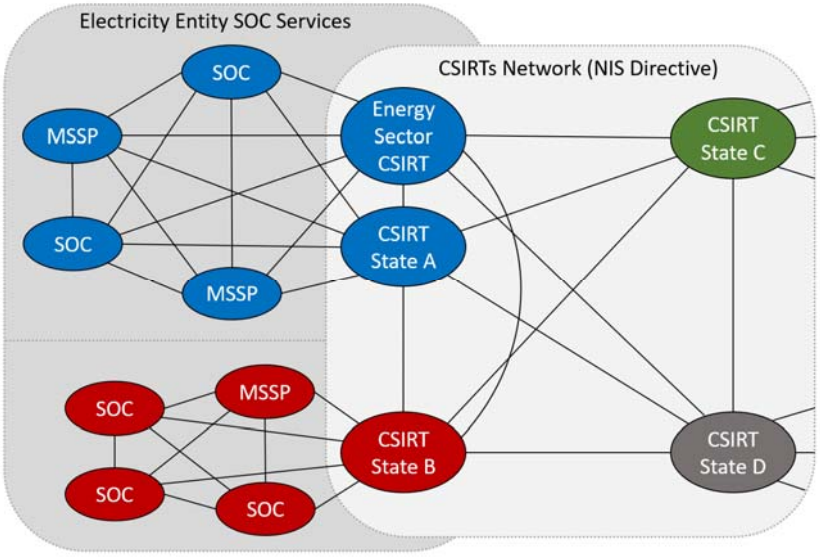

Figure 3: *Illustration of the information sharing meshed relationships between the critical-risk / high-risk entity SOCs or MSSPs and the CSIRTs Network as of the NIS Directive.*

As illustrated in Figure 4, an important role of critical-risk / high-risk entity SOCs or MSSPs shall be to ensure detection capabilities. When a vulnerability or incident is detected, critical-risk / high-risk entities shall have routines for how related information shall be shared within their national mesh networks. Data may be shared directly between the critical-risk / high-risk entities in the state, or through a CSIRT at Member State level for anonymity or sanitisation reasons.

A CSIRT with responsibility at Member State level shall be the main responsible for data collection, sanitisation and dissemination internationally. The execution of this task of the CSIRT shall be monitored by the CS-NCA. Data sanitisation may be conducted on SOC/entity level or on national CSIRT level. During data sanitisation, the CSIRT at Member State level shall ensure that data has been properly anonymised. The competent CSIRT may be appointed by each Member State. In most cases it would be expected that this will be either the national CSIRT established in compliance with the NIS Directive, or a dedicated Energy CSIRT who will receive this role.

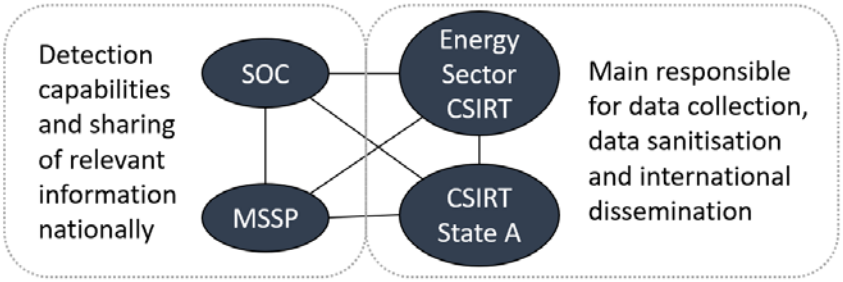

Figure 4: *Main roles of critical-risk / high-risk entity SOCs or MSSPs and CSIRT(s) on national mesh network level*.

The network code shall ensure frequent use of a suitable and highly trustable environment to exchange security information between critical-risk / high-risk entities in EU Member States. This environment should provide critical-risk / high-risk entities with the needed confidence to share incident related information with each other. Critical-risk / high-risk entity SOCs or MSSPs shall have one single point of contact for the purpose of information sharing. Contact points shall not be person-dependent and should have an alternative communication path as backup. Communication within Member State level and EU level information sharing networks shall be encrypted, or

otherwise protected using state of the art best practice techniques and standards. CSIRTs on Member State level may be given the task to define processes and technologies and ensure daily operations of the information sharing networks, complementing the NIS 2 directive.

