NISTify ENERGY

E-LEARNING COURSE

Detailed presentation of the NCCS regulation

NIS2U GmbH

1.00.3 – 02/17/2025

Contents

Chapter 1

Welcome

Welcome to the Introduction of Network Code on Cybersecurity (NCCS) Regulation Training Material Course

Embark on a journey to master the complexities of NCCS regulations with our expertly crafted training material.

The purpose of the training material is to support the players in the electricity sector in getting acquainted with the detailed provisions of specific articles of the NCCS cybersecurity regulation. The material presents the tasks of the participants article by article, the relationships between certain articles, and the schedule of the most important tasks.

Detailed Provisions: An in-depth look at specific articles within the regulation.

Roles and Responsibilities: What tasks and duties each participant in the electricity sector must perform to ensure compliance.

Interrelationships: How different articles and provisions interconnect and support each other.

Task Scheduling: A timeline for the completion of the most crucial tasks.

Chapter 2

Introduction

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [1] of the European Parliament and of the Council lays down measures for a high common level of cybersecurity across the Union. REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [2] of the European Parliament and of the Council complements DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [3] by ensuring that cybersecurity incidents in the electricity sector are properly identified as a risk and that the measures taken to address them are properly addressed in the risk preparedness plans. REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [4] complements Directive DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [5] and REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [6] by setting out specific rules for the electricity sector at Union level. Furthermore, this Delegated Regulation complements the provisions of DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [7] regarding the electricity sector, whenever cross-border electricity flows are concerned.

Key among the Commission actions is the establishment of a comprehensive legislative framework that builds on the EU Cybersecurity strategy (JOIN/2013/01) [8] the DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [9] the Cybersecurity Package (JOIN/2017/450 final) [10] from September 2017, which also includes the Cybersecurity Act

- NCCS entered into force on June 13, 2024.
- Delegated Act by the European Commission means **directly applicable and legally binding in**

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553779410177&uri=CELEX:52013JC0001
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN

all EU Member States.

- NCCS lays down **sector-specific rules** for **cybersecurity** aspects of cross-border electricity flows.
- NCCS **complements other European cyber security legislations**(DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [11]), whenever cross-border electricity flows are concerned.

The **ENTSO-E** (European Network of Transmission System Operators for Electricity), in collaboration with the **EU DSO** (European Distribution System Operators Organization), has developed a **provisional list of high-impact and critical-impact processes** across the Union.

The provisional list of processes can be accessed via the following links:

> FILE 1
>
> Provisional list of Union-wide high-impact and critical-impact processes (English)
>
> **files/Provisional list of Union-wide high-impact and critical-impact processes.pdf**

The **supporting methodological document** provides additional information and justification for the listed processes.

> FILE 2
>
> Supporting document for the provisional list of Union-wide high-impact and critical-impact processes (English)
>
> **files/Supporting document Provisional list of Union-wide high-impact and critical-impact processes.pdf**

As part of the NCCS, **ENTSO-E**, in collaboration with the **EU DSO**, has developed a **provisional Electricity Cybersecurity Impact Index (ECII) and threshold values for high-impact and critical-impact categories.**

The provisional Electricity Cybersecurity Impact Index (ECII) can be accessed via the following links:

> FILE 3
>
> Provisional Electricity Cybersecurity Impact Index (ECII) (English)

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

files/Provisional ECII.pdf

The **supporting methodological document** provides additional information and justification for the ECII.

FILE 4

Supporting document for the provisional Electricity Cybersecurity Impact Index (ECII) (English)

files/Supporting document provisional ECII.pdf

In the further part of the training material, there will be an opportunity for a comprehensive, paragraph-by-paragraph analysis of the content of the NCCS regulation.

- **Forward and Backward Buttons:** Use the navigation buttons at the bottom of the pages to review the training material step by step.
- **Left-side Table of Contents:** Provides quick access to individual sections and parts.
- **Top menu:** You can return to the homepage from any point in the study material, where you can view the articles of the NCCS regulation in tile view

2.1 Stakeholders

During the processing of the study material, you may encounter several actors involved in the NCCS regulation. It is worth getting to know them before starting the learning process.

2.1.1 A

TERM

Agency for the Cooperation of Energy Regulators (ACER)

The Agency for the Cooperation of Energy Regulators

A specialized agency of the European Union responsible for facilitating the integration and efficient functioning of EU energy markets.

https://www.acer.europa.eu/ [a]

REGULATION (EU) 2019/942 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [b]

[a] https://www.acer.europa.eu/
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942

2.1.2 C

TERM

Computer Security Incident Response Teams (CSIRT)

A dedicated center where a technical team consisting of one or more experts, supported by cybersecurity IT systems, performs security-related tasks (Cybersecurity Operation Center [CSOC] services) such as handling cyber-attacks and security configuration errors, security monitoring, log analysis, and cyber-attack detection.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

TERM

Computer Security Incident Response Teams (CSIRT)

A dedicated center where a technical team consisting of one or more experts, supported by cybersecurity IT systems, performs security-related tasks (Cybersecurity Operation Center [CSOC] services) such as handling cyber-attacks and security configuration errors, security monitoring, log analysis, and cyber-attack detection.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

TERM

Critical-impact entity

Means an entity that carries out a critical-impact process and that is identified by the competent authorities in accordance with Article 24. [a]

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [b]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

TERM

Critical ICT service provider

Means an entity which provides an ICT service, or ICT process that is necessary for a critical-impact or high-impact process affecting cybersecurity aspects of cross-border electricity flows and that, if compromised, may cause a cyber-attack with impact above the critical-impact or high-impact threshold.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

2.1.3 D

TERM

DG CONNECT (Directorate-General for Communications Networks, Content and Technology)

The Directorate-General for Communications Networks, Content and Technology (DG CONNECT) develops and implements the European Commission's policies.

TERM

DG ENER (Directorate-General for Energy)

The Directorate-General for Energy of the European Commission is responsible for the EU's energy policy.

TERM

Distribution System Operator (DSO)

A natural or legal person responsible for operating, maintaining, and, if necessary, developing a distribution system in a given area, as well as for ensuring long-term capacity to meet justified demands for electricity distribution.

DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944

TERM

DSO Entity (EU DSO)

European Distribution System Operators Organization

The European Distribution System Operators Organization was established by the European Union to coordinate and develop electricity distribution system operations. The role of the EU DSO is particularly crucial in the integration of energy markets, the incorporation of renewable energy sources, and supporting the energy transition.

The EU DSO's activities are regulated by the EU Clean Energy Package and the Electricity Market Regulation (Regulation (EU) 2019/943).

https://eudsoentity.eu/ [a]

REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [b]

[a] https://eudsoentity.eu/
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943

2.1.4 E

TERM

European Commission (EC)

The European Commission is the executive branch of the European Union, responsible for implementing EU legislation, developing policies, and managing the budget.

TERM

Electricity Coordination Group (ECG)

Electricity Coordination Group

The goal of the Electricity Coordination Group is to share and coordinate information on electricity policy measures with cross-border impacts, facilitating cooperation through knowledge and experience exchange.

COMMISSION DECISION 2012/C 353/02 [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D1117(01)

TERM

European Union Agency for Cybersecurity (ENISA)

ENISA is the EU's cybersecurity agency, supporting Member States in defending against cyber threats.

TERM

European Network of Transmission System Operators for Electricity (ENTSO-E)

European Network of Transmission System Operators for Electricity

ENTSO-E is the common organization of European transmission system operators (TSOs). It plays a central role in the integration of the European electricity market and ensuring the stability of the electricity system. ENTSO-E's activities are regulated by the EU Clean Energy Package and the Electricity Market Regulation (Regulation (EU) 2019/943).

https://www.entsoe.eu/ [a]

REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [b]

[a] https://www.entsoe.eu/

[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943

2.1.5 H

TERM

High-impact entity

Means an entity that carries out a high-impact process and that is identified by the competent authorities in accordance with Article 24. [a]

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [b]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_19
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

2.1.6 M

TERM

Member state

Means a country that is a member of the European Union and complies with EU legislation.