All critical-risk / high-risk entities shall report the following information within the national mesh:

i) Detected cyber-attacks, cyber threats and near misses.
ii) Vulnerabilities and attacks connected to third parties with which they have any commercial or working related relationship or suppliers and their services.
iii) When identified, Indicators of Compromise (IoCs): e.g., virus signatures, compromised URL and IP addresses, hashes of malware files, etc.
iv) Other information of importance for preventing, detecting, responding to or mitigating cybersecurity incidents.

Any critical-risk / high-risk entity shall share information with its national CSIRT. Information dissemination shall not constitute a risk for the sender or any actor in the energy landscape. In cases there is a high probability that information sharing would cause harm, critical-risk / high-risk entities should seek guidance from national CSIRTs to allow, where possible, data sanitisation to reduce risk from data sharing. If data dissemination at EU level is considered a risk despite data sanitisation, the CSIRT may withhold information and be advised by ACER and ENISA, who shall advise on how to proceed.

Routines shall be established to ensure that critical-risk / high-risk entities issue an initial notification to the national CSIRT within the following timelines:

- 4 hours after the determination of a Reportable Cyber Security Incident. The network code shall provide a definition of a Reportable Cyber Security Incident, including the time when the delay begins. The CSIRTs Network shall be consulted when defining criteria to define Reportable Cyber Security Incidents.

The CSIRTs at Member State level shall be required to share information with the CSIRT network, and the initial notification shall be given within the following timelines:

- 18 hours after receiving a reportable cybersecurity incident.
- Further delay than 12 hours must be justified by the national CSIRT.

CSIRTs at Member State level receiving reportable cybersecurity incidents through the CSIRT network but with origin in a Member State's electricity SOC network, shall be required to share its relevant information within its national electricity SOC network within the following timelines:

- 2 hours after receiving a reportable cybersecurity incident through the CSIRT network.

ENISA may provide critical-risk / high-risk entities with guidance on establishing SOC capabilities or engaging with MSSPs. ENISA shall also keep up to date an illustration of the information sharing network by mapping different information sharing initiatives and their connections. This may be done by extending the CSIRTs Network inventory that ENISA are maintaining today.[27]

RCCs, ENTSO-E and the EU DSO entity shall participate in the information collection and sharing system in a similar manner to critical-risk / high-risk entities, but their access point to the European CSIRT Network shall be through a central entity that may be CERT-EU of which they shall become constituents.

[27] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory

The network code shall promote cost efficiency. One example is that the network code shall allow two or more Member States to have a shared Energy Sector CSIRT. National CSIRTs shall also have the right to delegate to other National CSIRTs the supervision of entity's SOC on a case-by-case basis, e.g., for multinational entities.

ENISA may keep a track record of events such as incidents, crises and vulnerabilities that have been reported in the international information sharing network.

5.2 Electricity Cybersecurity Early Warning System (ECEWS)

An early warning system[28] can be described as a solution for threat information gathering, processing and notification of threat information. It is about systematically providing the right information to the right people at the right time – connecting the dots across relevant actors.[29] The network code shall establish an early warning system specific for cybersecurity events, which shall identify conditions and indicators that frequently correlate with larger cyber-attacks within the electricity sector or, in general, within the energy sector. By identifying such conditions and indicators, the ECEWS shall advise EU CSIRT and SOC networks on early preventive actions before incidents materialise and/or lead to cross-border effects. The ECEWS shall be operated by ENISA, and CERT-EU shall feed the system with information. ENISA shall ensure the ECEWS is operable within 3 years after the network code has entered into force.

The ECEWS shall focus on innovation in methodologies and follow trends in digital development. The ECEWS shall cooperate closely with relevant working groups and research communities, especially the Electricity Coordination Group and EU Cybersecurity Competence Centre.

The ECEWS process may follow four main steps:

1. Global scan of cyber risk conditions and relevant indicators for the electricity sector.
2. Identification of risk factors and indicators that do require further EU analysis and preventive actions.
3. Analysis that combines the relevant data available and investigate the potential risk, as well as effectiveness of possible preventive actions.
4. Notification to EU critical-risk / high-risk entities through the CSIRT Network about the identified risks and recommended preventive or mitigation actions.

The steps shall be repeated as illustrated in Figure 5.