2.1.7 N

TERM

National Competent Authority (NCA)

A national competent authority is an official body or organization authorized by legislation to regulate, supervise, and oversee a specific sector or area. These authorities ensure compliance with national and, where relevant, international laws and standards.

TERM

National Cybersecurity Competent Authorities (CS NCA)

The national competent authority responsible for cybersecurity within a given Member State.

TERM

National Regulatory Authority (NRA)

An official state or independent organization responsible for regulating, supervising, and overseeing designated areas within a country or region.

TERM

Network and Information Systems Cooperation Group (NIS CG)

Cybersecurity Cooperation Group

The Network and Information Security Cooperation Group (NIS CG) coordinates EU cyber-security cooperation. The tasks of the NIS Cooperation Group are outlined in Article 11 of the NIS Directive.

COMMISSION IMPLEMENTING DECISION (EU) 2017/179 [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017D0179

TERM

Nominated Electricity Market Operator (NEMO)

A Nominated Electricity Market Operator (NEMO) is a market operator designated by the competent authority of an EU Member State to participate in the operation of the Single Day-Ahead Market Coupling or the Single Intraday Market Coupling.

2.1.8 R

TERM

Regional Coordination Center (RCC)

Regional Coordination Centers (RCC)

These centers have a consultative role in the development of regional cybersecurity risk assessment and risk mitigation plans, coordinating Member States' cooperation in cybersecurity.

Established under Article 35 of Regulation (EU) 2019/943.

REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943

TERM

Risk Preparedness National Competent Authority (RP-NCA)

The RP-NCAs are responsible for developing and implementing risk preparedness plans.

2.1.9 S

TERM

System Operators

As defined in Article 2(29) and Article 2(35) of Directive (EU) 2019/944.

DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944

2.1.10 T

TERM

Transmission System Operator (TSO)

A natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity.

DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944

NOTE

TERM

Article 2

This Regulation applies to cybersecurity aspects of cross-border electricity flows in the activities of the following entities, if they are identified as high-impact or critical-impact entities in accordance with Article 24 [a]:

a. electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944; [b]

b. nominated electricity market operators ('NEMOs') as defined in Article 2(8) of Regulation (EU) 2019/943; [c]

c. organised market places or 'organised markets' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014 [d] (14) that arrange transactions on products relevant to cross-border electricity flows;

d. critical ICT service providers as referred to in Article 3, point (9) of this Regulation [e]

e. the ENTSO for Electricity established pursuant to Article 28 of Regulation (EU) 2019/943 [f]

f. the EU DSO entity established pursuant to Article 52 of Regulation (EU) 2019/943; [g]

g. balancing responsible parties as defined in Article 2, point (14) of Regulation (EU) 2019/943; [h]

h. operators of recharging points as defined in Annex I to Directive (EU) 2022/2555; [i]

i. regional coordination centres ('RCCs') as established pursuant to Article 35 of Regulation (EU) 2019/943; [j]

j. managed security service providers ('MSSP') as defined in Article 6(40) of Directive (EU) 2022/2555; [k]

k. any other entity or third party to whom responsibilities have been delegated or assigned pursuant to this Regulation. [l]

    1. The following authorities are, as part of their current mandates, responsible to perform tasks assigned in this Regulation [m]:

l. the European Union Agency for the Cooperation of Energy Regulators ('ACER') established by Regulation (EU) 2019/942 of the European Parliament and of the Council [n]

m. national competent authorities responsible for carrying out the tasks assigned to them under this Regulation [o] and designated by Member States pursuant to Article 4, or 'competent authority';

n. national regulatory authorities ('NRAs') designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944; [p]

o. competent authorities for risk preparedness ('RP-NCAs') established pursuant to Article 3 of Regulation (EU) 2019/941; [q]

p. computer security incident response teams ('CSIRTs') as designated or established pursuant to Article 10 of Directive (EU) 2022/2555; [r]

q. competent authorities responsible for cybersecurity ('CS-NCAs') as designated or established pursuant to Article 8 of Directive (EU) 2022/2555; [s]

r. the European Union Agency for Cybersecurity established pursuant to Regulation (EU) 2019/881; [t]

TERM

Article 4(3)

This Regulation shall also apply to all entities who are not established in the Union but who deliver services to entities in the Union, provided they have been identified as high or critical-impact entities by the competent authorities in accordance with https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885 [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

TERM

Article 2(1)

This Regulation applies to cybersecurity aspects of cross-border electricity flows in the activities of the following entities, if they are identified as high-impact or critical-impact entities in accordance with Article 24 [a]:

a. electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944; [b]
b. nominated electricity market operators ('NEMOs') as defined in Article 2(8) of Regulation (EU) 2019/943; [c]
c. organised market places or 'organised markets' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014 [d] (14) that arrange transactions on products relevant to cross-border electricity flows;
d. critical ICT service providers as referred to in Article 3, point (9) of this Regulation [e]
e. the ENTSO for Electricity established pursuant to Article 28 of Regulation (EU) 2019/943 [f]
f. the EU DSO entity established pursuant to Article 52 of Regulation (EU) 2019/943; [g]
g. balancing responsible parties as defined in Article 2, point (14) of Regulation (EU) 2019/943; [h]
h. operators of recharging points as defined in Annex I to Directive (EU) 2022/2555; [i]
i. regional coordination centres ('RCCs') as established pursuant to Article 35 of Regulation (EU) 2019/943; [j]
j. managed security service providers ('MSSP') as defined in Article 6(40) of Directive (EU) 2022/2555; [k]
k. any other entity or third party to whom responsibilities have been delegated or assigned pursuant to this Regulation. [l]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[c] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[d] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R1348
[e] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%253A32024R1366
[f] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[g] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[h] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[i] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art
[j] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[k] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[l] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

TERM

Article 2(2)

1. The following authorities are, as part of their current mandates, responsible to perform tasks assigned in this Regulation [a]:

   a. the European Union Agency for the Cooperation of Energy Regulators ('ACER') established by Regulation (EU) 2019/942 of the European Parliament and of the Council [b]

   b. national competent authorities responsible for carrying out the tasks assigned to them under this Regulation [c] and designated by Member States pursuant to Article 4, or 'competent authority';

   c. national regulatory authorities ('NRAs') designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944; [d]

   d. competent authorities for risk preparedness ('RP-NCAs') established pursuant to Article 3 of Regulation (EU) 2019/941; [e]

   e. computer security incident response teams ('CSIRTs') as designated or established pursuant to Article 10 of Directive (EU) 2022/2555; [f]

   f. competent authorities responsible for cybersecurity ('CS-NCAs') as designated or established pursuant to Article 8 of Directive (EU) 2022/2555; [g]

   g. the European Union Agency for Cybersecurity established pursuant to Regulation (EU) 2019/881; [h]

   h. any other authorities or third party to whom responsibilities have been delegated or assigned pursuant to Article 4(3). [i]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942
[c] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[d] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[e] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[f] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[g] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[h] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[i] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

TERM

Article 4(1)

As soon as possible and in any event by 13 December 2024, each Member State shall designate a national governmental or regulatory authority responsible for carrying out the tasks assigned to it in this Regulation ('competent authority'). Until the competent authority has been assigned with carrying out the tasks under this Regulation, the regulatory authority designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944 [a] shall carry out the tasks of the competent authority in accordance with this Regulation.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02019L0944-20240716#art_57

TERM

Article 4(2)

Member States shall, without delay, notify the Commission, ACER, ENISA, the NIS Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 [a] and the Electricity Coordination Group set up under Article 1 of Commission Decision of 15 November 2012 [b] and communicate to them the name and the contact details of their competent authority designated pursuant to paragraph 1 of this article and any subsequent changes thereto.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_14
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D1117(01)

TERM

Article 4(3)

Member States may allow their competent authority to delegate tasks assigned to it in this Regulation to other national authorities with the exception of the tasks listed in Article 5. Each competent authority shall monitor the application of this Regulation by the authorities to whom it has delegated tasks.

The competent authority shall communicate the name, contact details, assigned tasks and any subsequent changes thereto of the authorities to whom a task has been delegated to the Commission, to ACER, to the Electricity Coordination Group, to ENISA and to the NIS Cooperation Group.