[28] Smart Grid Task Force Expert Group 2 - Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. Final Report June 2019, p. 75.
[29] Factsheet - EU Conflict Early Warning System: https://eeas.europa.eu/archives/docs/cfsp/conflict_prevention/docs/201409_factsheet_conflict_earth_warning_en.pdf

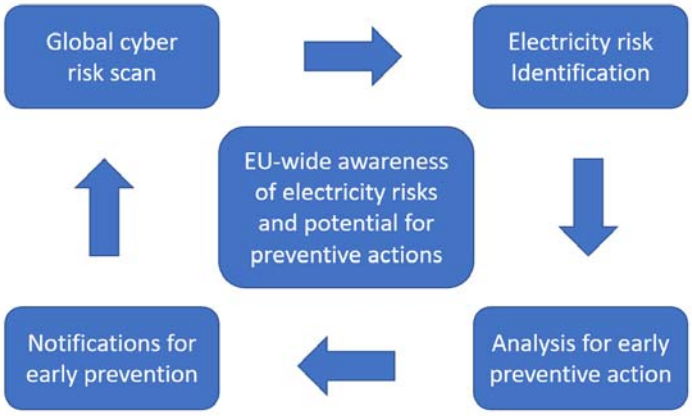

Figure 5: *Illustration of steps of a ECEWS for the EU electricity sector.*

The global scan of cyber risk factors and indicators should include information shared through the EU CSIRT Network.

ENTSO-E and the EU DSO entity shall monitor the effectiveness of ECEWS. The European Commission, ACER, CS-NCAs, NRAs and national CSIRTs shall be regularly informed. A report on the effectiveness of ECEWS shall be sent annually to the European Commission, ACER and ENISA. ACER, advised by ENISA and after consulting the CS-NCAs, NRAs, SOCs and CSIRTs, if deemed necessary, shall issue an opinion to the European Commission on the report on the effectiveness of the ECEWS.

5.3 Incident Detection and Handling

The network code shall establish effective processes to identify, classify and respond to cross-border cybersecurity incidents that will or may affect cross-border electricity flows. The processes shall aim to minimise the impact of a cyber-incident or attack and to react quickly to restore the cross-border electricity flows. The network code shall focus particularly on the management of cyber-attacks or incidents that:

i) may reoccur within the geographical areas of different system operation regions, multiplying the effects of cross-border electricity flows;
ii) may, through cyber means, generate a general instability that may have a potential impact on the electricity flows (e.g., in operational aspects such as frequency, voltage, balancing);
iii) involve legacy systems in which attacks on equipment cannot be mitigated in a normal fashion or in a reasonable time and at a justifiable cost.

Critical-risk / high-risk entities shall have the necessary capabilities to detect cyber incidents and manage cross border cybersecurity incidents with the necessary support from national, regional and EU wide resources.

The network code shall establish a system in which, in the event of incidents with significant effects, personnel from affected critical-risk / high-risk entity SOCs or MSSPs shall coordinate efforts through an ad hoc coordination group. Rules shall be defined on how to appoint the entity which shall lead the ad hoc coordination group. This function of the ad hoc coordination group shall be exercised periodically to ensure its efficiency in the case of incidents with significant effects.

The network code shall:

i) Ensure the own SOCs or MSSPs have access to information provided by the CSIRT network at a need to know level.
ii) Describe how incidents shall be classified based on an incident classification scale[30] established prior to reporting to the national information sharing network or just a national CSIRT.
iii) Provide criteria to determine if an identified cybersecurity Incident is a **Reportable Cyber Security Incident**.[31]
iv) Require critical-risk / high-risk entities to establish incident management procedures for cybersecurity incidents, including roles and responsibilities, standardising tasks and reactions based on the observable evolution of the incident within the entity and in the nearby cybersecurity perimeters.
v) Provide specific requirements to handle incidents with potential cross-border effects, based on the principle of proximity to the incident.

Cross-border cybersecurity incidents shall be dealt in accordance with the principle of proximity, which implies that an incident shall be handled organisationally as close to the affected entities as possible. Examples of involvement in incident management are provided in Figure 6. Incident X illustrates a smaller incident that is handled locally by a critical-risk / high-risk entity and its MSSP without the involvement of any other entities on the network.

Incident Y illustrates a larger incident impacting two critical-risk / high-risk entities. Here, the national CSIRT is involved to support the SOCs of the affected entities. In this case an ad hoc coordination group made up of personnel from the affected critical-risk entities and with support from the national CSIRT shall coordinate, support and provide all tools required to remediate the crisis.

Incident Z illustrates an incident with cross-border effects, in which a critical-risk / high-risk entity in state A and one or more entities in state C are affected. As in the case of incident Y, the affected entities will establish an ad hoc coordination group. The ad hoc coordination group shall, upon request, be supported by national CSIRTs from all affected Member States. In cases of cross-border incidents, the ad hoc coordination group shall coordinate, support and provide tools to remediate the crisis. The CSIRTs network shall be informed of ongoing developments and changes at regular intervals. Ad hoc coordination groups dealing with cross-border incidents should also be able to count on the support of ENISA and other EU resources.

ENTSO-E and the EU DSO entity in cooperation with RCCs shall handle incidents within their own organization. In cases of larger incidents, and under the condition that they will become members of the CERT-EU, they may be able to receive support through the CERT EU.

The network code shall consider the reporting guidelines developed by the NIS Coordination Group pursuant to Article 14(3) of the NIS Directive, including the circumstances for reporting incidents and the format and procedure for such reporting.

[30] One example on an established incident classification scale is: https://eepublicdownloads.entsoe.eu/clean-documents/SOC%20documents/Incident_Classification_Scale/2014_ICS_Methodology.pdf Further, there are ongoing work on incident taxonomy/classification by the Reference Security Incident Taxonomy Working Group created by ENISA and TF-CSIRT: https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

[31] Criteria may be based upon the definition of a Reportable Cyber Security Incident from the NERC Implementation Guidance for the CIP-008-6 Standard: A Cyber Security Incident that compromised or disrupted i) A Bulk Energy System Cyber System that performs one or more reliability tasks of a functional entity, ii) An Electronic Security Perimeter of a high or medium impact Bulk Energy System Cyber System, or iii) An Electronic Access Control or Monitoring System of a high or medium impact Bulk Energy System Cyber System.

NRAs or CS-NCAs shall report large-scale cross-border incidents[32] arising from cyber-attacks to Europol's European Cybercrime Centre as soon as there is a reasonable certainty that the disruption is the result of a cyber-crime. The network code shall define a threshold for cyber incidents to be defined as large.

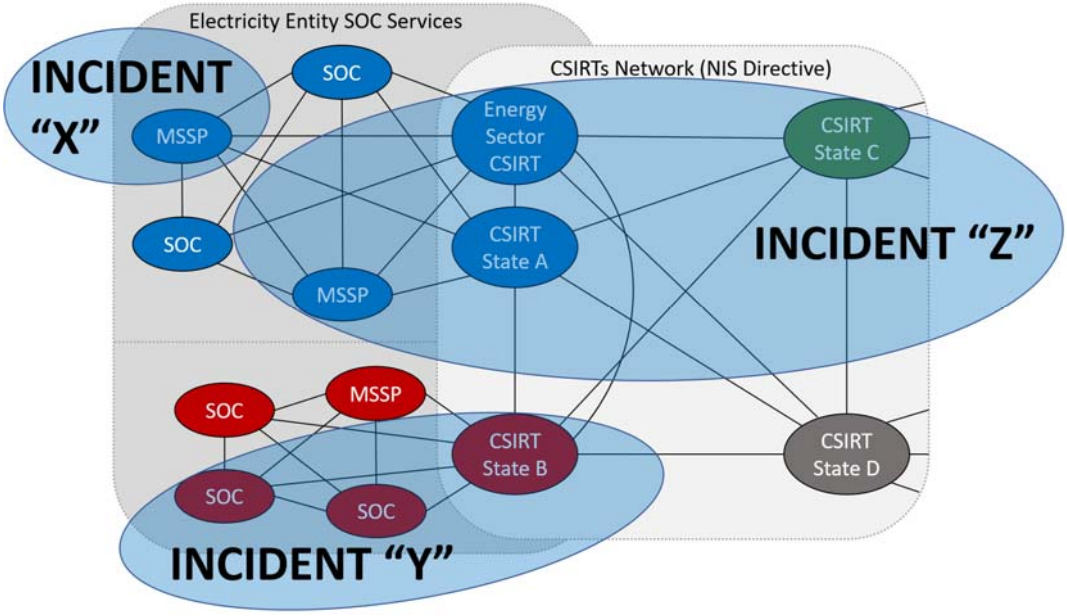

Figure 6: *Examples of involvement of response environments for incident handling on critical-risk/high-risk entity (X), national (Y) and regional (Z) level. Involvement shall follow the principle of proximity.*

5.4 Crisis Management[33]

The Crisis Management processes shall build on the Incident Handling processes described in chapter 5.2. A combination of cyber incidents may lead to a crisis and in such cases, the principle of organisational proximity shall still be respected. This means that if, for example, an ad hoc coordination group has been established to coordinate and support during an incident as described in Chapter 5.2, and that incident leads to a crisis, the ad hoc coordination group shall simply be expanded as needed and combined with one or more crisis management team(s) in charge of crisis management.