TERM

Article 5

The competent authorities shall coordinate and ensure appropriate cooperation between the competent authorities responsible for cybersecurity, the cyber crisis management authorities, the NRAs, competent authorities for risk preparedness and CSIRTs for the purpose of the fulfilment of the relevant obligations laid down in this Regulation. The competent authorities shall also coordinate with any other bodies or authorities as determined by each Member State, to ensure efficient procedures and avoid duplications of tasks and obligations. The competent authorities shall be able to instruct the respective NRAs to request ACER for an opinion pursuant to Article 8(3).

TERM

Article 6(1)

TSOs shall develop, in cooperation with the EU DSO entity, proposals for the terms and conditions or methodologies pursuant to paragraph 2, or for plans pursuant to paragraph 3.

TERM

Article 6(2)

The following terms and conditions or methodologies and any amendments thereof shall be subject to approval by all competent authorities:

a. the cybersecurity risk assessment methodologies pursuant to Article 18(1);

b. the comprehensive cross-border electricity cybersecurity risk assessment report pursuant to Article 23;

c. the minimum and advanced cybersecurity controls pursuant to Article 29, the mapping of electricity cybersecurity controls against standards pursuant to Article 34, including minimum and advanced cybersecurity controls in the supply chain in accordance with Article 33;

d. a cybersecurity procurement recommendation pursuant to Article 35;

e. the cyber-attacks classification scale methodology pursuant to Article 37(8).

TERM

Article 6(3)

The proposals for the regional cybersecurity risk mitigation plans pursuant to Article 22 shall be subject to approval by all competent authorities of the concerned system operation region.

TERM

Article 6(4)

The proposals for terms and conditions, methodologies listed in paragraph 2, or for plans listed in paragraph 3, shall include a proposed timescale for their implementation and a description of their expected impact on the objectives of this Regulation.

TERM

Article 6(5)

The EU DSO entity may provide a reasoned opinion to the concerned TSOs until 3 weeks before the deadline to submit the proposal for terms and conditions or methodologies or plans to the competent authorities.

TSOs responsible for the proposal for terms and conditions or methodologies or plans shall take into consideration the reasoned opinion of the EU DSO entity prior to its submission for competent authorities' approval. TSOs shall provide reasoning where the EU DSO entity opinion is not taken into account.

TERM

Article 6(6)

When jointly developing terms, conditions and methodologies and plans, the participating TSOs shall closely cooperate. TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall regularly inform competent authorities and ACER about the progress of developing the terms and conditions or methodologies, or plans.

TERM

Article 7(1)

Where TSOs deciding on proposals for terms and conditions or methodologies are not able to reach an agreement, they shall decide by qualified majority voting. A qualified majority for such proposals shall be calculated as follows:

a. TSOs representing at least 55 % of the Member States; and

b. TSOs representing Member States comprising at least 65 % of the population of the Union.

TERM

Article 7(2)

A blocking minority for decisions on proposals for terms and conditions or methodologies listed in Article 6(2) shall include TSOs representing at least four Member States, failing of which the qualified majority shall be deemed attained.

TERM

Article 7(3)

Where TSOs of a system operation region deciding on proposals for plans listed in Article 6(2) are not able to reach an agreement, and where the system operation region concerned is composed of more than five Member States, TSOs shall decide by qualified majority voting. A qualified majority for proposals listed in Article 6(2) shall require the following majority:

a. TSOs representing at least 72 % of the Member States concerned; and

b. TSOs representing Member States comprising at least 65 % of the population of the concerned area.

TERM

Article 7(4)

A blocking minority for decisions on proposals for the plans shall include at least a minimum number of TSOs representing more than 35 % of the population of the participating Member States, plus TSOs representing at least one additional Member State concerned, failing of which the qualified majority shall be deemed attained.

TERM

Article 7(5)

For TSO decisions on proposals for terms and conditions or methodologies pursuant to Article 6(2), one vote shall be attributed per Member State. If there is more than one TSO in the territory of a Member State, the Member State shall allocate the voting powers among the TSOs.

TERM

Article 7(6)

If TSOs, in cooperation with the EU DSO entity, fail to submit an initial or amended proposal for terms and conditions or methodologies, or for plans, to the relevant competent authorities within the deadlines set out in this Regulation, they shall provide the relevant competent authorities and ACER with the relevant drafts of the terms and conditions or methodologies, or of the plans. They shall explain what has prevented an agreement. The competent authorities shall jointly take the appropriate steps for the adoption of the required terms and conditions or methodologies, or of the required plans. This may be done for instance by requesting amendments to the drafts pursuant to this paragraph, by revising and completing those drafts, or, where no drafts have been provided, by defining and approving the required terms and conditions or methodologies or plans.

TERM

Article 8(1)

TSOs shall submit the proposals for terms and conditions or methodologies, or for plans for approval to the relevant competent authorities within the respective deadlines set out in Articles 18, 23, 29, 33, 34, 35 and 37.

The competent authorities may jointly prolong these deadlines in exceptional circumstances, notably in cases where a deadline cannot be met due to circumstances external to the sphere of TSOs or of the EU DSO entity.

TERM

Article 8(2)

Proposals for terms and conditions, methodologies or for plans pursuant to paragraph 1, shall be submitted for information to ACER at the same time that they are submitted to the competent authorities.

TERM

Article 8(3)

Upon a joint request of the NRAs, ACER shall issue an opinion on the proposal for terms and conditions or methodologies, or for the plans, within six months of the receipt of the proposals for terms and conditions or methodologies, or for plans and notify NRAs and competent authorities of the opinion.

NRAs, CS-NCAs and any other authorities designated as competent authorities shall coordinate with each other before the NRAs requests an opinion to ACER.

ACER may include recommendations in such opinion. ACER shall consult ENISA before issuing an opinion on the proposals listed in Article 6(2).

TERM

Article 8(4)

The competent authorities shall consult and closely cooperate and coordinate with each other in order to reach an agreement on the proposed terms and conditions, methodologies, or plans. Before approving the terms and conditions or methodologies, or the plans, they shall revise and complete the proposals where necessary, after consulting the ENTSO for Electricity and the EU DSO entity, in order to ensure that the proposals are in line with this Regulation and contribute to a high common level of cybersecurity across the Union.

TERM

Article 8(5)

The competent authorities shall decide on the terms and conditions or methodologies or on the plans within six months following the receipt of the terms and conditions or methodologies or of the plans by the relevant competent authority or, where applicable, by the last relevant competent authority concerned.

TERM

Article 8(6)

Where ACER issues an opinion, the relevant competent authorities shall take that opinion into account and shall take their decisions within six months from the receipt of ACER's opinion.

TERM

Article 8(7)

Where the competent authorities jointly require an amendment to the proposed terms and conditions or methodologies, or the plans, in order to approve them, the TSOs shall develop, in cooperation with the EU DSO entity, a proposal for such amendment to the terms and conditions or methodologies, or the plans. The TSOs shall submit the amended proposal for approval within two months following the request of the competent authorities.

The competent authorities shall decide on the amended terms and conditions or methodologies, or plans, within two months following their submission.

TERM

Article 8(8)

Where the competent authorities have not been able to reach an agreement within the period referred to in paragraph 5 or 7, they shall inform the Commission. The Commission may take appropriate steps to make possible the adoption of the required terms and conditions or methodologies, or plans.

TERM

Article 8(9)

TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO entity shall publish the terms and conditions or methodologies, or the plans, on their websites following approval by the relevant competent authorities, except where such information is considered as confidential in accordance with Article 47.

TERM

Article 8(10)

The competent authorities may jointly request proposals for amendments of the approved terms and conditions or methodologies, or of the approved plans, from TSOs and the EU DSO entity and determine a deadline for the submission of those proposals.

TSOs, in cooperation with the EU DSO entity, may propose amendments to the competent authorities also on its own initiative. The proposals for amendment to the terms and conditions or methodologies, or for the amendments to the plans, shall be developed and approved in accordance with the procedure set out in this Article.

TERM

Article 8(11)

At least every three years after the first adoption of the respective terms and conditions or methodologies, or the respective adopted plans, TSOs in cooperation with the EU DSO entity, shall review the effectiveness of the adopted terms and conditions or methodologies, or the adopted plans, and shall report the findings of the review to the competent authorities and ACER without undue delay.