Critical-risk / high-risk entities shall have the necessary crisis management capabilities to manage crises with the support from national, regional and European resources, depending on the nature of the crisis.

The network code shall support the functioning of the European Union society and economy in a crisis by increasing the capability of critical-risk / high-risk entities to handle crisis situations caused by cyber incidents. This includes the ability of critical-risk / high-risk entities to keep business processes running during a crisis.

[32] We apply the NIS Directive's definition of a large-scale incident: An incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market.

[33] The term crisis refers to a cybersecurity-related incident with potential of generating a cascading effect that would make it impossible to supply electricity to customers

Additional rules shall be established in the network code on how the cross-border cybersecurity crisis shall be managed in a joint effort between affected critical-risk / high-risk entities, National Energy CERTs, NRAs, CS-NCAs and/or RP-NCAs, National CSIRTs and RCCs.

The network code shall include general requirements on crisis management, including:

i) Testing and exercise routines for the critical-risk / high-risk entities Crisis Management, Business Continuity and Disaster Recovery Plans.
ii) How critical-risk / high-risk entities shall analyse and share lessons learned after managing a crisis.
iii) An obligation to participate in information sharing with the Crisis Management System CyCLONe[34] and the CSIRT network though national or sectorial representatives.

The network code shall define specific requirements related to:

i) Minimum content of Crisis Management Plans for critical-risk / high-risk entities, including:
   - Metrics to define a crisis, including metrics to activate cross-border crisis management plans.
   - Roles and responsibilities for crisis management within the critical-risk / high-risk entities and the CSIRT Network.
   - Rules for communication and information sharing during a crisis.
   - The Crisis Management Plan shall also specify the rules for the use of the metrics defined above.

ii) Minimum content of Business Continuity Plans for critical-risk / high-risk entities, including:
   - Cyber business continuity processes.
   - Business continuity locations including hardware and software.
   - Roles and responsibilities connected to Business Continuity Processes.

iii) Minimum content of Disaster Recovery Plans for critical-risk / high-risk entities, including:
   - Processes for the backup and storage of information required to recover Cyber System functionality of critical-risk / high-risk entities.
   - Processes to complete a full cyber recovery.

Finally, the network code shall also consider the following:

- ENISA may provide expert help and advice for critical-risk / high-risk entities on crisis management, with special attention to ICS/SCADA cybersecurity events.
- The network code shall complement existing rules in the Risk Preparedness Regulation. In particular, the declaration of an electricity cybersecurity crisis shall follow the methodology for declaring an electricity crisis described in Point 2 and 3 of Article 14 of the Risk Preparedness Regulation.
- Crisis situations with cross-border effects and stemming from cyber-attacks shall be reported to Europol following the same method as described in chapter 5.2.
- If the crisis entails an important EU external or an EU Common Security and Defence Policy dimension, the European External Action Service shall be promptly informed, enabling them to activate their Crisis Response Mechanism.

[34] The Cyber Crises Liaison Organisation Network (CyCLONe) was established in 2020 to support the implementation of rapid emergency response during larger cross-border cyber incidents or crisis. CyCLONe links cooperation at technical (e.g., CSIRTs) and political levels (e.g., Integrated Political Crisis Response), thus enabling consultations on national response strategies and coordinated impact assessment on the anticipated or observed impacts of a crisis, both at national and EU level.

Box 5: List of deliverables chapter 5	
Deliverable	Responsibility
1. An illustration of the information sharing network by mapping different information sharing initiatives and their connections	ENISA
2. A track record of events such as incidents, crises and vulnerabilities that have been reported in the international information sharing network	CERT-EU, may, with support from ENISA
3. A report on the effectiveness of the Electricity Cybersecurity Early Warning System (ECEWS)	ENISA
4. Criteria to determine if an identified cybersecurity Incident is a Reportable Cyber Security Incident	ENTSO-E and the EU DSO entity
5. Rules for how cross-border cybersecurity crisis shall be managed	ENTSO-E and the EU DSO entity
6. Minimum content of crisis management plans, BCP and recovery plans	ENTSO-E and the EU DSO entity

6 Electricity cybersecurity exercise framework

The network code shall require the establishment of a multi-year programme of electricity cybersecurity exercises. The programme shall affect different levels of the electricity system each year, with the aim of providing all actors involved with the possibility of becoming familiar with these exercises and to contribute to the improvement of the programme and to the preparedness of the entire sector. Furthermore, exercises can assist in the revaluation of the criticality of assets and overall improve the risk management process.

In the context of cybersecurity exercises, the network code shall include the provision to plan and execute the following activities:

1. A mandatory internal cybersecurity exercise for all critical-risk entities, simulating a situation that will impact cross-border electricity flows, at least every three years after the network code enters into force.
2. For each Member State, a national cybersecurity exercise of all national critical-risk entities of the considered Member State, in substitution of point 1. ENISA could provide to NRAs dedicated training on how to plan and organise their own cyber exercises using ENISA's methodology.
3. A mandatory regional or cross-regional cybersecurity exercise. It shall be organised by ENTSO-E in coordination with the EU DSO entity and with the support of one or more RCCs and shall involve all critical-risk entities operating under the same RCC. The cybersecurity exercise shall take place at least every three years after the network code enters into force.

Exercises at point 1, 2 and 3 may include and alternate, to the extent possible, Tabletop Cybersecurity Exercises, Red/Blue team exercises, hybrid threats, etc., including the participation of critical service providers. The cybersecurity exercise organizer at point 1, 2 and 3 shall analyse and finalize the exercise through a lesson learnt report including at least the exercise scenario, meeting reports, main positions and lessons learnt. Lessons learnt shall lead to improvements tasks to correct, adapt, or change cybersecurity crisis processes, associated governance models, and potentially contractual engagements with the third parties. The entities participating in the exercise shall guarantee the implementation of their actions and tasks ahead the exercise.

For the follow-up of the exercises in point 3, the network code will request the ENTSO-E and the EU DSO entity to consult the critical-risk entities and include a periodic analysis of the lessons learned and recommendations in the follow-up activity, indicated in chapter 8.1, and must also be reflected in the Risk Assessment Report, indicated in chapter 8.3.

ENTSO-E and the EU DSO entity, advised by ACER and ENISA, shall prepare on a yearly basis an exercise template for exercises at point 1 and 2, based on major risks that would emerge in the risk assessment exercise. The NRAs and/or the CS-NCAs, shall supervise, when a supervisory role is attributed at Member State level, the execution of cybersecurity exercises at point 1 and 2.

ENTSO-E and the EU DSO entity, advised by ACER, ENISA and by the Joint Research Centre of the European Commission, shall prepare every three years an exercise scenario for the exercises in point 3, based on the indication of the European Commission.

Finally, the network code may lay the foundation for the creation of a shared and distributed electricity cybersecurity simulation testbed to give access to a realistic setup for the cybersecurity exercises. The testbed may be used to better understand, ex-post, the underlying dynamics of cyber incidents and attacks, as well as to assess the actual consequences of specific incidents or attacks on cross-border electricity flows. In this respect, the network code may request all critical-risk / high-risk entities to contribute to the creation of the electricity cybersecurity testbed by sharing the costs in a proportionate manner.

Box 6: List of deliverables chapter 6	
Deliverable	Responsibility
1. A multi-year programme of electricity cybersecurity exercises	ENTSO-E and the EU DSO entity
2. A voluntary cybersecurity simulation testbed	ENTSO-E and the EU DSO entity

7 Protection of information exchanged in the context of this network code

All information exchanged among all stakeholders for the implementation of the network code shall be protected, considering the level of classification of the information applied to the information by the originator. The classification system shall consider the risk of loss, modification, or alteration of essential information to allow cross-border electricity flows.

The protection of information exchanged in the context of this network code shall follow the following principles:

1. Each critical-risk / high-risk entity, when dealing with information internally and when transferring information related, shall assure that all information is properly classified and protected, and classification and classifying entity are correctly indicated.
2. Each stakeholder shall refuse any information without classification or classifying entity and shall inform NRAs/CS-NCAs and ACER in case of any breach of information protection rules.
3. Each originator of information shall set the level of classification and include themselves as classifying entity in compliance with rules at point (1) of the methodology.
4. It is the responsibility of each processor to protect, respect and further disseminate the level of classification.

5. Information shall only be exchanged internally and externally as part of necessary information processing and following the “need to know” principle[35].
6. ENTSO-E and the EU DSO entity are responsible for defining the rules for the classification and protection of information as defined in the scope and objectives in points (1), (2) and (3), after consulting all the critical-risk / high-risk entities as well as all CS-NCAs and NRAs.
7. ACER, advised by ENISA, and after receiving the opinion of the NIS Cooperation Group - WS 8,[36] shall issue an opinion on the rules described in point 6 to the European Commission.
8. The NRAs or CS-NCAs shall be responsible vis-à-vis the entities to whom the network code applies, for monitoring compliance of the rules for protection of information, as well as sanctioning when rules are not respected.
9. The relevant NRAs are responsible for supervising compliance of the RCCs with the information protection regulations.
10. Each stakeholder shall, when exchanging information, always verify that the information transferred includes information on the classification level prior initiating any processing and promptly report to the counterparty when a discrepancy may occur.
11. Each entity may classify the same information at a different level according to national legislation. If the same information is classified at a different level by different entities, the highest classification level shall prevail as the applicable one.