TERM

Article 9(1)

TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall consult stakeholders, including ACER, ENISA and the competent authority of each Member State, on the draft proposals for terms and conditions or methodologies listed in Article 6(2) and for plans referred to in Article 6(3). The consultation shall last for a period of not less than one month.

TERM

Article 9(2)

The proposals for terms and conditions or methodologies listed in Article 6(2) submitted by the TSOs, in cooperation with the EU DSO entity, shall be published and submitted to consultation at Union level. The proposals for plans listed in Article 6(3) submitted by the relevant TSOs, in cooperation with the EU DSO entity, at regional level shall be submitted to consultation at least at regional level.

TERM

Article 9(3)

TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO Entity responsible for the proposal for terms and conditions or methodologies or plans shall duly take into account the views of stakeholders resulting from the consultations undertaken in accordance with paragraph 1, prior to its submission for regulatory approval. In all cases, a sound justification for including or not including the views resulting from the consultation shall be provided together with the submission and published in a timely manner before or simultaneously with the proposal for terms and conditions or methodologies.

TERM

Article 10

ACER, in close cooperation with ENTSO for Electricity and the EU DSO entity, shall organise stakeholder involvement, including regular meetings with stakeholders to identify problems and propose improvements related to the implementation of this Regulation.

TERM

Article 11(1)

The costs borne by TSOs and DSOs subject to network tariff regulation and stemming from the obligations laid down in this Regulation, including the costs borne by the ENTSO for Electricity and the EU DSO entity, shall be assessed by the relevant NRA of each Member State.

TERM

Article 11(2)

Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms, as determined by the relevant NRA.

TERM

Article 11(3)

If requested by the relevant NRAs, TSOs and DSOs referred to in paragraph 1 shall, within a reasonable period determined by the NRA, provide the information necessary to facilitate the assessment of the costs incurred.

TERM

Article 12(1)

ACER shall monitor the implementation of this Regulation in accordance with Article 32(1) of Regulation (EU) 2019/943 [a] and Article 4(2) of Regulation (EU) 2019/942 [b]. In carrying out this monitoring, ACER may cooperate with ENISA and request support from the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group and the NIS Cooperation Group on the implementation of this Regulation.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943&qid=1733993709560#d1e3462-54-1

[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942#d1e519-22-1

TERM

Article 12(2)

ACER shall publish a report at least every three years after the entry into force of this Regulation to:

a. review the status of implementation of the applicable cybersecurity risk management measures with regard to the high-impact and critical-impact entities;

b. identify whether additional rules on common requirements, planning, monitoring, reporting and crisis management may be necessary to prevent risks for the electricity sector; and

c. identify areas of improvement for the revision of this Regulation, or determine uncovered areas and new priorities that may emerge due to technological developments.

TERM

Article 12(3)

By 13 June 2025, ACER, in cooperation with ENISA and after consultation of the ENTSO for Electricity and the EU DSO entity, may issue guidance on the relevant information to be communicated to ACER for the monitoring purposes as well as the process and frequency for the collection, based on the performance indicators defined in accordance with paragraph 5.

TERM

Article 12(4)

The competent authorities may have access to the relevant information held by ACER, which it has collected in accordance with this Article.

TERM

Article 12(5)

ACER in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity, shall issue non-binding performance indicators for the assessment of operational reliability that are related to cybersecurity aspects of cross-border electricity flows.

TERM

Chapter 3

Article 1: Subject matter

This Regulation establishes a network code which lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

Chapter 4

Article 2: Scope

1. This Regulation applies to cybersecurity aspects of cross-border electricity flows in the activities of the following entities, if they are identified as high-impact or critical-impact entities in accordance with Article 24 [1]:

   a. electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944; [2]
   b. nominated electricity market operators ('NEMOs') as defined in Article 2(8) of Regulation (EU) 2019/943; [3]
   c. organised market places or 'organised markets' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014 [4] (14) that arrange transactions on products relevant to cross-border electricity flows;
   d. critical ICT service providers as referred to in Article 3, point (9) of this Regulation [5]
   e. the ENTSO for Electricity established pursuant to Article 28 of Regulation (EU) 2019/943 [6]
   f. the EU DSO entity established pursuant to Article 52 of Regulation (EU) 2019/943; [7]
   g. balancing responsible parties as defined in Article 2, point (14) of Regulation (EU) 2019/943; [8]
   h. operators of recharging points as defined in Annex I to Directive (EU) 2022/2555; [9]
   i. regional coordination centres ('RCCs') as established pursuant to Article 35 of Regulation (EU) 2019/943; [10]
   j. managed security service providers ('MSSP') as defined in Article 6(40) of Directive (EU) 2022/2555; [11]

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R1348
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%253A32024R1366
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

k. any other entity or third party to whom responsibilities have been delegated or assigned pursuant to this Regulation. [12]

2. The following authorities are, as part of their current mandates, responsible to perform tasks assigned in this Regulation [13]:

   a. the European Union Agency for the Cooperation of Energy Regulators ('ACER') established by Regulation (EU) 2019/942 of the European Parliament and of the Council [14]
   b. national competent authorities responsible for carrying out the tasks assigned to them under this Regulation [15] and designated by Member States pursuant to Article 4, or 'competent authority';
   c. national regulatory authorities ('NRAs') designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944; [16]
   d. competent authorities for risk preparedness ('RP-NCAs') established pursuant to Article 3 of Regulation (EU) 2019/941; [17]
   e. computer security incident response teams ('CSIRTs') as designated or established pursuant to Article 10 of Directive (EU) 2022/2555; [18]
   f. competent authorities responsible for cybersecurity ('CS-NCAs') as designated or established pursuant to Article 8 of Directive (EU) 2022/2555; [19]
   g. the European Union Agency for Cybersecurity established pursuant to Regulation (EU) 2019/881; [20]
   h. any other authorities or third party to whom responsibilities have been delegated or assigned pursuant to Article 4(3). [21]

3. This Regulation shall also apply to all entities who are not established in the Union but who deliver services to entities in the Union, provided they have been identified as high or critical-impact entities by the competent authorities in accordance with Article 24(2). [22]

4. This Regulation is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

5. This Regulation is without prejudice to the Member States' responsibility for safeguarding national security with respect to activities in the production of electricity from nuclear powers plants, including activities within the nuclear value chain, in accordance with the Treaties.

6. Entities, the competent authorities, the single points of contact at entity level and the CSIRTs shall process personal data to the extent necessary for the purposes of this Regulation and in accordance with Regulation (EU) 2016/679 [23] in particular such processing shall rely on Article 6 thereof.

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Chapter 5

Article 3: Definitions

The following definitions apply:

1. ‘asset’ means any information, software or hardware in the network and information systems either tangible or intangible, that has value to an individual, an organisation or a government;
2. ‘competent authority for risk preparedness’ means the competent authority designated pursuant to Article 3 of Regulation (EU) 2019/941; [1]
3. computer security incident response team’ means a team responsible for risk and incident handling in accordance with Article 10 of Directive (EU) 2022/2555; [2]
4. ‘critical-impact asset’ means an asset that is necessary to carry out a critical-impact process;
5. ‘critical-impact entity’ means an entity that carries out a critical-impact process and that is identified by the competent authorities in accordance with Article 24; [3]
6. ‘critical-impact perimeter’ means a perimeter defined by an entity referred to in Article 2(1) [4] that contains all critical-impact assets and on which access to these assets can be controlled and that defines the scope where the advanced cybersecurity controls apply;
7. ‘critical-impact process’ means a business process carried out by an entity for which the electricity cybersecurity impact indices are above the critical-impact threshold;
8. ‘critical-impact threshold’ means the values of the electricity cybersecurity impact indices referred to in Article 19(3)b [5] above which a cyber-attack on a business process will cause critical disruption of cross-border electricity flows;
9. ‘critical ICT service provider’ means an entity which provides an ICT service, or ICT process that is necessary for a critical-impact or high-impact process affecting cybersecurity aspects

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

of cross-border electricity flows and that, if compromised, may cause a cyber-attack with impact above the critical-impact or high-impact threshold;