Regarding litigation over classification, or about the refusal to process or exchange information involving entities from the same Member State, the CS-NCAs must decide. In the case of an exchange of information that involves more than one Member State, the concerned NRAs shall decide.

The network code shall also cover the following aspects:

i) The rules for the classification of the information exchanged and for the definition of the classifying entity shall be defined in the context of the network code and may use any other existing EU classification when applicable.
ii) The rules and methods for the secure transfer of information shall be defined in the context of the network code based on the information classification in point (i).
iii) The rules for the secure treatment of the information will be defined in the context of the network code based on the classification of the information in point (i).
iv) The classification shall foresee the indication of the classifying entity.
v) When multiple sets of information are aggregated into a single set, the applicable level of classification is equal to the highest level of information classification among the original sets.

Compatibility with obligations deriving from existing legislation must be ensured. Any provisions of the network code on confidentiality and protection of data shall be without prejudice and in line with

[35] The general security principle under which an information can be provided to any other actor, only if it is a strict requirement for the actors to fulfil its current role.
[36] WS 8 is the work stream of the NIS Cooperation Group for the energy sector which consists of the national authorities which are responsible for the implementation of the NIS Directive requirements for the energy sector.

existing legislation for the protection of commercially sensitive, confidential information and trade secrets, and in particular, consistent with REMIT[37] and GDPR[38] provisions.

Box 7: List of deliverables chapter 7	
Deliverable	Responsibility
1. An information classification system[39]	ENTSO-E and the EU DSO entity

8 Monitoring, benchmarking and reporting

8.1 Monitoring

ACER shall be responsible for carrying out the monitoring activities as described below and shall assess if the network code actively contributes to the strategic objectives set in the "Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade[40]". ACER shall carry out the monitoring activities in cooperation with ENISA and supported by ENTSO-E and the EU DSO entity. The main objectives of the monitoring activities shall be, in particular:

i) periodically verify the status of implementation of the applicable cybersecurity standards, in regard to the high-risk and critical-risk entities, prioritising the monitoring on the high-risk entities and later on critical-risk entities;
ii) verify whether the size cap (at chapter 1.3) does not directly or indirectly cause a systemic cybersecurity risk for cross-border electricity flows and whether it is necessary to introduce additional measures in this respect to prevent risks for the electricity sector.

Monitoring activities shall be able to determine and offer performance indicators that allow assessing operational reliability that can be related to cybersecurity matters. Monitoring activities shall also help identifying areas of improvement for the revisions of the network code, or to determine uncovered areas and new priorities that may emerge due to technological advances.

ACER, in cooperation with ENISA and supported by ENTSO-E and the EU DSO entity, shall define on the information to collect for the purpose of the regular (at least biannually) monitoring of the network code, the methodology and the rules to collect such information.

The information gathering process shall be kept in reasonable and achievable conditions, minimising the efforts of all stakeholders involved and avoiding double notification by the concerned critical-risk / high-risk electricity entities and their associations. ACER, ENTSO-E and the EU DSO entity shall agree on a reasonable time frame to update such information and on common standardised ways of analysing the information. The network code shall allow access to such information also to NRAs and to CS-NCAs.

[37] Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency Text with EEA relevance, OJ L 326, 8.12.2011, p. 1–16
[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88
[39] The information classification system may be based on already established schemes such as the Commission decision 2015/444 on the security rules for protecting EU classified information and the Council decision 2013/488 on the security rules for protecting EU classified information.
[40] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2020:18:FIN

8.2 Benchmarking

The NRAs shall carry out the benchmarking activities described below. ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide and provide target values based on previous reports. Information related to cybersecurity spending shall remain sensitive information and shall be managed jointly and securely by the CS-NRAs and NRAs with national security clearances at the Member State level and ACER and ENISA at the European level. If an NRA has no security clearances at the Member State level, the CS-NCA will grant the NRA relevant access to classify information on a "need to know" basis. These potential situations shall be described in the Risk Assessment Report.

The benchmarking shall assess whether current investments in cybersecurity to protect cross-border electricity flows provide the desired results and do not generate adverse effects on the development of the electricity systems. In addition, it shall assess whether such investments are efficient and integrated into the overall procurement of assets and services. The main objectives of the benchmarking activities in the context of the network code shall verify:

i) the average expenditure in cybersecurity for the protection of electricity cross-border flows, especially in respect to the high-risk entities and to the critical-risk entities;
ii) the average expenditure in cybersecurity hygiene for all the entities which are not critical-risk or high-risk entities;
iii) in coordination with RCCs, the average prices of cybersecurity services, systems and products that mainly contribute to the enhancement and maintenance of the cybersecurity posture in the different system operation geographical areas; it will allow to analyse the existence of similar costs associated with cybersecurity as well as to identify possible measures needed to foster efficiency in spending, particularly where cybersecurity technological investments may be needed;
iv) the level of efficiency of spending on cybersecurity and observe the correlation between the level of spending and the maturity of the sector (prudence of cybersecurity expenditure). To know whether a security measure is cost efficient, the cost of the measure must be compared with the economic impact of a cyber incident in case the measure is not in place. To find the cost of the measure, the price of operating a service without cyber measures and cyberattacks may be compared with the price of operating a service which includes security systems. To enable such a comparison, security costs must be separated from other investment and operations costs.

8.3 Reporting

The main objective of reporting shall be to consolidate knowledge and experiences in the boundaries of the network code, and analyse lessons learned and new trends in cybersecurity that may not directly be included in the network code at the time of the release, but that may need the attention of the policy makers, together with a revision of the network code. In this respect, the "Cross-Border Electricity Cybersecurity Risk Assessment Report" will be crucial for policy makers to identify past behaviours, trends and risks that may emerge, and to identify the need for improvements and changes to the current plans. The network code shall provide for the regular (meaning, at least once every two years) publication of such a report.

The report shall be drafted by ENTSO-E and the EU DSO entity with the contribution of all the entities listed in Table 1 and shall be submitted to the European Commission and to ACER for opinion. In preparing the draft, ENTSO-E and the EU DSO entity shall consult, from an early stage, ENISA, ACER, NRAs and CS-NCAs who may aim to contribute.

The report shall include at least the following information:

- High level asset inventory lists putting emphasis on:
  - Legacy systems still in use and planned to be replaced;
  - Systems that implement the highest level and lowest level of security;
  - Systems that contribute to operating the cross-border electricity flows.
- current threats, with emphasis on emerging threats and risks for the electricity system;
- incidents for the previous period both at EU level and international level, providing a critical overview of how such incidents may have had an impact on electricity cross border flows, if replicated in the EU;
- overall status of implementation of the cybersecurity measures and the regional approaches;
- status of implementation of the critical information flows (at chapter 5);
- identified and highlighted risks that may derive from poor supply chain management;
- results and accumulated experiences from mandatory regional and cross-regional cybersecurity exercises;
- any other information that may be useful to identify a partial failure of the network code or the need for a revision of the network code or any of its tools.

The report shall be subject to the rules on protection of exchange of information (see chapter 7). For this reason, the report may be released in a sanitised public version without those annexes that, for the nature of their confidentiality, may be released on "need-to-know basis". A full and confidential version shall be distributed on "need-to-know basis", only to NISCG members, to ACER, to ENISA and to the European Commission. Before the release of the public sanitised version, the NIS Coordination Group shall provide its approval. ENTSO-E and the EU DSO entity are responsible for the compilation and the release of the report in line with the rules defined above.

Box 8: List of deliverables chapter 8	
Deliverable	Responsibility
1. A monitoring report including performance indicators that allow assessing operational reliability	ACER, in cooperation with ENTSO-E and the EU DSO entity, advised by ENISA
2. A benchmarking guide	ACER, in cooperation with ENISA
3. A benchmarking report	NRAs
4. Cross-Border Electricity Cybersecurity Risk Assessment Report"	ENTSO-E and the EU DSO entity

9 New systems, processes and procedures

The network code shall be elaborated in a way that is not detrimental to innovation. It shall not constitute a barrier to the access of new entities to the electricity markets and the subsequent use of innovative solutions that contribute to the efficiency of the electricity system. As a fundamental principle, all new systems, processes and procedures shall be acquired, designed, configured and maintained embedding principles such as, but not limited to, security in-depth and security by design. Therefore, the network code shall promote the safe digitalisation of the electricity sector, discouraging and penalising any intervention that does not imply due consideration of aspects of security and cybersecurity.