10. 'cross-border electricity flow' means a cross-border flow as defined in Article 2(3) of Regulation (EU) 2019/943; [6]

11. 'cyber-attack' means an incident as defined in Article 3, point (14), of Regulation (EU) 2022/2554; [7]

12. 'cybersecurity' means cybersecurity as defined in Article 2, point (1) of Regulation (EU) 2019/881; [8]

13. 'cybersecurity control' means the actions or procedures carried out with the purpose of avoiding, detecting, counteracting, or minimising cybersecurity risks;

14. 'cybersecurity incident' means an incident as defined in Article 6 [9] point (6) of Directive (EU) 2022/2555;

15. 'cybersecurity management system' means the policies, procedures, guidelines, and associated resources and activities, collectively managed by an entity, in the pursuit of protecting its information assets from cyber threats systematically establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's network and information system security;

16. 'cybersecurity operation centre' means a dedicated centre where a technical team consisting of one or more experts, supported by cybersecurity IT systems, performs security-related tasks (Cybersecurity operation center ('CSOC') services) such as handling of cyber-attacks and security configuration errors, security monitoring, log analysis, and cyber-attack detection;

17. 'cyber threat' means a cyber threat as defined in Article 2, point (8) of Regulation (EU) 2019/881; [10]

18. 'cybersecurity vulnerability management' means the practice of identifying and addressing vulnerabilities;

19. 'entity' means entity as defined in Article 6, point (38) of Directive (EU) 2022/2555; [11]

20. 'early alert' means the information necessary to indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

21. 'electricity cybersecurity impact index' ('ECII') means an index or classification scale that ranks possible consequences of cyber-attacks to business processes involved in cross-border electricity flows;

22. 'European cybersecurity certification scheme' means a scheme as defined in Article 2, point (9) of Regulation (EU) 2019/881; [12]

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881

23. ‘high-impact entity’ means an entity that carries out a high-impact process and that is identified by the competent authorities in accordance with Article 24; [13]

24. ‘high-impact process’ means any business process carried out by an entity for which the electricity cybersecurity impact indices are above the high-impact threshold;

25. ‘high-impact asset’ means an asset that is necessary to carry out a high-impact process;

26. ‘high-impact threshold’ means the values of the electricity cybersecurity impact indices referred to in Article 19(3)b, [14] above which a successful cyber-attack on a process will cause high disruption of cross-border electricity flows;

27. ‘high-impact perimeter’ means a perimeter defined by any entity listed in Article 2(1) [15] that contains all high-impact assets and on which access to these assets can be controlled and that defines the scope where the minimum cybersecurity controls apply;

28. ICT product’ means an ICT product as defined in Article 2, point (12) of Regulation (EU) 2019/881; [16]

29. ‘ICT service’ means an ICT service as defined in Article 2, point (13) of Regulation (EU) 2019/881; [17]

30. ‘ICT process’ means an ICT process as defined in Article 2, point (13) of Regulation (EU) 2019/881; [18]

31. ‘legacy system’ means a legacy ICT system as defined in Article 3(3) of Regulation (EU) 2022/2554; [19]

32. ‘national single point of contact’ means the single point of contact designated or established by each Member State pursuant to Article 8(3) of Directive (EU) 2022/2555; [20]

33. ‘NIS cyber crisis management authorities’ means the authorities designated or established pursuant to Article 9, point (1) of Directive (EU) 2022/2555; [21]

34. ‘originator’ means an entity that initiates an information exchange, information sharing or information storage event;

35. ‘procurement specifications’ means the specifications that entities define for the procurement of new or updated ICT products, ICT processes or ICT services;

36. ‘representative’ means a natural or legal person established in the Union who is explicitly designated to act on behalf of a high or critical-impact entity not established in the Union but delivering services to entities in the Union and who may be addressed by a competent authority or a CSIRT in the place of the high or critical-impact entity itself with regard to the obligations of that entity under this Regulation;

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

37. ‘risk’ means risk as defined in az Article 6, point (9) of Directive (EU) 2022/2555; [22]

38. ‘risk impact matrix’ means a matrix used during risk assessment to determine the resulting risk impact level for each risk assessed;

39. ‘simultaneous electricity crisis’ means an electricity crisis as defined inhttps://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941[Article 2, point (10) of Regulation (EU) 2019/941;]

40. ‘single point of contact at entity level’ means single point of contact at entity level as designated under Article 38(1) point (c); [23]

41. ‘stakeholder’ is any party that has an interest in the success and ongoing operation of an organisation or process such as employees, directors, shareholders, regulators, associations, suppliers and customers;

42. ‘standard’ means a standard as defined in Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council (16); [24]

43. ‘system operation region’ means the system operation regions as defined in Annex I to ACER Decision 05-2022 on the Definition of System Operation Regions [25], established in accordance with Article 36 of Regulation (EU) 2019/943;

44. ‘system operators’ means ‘distribution system operator’ (DSO) and ‘transmission system operator’ (TSO) as defined in Articles 2(29) and 2(35) of Directive (EU) 2019/944; [26]

45. ‘Union-wide critical-impact process’ means any electricity sector process, possibly involving multiple entities, for which the possible impact of a cyber-attack may be deemed critical during the performance of the Union-wide cybersecurity risk assessment;

46. ‘Union-wide high-impact process’ means any electricity sector process, possibly involving multiple entities, for which the possible impact of a cyber-attack may be deemed high during the performance of the Union-wide cybersecurity risk assessment;

47. ‘unpatched actively exploited vulnerability’ means a vulnerability, which has not yet been publicly disclosed and patched and for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner;

48. ‘vulnerability’ means a vulnerability as defined in Article 6, point (15) of Directive (EU) 2022/2555. [27]

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[24] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

Chapter 6

Article 4: Competent authority

6.1 Paragraph 1

As soon as possible and in any event by 13 December 2024, each Member State shall designate a national governmental or regulatory authority responsible for carrying out the tasks assigned to it in this Regulation ('competent authority'). Until the competent authority has been assigned with carrying out the tasks under this Regulation, the regulatory authority designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944 [a] shall carry out the tasks of the competent authority in accordance with this Regulation.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02019L0944-20240716#art_57

Output

- Assigned authorithy

GOOD TO KNOW

Timing

As soon as possible and in any event by 13 December 2024

Accountable: MS

Involved Stakeholders

Responsible: MS

6.2 Paragraph 2

Member States shall, without delay, notify the Commission, ACER, ENISA, the NIS Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 [a] and the Electricity Coordination Group set up under Article 1 of Commission Decision of 15 November 2012 [b] and communicate to them the name and the contact details of their competent authority designated pursuant to paragraph 1 of this article and any subsequent changes thereto.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_14
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D1117(01)

Relevant NCCS Articles

- Article 4(1)

Output

- Notification

GOOD TO KNOW

Timing

Without delay

Accountable: MS

Involved Stakeholders

Responsible: MS

Informed: EC, ACER, ENISA, NIS CG, ECG

6.3 Paragraph 3 (/1)

Member States may allow their competent authority to delegate tasks assigned to it in this Regulation to other national authorities with the exception of the tasks listed in Article 5. Each competent authority shall monitor the application of this Regulation by the authorities to whom it has delegated tasks.

Relevant NCCS Articles

- Article 5

Output

- Delegation

Accountable: MS

Involved Stakeholders

Responsible: MS, NCA

6.4 Paragraph 3 (/2)

The competent authority shall communicate the name, contact details, assigned tasks and any subsequent changes thereto of the authorities to whom a task has been delegated to the Commission, to ACER, to the Electricity Coordination Group, to ENISA and to the NIS Cooperation Group.

Other NCCS Articles

- Article 5

Input

- Delegation

Output

- Delegation details

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: EC, ACER, ENISA, NIS CG, ECG

Chapter 7

Article 5: Cooperation between relevant authorities and bodies at national level

The competent authorities shall coordinate and ensure appropriate cooperation between the competent authorities responsible for cybersecurity, the cyber crisis management authorities, the NRAs, competent authorities for risk preparedness and CSIRTs for the purpose of the fulfilment of the relevant obligations laid down in this Regulation. The competent authorities shall also coordinate with any other bodies or authorities as determined by each Member State, to ensure efficient procedures and avoid duplications of tasks and obligations. The competent authorities shall be able to instruct the respective NRAs to request ACER for an opinion pursuant to Article 8(3).

Relevant NCCS Articles

- Article 8(3)

Other NCCS Articles

- Article 4(3)

Accountable: NCA

Involved Stakeholders

Responsible: ACER, NCA, NRA, RP NCA, CSIRT, CS NCA

Chapter 8

Article 6: Terms and conditions or methodologies or plans

8.1 Paragraph 1

TSOs shall develop, in cooperation with the EU DSO entity, proposals for the terms and conditions or methodologies pursuant to paragraph 2, or for plans pursuant to paragraph 3.

Relevant NCCS Articles

- Article 6(2)
- Article 6(3)

Output

- Risk assesment methodologies (draft)

- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Regional risk mitigation plan (draft)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: ACER, NCA

8.2 Paragraph 2

The following terms and conditions or methodologies and any amendments thereof shall be subject to approval by all competent authorities:

a. the cybersecurity risk assessment methodologies pursuant to Article 18(1);

b. the comprehensive cross-border electricity cybersecurity risk assessment report pursuant to Article 23;

c. the minimum and advanced cybersecurity controls pursuant to Article 29, the mapping

of electricity cybersecurity controls against standards pursuant to Article 34, including minimum and advanced cybersecurity controls in the supply chain in accordance with Article 33;

d. a cybersecurity procurement recommendation pursuant to Article 35;

e. the cyber-attacks classification scale methodology pursuant to Article 37(8).

Relevant NCCS Articles

- Article 18(1)
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)

Other NCCS Articles

- Article 8
- Article 23

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Output

- Risk assesment methodologies (approved)
- Comprehensive risk assesment report (approved)
- Minimum cyber security controls (approved)
- Advanced cyber security controls (approved)
- Minimum cyber security controlls in supply chain (approved)
- Advanced cyber security controlls in supply chain (approved)
- Mapping matrix (approved)
- Procurement recommandations (approved)
- Cyber-attack classification scale methodology (approved)

Accountable: NCA

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO, NCA

8.3 Paragraph 3

The proposals for the regional cybersecurity risk mitigation plans pursuant to Article 22 shall be subject to approval by all competent authorities of the concerned system operation region.

Relevant NCCS Articles

- Article 22

Input

- Regional risk mitigation plan (draft)

Output

- Regional risk mitigation plan (approved)

Accountable: NCA

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO, NCA

Consulted: NIS CG, RCC

8.4 Paragraph 4

The proposals for terms and conditions, methodologies listed in paragraph 2, or for plans listed in paragraph 3, shall include a proposed timescale for their implementation and a description of their expected impact on the objectives of this Regulation.

Relevant NCCS Articles

- Article 6(2)
- Article 6(3)

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)

- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Regional risk mitigation plan (draft)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: ACER, NCA

8.5 Paragraph 5 (/1)

The EU DSO entity may provide a reasoned opinion to the concerned TSOs until 3 weeks before the deadline to submit the proposal for terms and conditions or methodologies or plans to the competent authorities.

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)

- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Regional risk mitigation plan (draft)

Output

- EU DSO Opinion

> GOOD TO KNOW
>
> **Timing**
>
> until 3 weeks before submission

Accountable: EU DSO

Involved Stakeholders

Responsible: EU DSO

Informed: TSO

8.6 Paragraph 5 (/2)

TSOs responsible for the proposal for terms and conditions or methodologies or plans shall take into consideration the reasoned opinion of the EU DSO entity prior to its submission for competent authorities' approval. TSOs shall provide reasoning where the EU DSO entity opinion is not taken into account.

Other NCCS Articles

- Article 6(6)

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Regional risk mitigation plan (draft)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: ACER, NCA

8.7 Paragraph 6

When jointly developing terms, conditions and methodologies and plans, the participating TSOs shall closely cooperate. TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall regularly inform competent authorities and ACER about the progress of developing the terms and conditions or methodologies, or plans.

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Regional risk mitigation plan (draft)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: ACER, NCA

Chapter 9

Article 7: Voting rules in the TSOs

9.1 Paragraph 1

Where TSOs deciding on proposals for terms and conditions or methodologies are not able to reach an agreement, they shall decide by qualified majority voting. A qualified majority for such proposals shall be calculated as follows:

a. TSOs representing at least 55 % of the Member States; and

b. TSOs representing Member States comprising at least 65 % of the population of the Union.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35

- Article 37(8)
- Article 8

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Output

- Decision on proposals

Accountable: TSO

Involved Stakeholders

Responsible: TSO

9.2 Paragraph 2

A blocking minority for decisions on proposals for terms and conditions or methodologies listed in Article 6(2) shall include TSOs representing at least four Member States, failing of which the qualified majority shall be deemed attained.

Relevant NCCS Articles

- Article 6(2)

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 8

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Output

- Decision on proposals

Accountable: TSO

Involved Stakeholders

Responsible: TSO

9.3 Paragraph 3

Where TSOs of a system operation region deciding on proposals for plans listed in Article 6(2) are not able to reach an agreement, and where the system operation region concerned is composed of more than five Member States, TSOs shall decide by qualified majority voting. A qualified majority for proposals listed in Article 6(2) shall require the following majority:

a. TSOs representing at least 72 % of the Member States concerned; and

b. TSOs representing Member States comprising at least 65 % of the population of the concerned area.

Relevant NCCS Articles

- Article 6(2)

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 8

Input

- Risk assesment methodologies (draft)

- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Output

- Decision on proposals

Accountable: TSO

Involved Stakeholders

Responsible: TSO

9.4 Paragraph 4

A blocking minority for decisions on proposals for the plans shall include at least a minimum number of TSOs representing more than 35 % of the population of the participating Member States, plus TSOs representing at least one additional Member State concerned, failing of which the qualified majority shall be deemed attained.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 8

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Output

- Decision on proposals

Accountable: TSO

Involved Stakeholders

Responsible: TSO

9.5 Paragraph 5

For TSO decisions on proposals for terms and conditions or methodologies pursuant to Article 6(2), one vote shall be attributed per Member State. If there is more than one TSO in the territory of a Member State, the Member State shall allocate the voting powers among the TSOs.

Relevant NCCS Articles

- Article 6(2)

Other NCCS Articles

- Article 18(1)

- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 8

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

GOOD TO KNOW

Timing

Decision on proposals

Accountable: TSO

Involved Stakeholders

Responsible: TSO

9.6 Paragraph 6 (/1)

If TSOs, in cooperation with the EU DSO entity, fail to submit an initial or amended proposal for terms and conditions or methodologies, or for plans, to the relevant competent authorities within the deadlines set out in this Regulation, they shall provide the relevant competent authorities and ACER with the relevant drafts of the terms and conditions or methodologies, or of the plans. They shall explain what has prevented an agreement.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 8

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Explanation

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: ACER, NCA

9.7 Paragraph 6 (/2)

The competent authorities shall jointly take the appropriate steps for the adoption of the required terms and conditions or methodologies, or of the required plans. This may be done for instance by requesting amendments to the drafts pursuant to this paragraph, by revising and completing those drafts, or, where no drafts have been provided, by defining and approving the required terms and conditions or methodologies or plans.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 8

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Explanation

Output

- Risk assesment methodologies (approved)
- Comprehensive risk assesment report (approved)
- Minimum cyber security controls (approved)
- Advanced cyber security controls (approved)
- Minimum cyber security controlls in supply chain (approved)
- Advanced cyber security controlls in supply chain (approved)
- Mapping matrix (approved)
- Procurement recommandations (approved)
- Cyber-attack classification scale methodology (approved)

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: TSO, ACER

Chapter 10

Article 8: Submission of proposals to the competent authorities

10.1 Paragraph 1 (/1)

TSOs shall submit the proposals for terms and conditions or methodologies, or for plans for approval to the relevant competent authorities within the respective deadlines set out in Articles 18, 23, 29, 33, 34, 35 and 37.

Relevant NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)

Other NCCS Articles

- Article 6(2)

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Explanation

Accountable: TSO

Involved Stakeholders

Responsible: TSO, NCA

10.2 Paragraph 1 (/2)

The competent authorities may jointly prolong these deadlines in exceptional circumstances, notably in cases where a deadline cannot be met due to circumstances external to the sphere of TSOs or of the EU DSO entity.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)

- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Output

- Prolongation

Accountable: NCA

Involved Stakeholders

Responsible: NCA

10.3 Paragraph 2

Proposals for terms and conditions, methodologies or for plans pursuant to paragraph 1, shall be submitted for information to ACER at the same time that they are submitted to the competent authorities.

Relevant NCCS Articles

- term:a18 Articlep1[Article 18. Article(1)]

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Accountable: TSO

Involved Stakeholders

Responsible: TSO

Informed: ACER

10.4 Paragraph 3 (/1)

Upon a joint request of the NRAs, ACER shall issue an opinion on the proposal for terms and conditions or methodologies, or for the plans, within six months of the receipt of the proposals for terms and conditions or methodologies, or for plans and notify NRAs and competent authorities of the opinion.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Opinion request

Output

- ACER opinion

GOOD TO KNOW

Timing

Within 6 months from receiving recommendations regarding conditions or methodologies, as well as plans

Accountable: ACER

Involved Stakeholders

Responsible: ACER

Informed: NCA, NRA

10.5 Paragraph 3 (/2)

NRAs, CS-NCAs and any other authorities designated as competent authorities shall coordinate with each other before the NRAs requests an opinion to ACER.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Output

- ACER opinion request

Accountable: NRA

Involved Stakeholders

Responsible: ACER, NCA, NRA, CS NCA

10.6 Paragraph 3 (/3)

ACER may include recommendations in such opinion. ACER shall consult ENISA before issuing an opinion on the proposals listed in Article 6(2).

Relevant NCCS Articles

- Article 6(2)

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)

- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Opinion request

Output

- ACER opinion

> GOOD TO KNOW
>
> **Timing**
>
> Within 6 months

Accountable: ACER

Involved Stakeholders

Responsible: ACER

Consulted: ENISA

10.7 Paragraph 4

The competent authorities shall consult and closely cooperate and coordinate with each other in order to reach an agreement on the proposed terms and conditions, methodologies, or plans. Before approving the terms and conditions or methodologies, or the plans, they shall revise and complete the proposals where necessary, after consulting the ENTSO for Electricity and the EU DSO entity, in order to ensure that the proposals are in line with this Regulation and contribute to a high common level of cybersecurity across the Union.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)

- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Consulted: ENTSO-E, EU DSO

10.8 Paragraph 5

The competent authorities shall decide on the terms and conditions or methodologies or on the plans within six months following the receipt of the terms and conditions or methodologies or of the plans by the relevant competent authority or, where applicable, by the last relevant competent authority concerned.

Other NCCS Articles

- Article 18(1)
- Article 23

- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)

Output

- Decision

> GOOD TO KNOW
>
> **Timing**
>
> Within 6 months from receiving recommendations regarding conditions or methodologies,

> as well as plans

Accountable: NCA

Involved Stakeholders

Responsible: NCA

10.9 Paragraph 6

Where ACER issues an opinion, the relevant competent authorities shall take that opinion into account and shall take their decisions within six months from the receipt of ACER's opinion.

>

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Acer opinion

Output

- Decision

GOOD TO KNOW

Timing

Within 6 months from receiving the opinion of ACER

Accountable: NCA

Involved Stakeholders

Responsible: NCA

10.10 Paragraph 7 (/1)

Where the competent authorities jointly require an amendment to the proposed terms and conditions or methodologies, or the plans, in order to approve them, the TSOs shall develop, in cooperation with the EU DSO entity, a proposal for such amendment to the terms and conditions or methodologies, or the plans. The TSOs shall submit the amended proposal for approval within two months following the request of the competent authorities.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Decision

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controls in supply chain (draft)
- Advanced cyber security controls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Acer opinion

GOOD TO KNOW

Timing

Within 2 months from the request

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: NCA

10.11 Paragraph 7 (/2)

The competent authorities shall decide on the amended terms and conditions or methodologies, or plans, within two months following their submission.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)

- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Acer opinion

Output

- Decision

> GOOD TO KNOW
>
> **Timing**
>
> Within 2 months from submission

Accountable: NCA

Involved Stakeholders

Responsible: NCA

10.12 Paragraph 8 (/1)

> Where the competent authorities have not been able to reach an agreement within the period referred to in paragraph 5 or 7, they shall inform the Commission.

Relevant NCCS Articles

- Article 8(5)
- Article 8(7)

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)

- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Acer opinion
- Notification

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: EC

10.13 Paragraph 8 (/2)

The Commission may take appropriate steps to make possible the adoption of the required terms and conditions or methodologies, or plans.

Other NCCS Articles

- Article 18(1)
- Article 23

- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Acer opinion
- Notification

Output

- Decision

Accountable: EC

Involved Stakeholders

Responsible: EC

Informed: NCA

10.14 Paragraph 9

TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO entity shall publish the terms and conditions or methodologies, or the plans, on their websites following approval by the relevant competent authorities, except where such information is considered as confidential in accordance with Article 47.

Relevant NCCS Articles

- Article 47

Other NCCS Articles

- Article 18(1)

- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Decision

Output

- Risk assesment methodologies (approved)
- Comprehensive risk assesment report (approved)
- Minimum cyber security controls (approved)
- Advanced cyber security controls (approved)
- Minimum cyber security controlls in supply chain (approved)
- Advanced cyber security controlls in supply chain (approved)
- Mapping matrix (approved)
- Procurement recommandations (approved)
- Cyber-attack classification scale methodology (approved)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO, NCA

Informed: HIE, CIE

10.15 Paragraph 10 (/1)

The competent authorities may jointly request proposals for amendments of the approved terms and conditions or methodologies, or of the approved plans, from TSOs and the EU DSO entity and determine a deadline for the submission of those proposals.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (approved)
- Comprehensive risk assesment report (approved)
- Minimum cyber security controls (approved)
- Advanced cyber security controls (approved)
- Minimum cyber security controlls in supply chain (approved)
- Advanced cyber security controlls in supply chain (approved)
- Mapping matrix (approved)
- Procurement recommandations (approved)
- Cyber-attack classification scale methodology (approved)

Output

- Modification request

Accountable: NCA

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO, NCA

10.16 Paragraph 10 (/2)

TSOs, in cooperation with the EU DSO entity, may propose amendments to the competent authorities also on its own initiative. The proposals for amendment to the terms and conditions or methodologies, or for the amendments to the plans, shall be developed and approved in accordance with the procedure set out in this Article.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (approved)
- Comprehensive risk assesment report (approved)
- Minimum cyber security controls (approved)
- Advanced cyber security controls (approved)
- Minimum cyber security controlls in supply chain (approved)
- Advanced cyber security controlls in supply chain (approved)
- Mapping matrix (approved)

- Procurement recommandations (approved)
- Cyber-attack classification scale methodology (approved)

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Acer opinion

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: NCA

10.17 Paragraph 11

At least every three years after the first adoption of the respective terms and conditions or methodologies, or the respective adopted plans, TSOs in cooperation with the EU DSO entity, shall review the effectiveness of the adopted terms and conditions or methodologies, or the adopted plans, and shall report the findings of the review to the competent authorities and ACER without undue delay.

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 6(2)

Input

- Risk assesment methodologies (approved)
- Comprehensive risk assesment report (approved)
- Minimum cyber security controls (approved)
- Advanced cyber security controls (approved)
- Minimum cyber security controlls in supply chain (approved)

- Advanced cyber security controlls in supply chain (approved)
- Mapping matrix (approved)
- Procurement recommandations (approved)
- Cyber-attack classification scale methodology (approved)

Output

- Review report

> GOOD TO KNOW
>
> **Timing**
>
> Within 3 years

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: ACER

Chapter 11

Article 9: Consultation

11.1 Paragraph 1

TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall consult stakeholders, including ACER, ENISA and the competent authority of each Member State, on the draft proposals for terms and conditions or methodologies listed in Article 6(2) and for plans referred to in Article 6(3). The consultation shall last for a period of not less than one month.

Relevant NCCS Articles

- Article 6(2)
- Article 6(3)

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 22

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Regional risk mitigation plan (draft)

Output

- Comments

GOOD TO KNOW

Timing

Min. 1 month

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: ACER, ENISA

11.2 Paragraph 2

The proposals for terms and conditions or methodologies listed in Article 6(2) submitted by the TSOs, in cooperation with the EU DSO entity, shall be published and submitted to consultation at Union level. The proposals for plans listed in Article 6(3) submitted by the relevant TSOs, in cooperation with the EU DSO entity, at regional level shall be submitted to consultation at least at regional level.

Relevant NCCS Articles

- Article 6(2)
- Article 6(3)

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 22

Input

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)
- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)

- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Regional risk mitigation plan (draft)

Output

- Comments

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

11.3 Paragraph 3

TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO Entity responsible for the proposal for terms and conditions or methodologies or plans shall duly take into account the views of stakeholders resulting from the consultations undertaken in accordance with paragraph 1, prior to its submission for regulatory approval. In all cases, a sound justification for including or not including the views resulting from the consultation shall be provided together with the submission and published in a timely manner before or simultaneously with the proposal for terms and conditions or methodologies.

Relevant NCCS Articles

- Article 9(1)

Other NCCS Articles

- Article 18(1)
- Article 23
- Article 29
- Article 34
- Article 33
- Article 35
- Article 37(8)
- Article 22

Input

- Comments

Output

- Risk assesment methodologies (draft)
- Comprehensive risk assesment report (draft)

- Minimum cyber security controls (draft)
- Advanced cyber security controls (draft)
- Minimum cyber security controlls in supply chain (draft)
- Advanced cyber security controlls in supply chain (draft)
- Mapping matrix (draft)
- Procurement recommandations (draft)
- Cyber-attack classification scale methodology (draft)
- Regional risk mitigation plan (draft)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Chapter 12

Article 10: Stakeholder involvement

ACER, in close cooperation with ENTSO for Electricity and the EU DSO entity, shall organise stakeholder involvement, including regular meetings with stakeholders to identify problems and propose improvements related to the implementation of this Regulation.

Input

- Comments

Output

- Review report

Accountable: ACER

Involved Stakeholders

Responsible: ENTSO-E, ACER, EU DSO

Chapter 13

Article 11: Recovery of costs

13.1 Paragraph 1

The costs borne by TSOs and DSOs subject to network tariff regulation and stemming from the obligations laid down in this Regulation, including the costs borne by the ENTSO for Electricity and the EU DSO entity, shall be assessed by the relevant NRA of each Member State.

Accountable: NRA

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO, DSO, NRA

13.2 Paragraph 2

Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms, as determined by the relevant NRA.

Accountable: NRA

Involved Stakeholders

Responsible: NRA

13.3 Paragraph 3

If requested by the relevant NRAs, TSOs and DSOs referred to in paragraph 1 shall, within a reasonable period determined by the NRA, provide the information necessary to facilitate the assessment of the costs incurred.

Relevant NCCS Articles

- Article 11(1)

Accountable: NRA

Involved Stakeholders

Responsible: TSO, DSO, NRA

Chapter 14

Article 12: Monitoring

14.1 Paragraph 1

ACER shall monitor the implementation of this Regulation in accordance with Article 32(1) of Regulation (EU) 2019/943 [a] and Article 4(2) of Regulation (EU) 2019/942 [b]. In carrying out this monitoring, ACER may cooperate with ENISA and request support from the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group and the NIS Cooperation Group on the implementation of this Regulation.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943&qid=1733993709560#d1e3462-54-1

[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942#d1e519-22-1

Other NCCS Articles

- Article 12(2)

Accountable: ACER

Involved Stakeholders

Responsible: ENTSO-E, ACER, ENISA, EU DSO

Informed: NIS CG, ECG

14.2 Paragraph 2

ACER shall publish a report at least every three years after the entry into force of this Regulation to:

a. review the status of implementation of the applicable cybersecurity risk management measures with regard to the high-impact and critical-impact entities;

b. identify whether additional rules on common requirements, planning, monitoring, reporting and crisis management may be necessary to prevent risks for the electricity sector; and

c. identify areas of improvement for the revision of this Regulation, or determine uncovered areas and new priorities that may emerge due to technological developments.

Other NCCS Articles

- Article 12(1)
- Article 12(6)

Input

- Monitoring data

Output

- Status report

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

By 13 October 2026

Accountable: ACER

Involved Stakeholders

Responsible: ACER

14.3 Paragraph 3

By 13 June 2025, ACER, in cooperation with ENISA and after consultation of the ENTSO for Electricity and the EU DSO entity, may issue guidance on the relevant information to be communicated to ACER for the monitoring purposes as well as the process and frequency for the collection, based on the performance indicators defined in accordance with paragraph 5.

Relevant NCCS Articles

- Article 12(5)

Output

- Guidance

GOOD TO KNOW

Timing

By 13 June 2025

Accountable: ACER

Involved Stakeholders

Responsible: ACER, ENISA

Consulted: ENTSO-E, EU DSO

14.4 Paragraph 4

The competent authorities may have access to the relevant information held by ACER, which it has collected in accordance with this Article.

Accountable: ACER

Involved Stakeholders

Responsible: ACER

Informed: NCA

14.5 Paragraph 5

ACER in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity, shall issue non-binding performance indicators for the assessment of operational reliability that are related to cybersecurity aspects of cross-border electricity flows.

Output

- ORPI

GOOD TO KNOW

Timing

By 13 June 2027

Accountable: ACER

Involved Stakeholders

Responsible: ENTSO-E, ACER, ENISA, EU DSO

14.6 Paragraph 6

The entities listed in Article 2(1) of this Regulation shall submit to ACER the information required for ACER to perform the tasks listed in paragraph 2.

Relevant NCCS Articles

- Article 2(1)
- Article 2(2)

Input

- Guidance
- ORPI

Output

- Monitoring data

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: ACER

Chapter 15

Article 13: Benchmarking

15.1 Paragraph 1

By 13 June 2025, ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide. The guide shall explain to NRAs the principles of benchmarking of the implemented cybersecurity controls pursuant to paragraph 2 of this Article, taking into consideration the costs of implementing the controls and the effectiveness of the function played by processes, products, services, systems and solutions used to implement such controls. ACER shall take into account existing benchmarking reports when establishing the non-binding cybersecurity benchmarking guide. ACER shall submit the non-binding cybersecurity benchmarking guide to the NRAs for information.

Relevant NCCS Articles

- Article 13(2)

Output

- Non-binding cybersecurity benchmarking guidance

GOOD TO KNOW

Timing

By 13 June 2025

Accountable: ACER

Involved Stakeholders

Responsible: ACER, ENISA

Informed: NRA

15.2 Paragraph 2

Within 12 months after the establishment of the benchmarking guide pursuant to paragraph 1, the NRAs shall carry out a benchmarking analysis to assess whether current investments in cybersecurity:

a. mitigate risks having an impact on cross-border electricity flows;

b. provide the desired results and engender efficiency gains for the development of the electricity systems;

c. are efficient and integrated into the overall procurement of assets and services.

Relevant NCCS Articles

- Article 13(1)

Input

- Non-binding cybersecurity benchmarking guidance

Output

- Benchmarking analys

GOOD TO KNOW

Timing

By 13 June 2026

Accountable: NRA

Involved Stakeholders

Responsible: NRA

15.3 Paragraph 3

For the benchmarking analysis, the NRAs may take into account the non-binding cybersecurity benchmarking guide established by ACER, and shall assess in particular:

a. the average expenditure related to cybersecurity for mitigating risks having an impact on electricity cross-border flows, especially with respect to the high-impact and critical-impact entities;

b. in cooperation with the ENTSO for Electricity and the EU DSO entity, the average prices of cybersecurity services, systems and products that contribute to a large extent to the enhancement and maintenance of the cybersecurity risk-management measures in the different system operation regions;

c. the existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of this Regulation, identifying possible measures necessary to foster efficiency in spending, particularly where cybersecurity technological investments may be needed.

Other NCCS Articles

- Article 13(1)

Input

- Non-binding cybersecurity benchmarking guidance

Output

- Benchmarking analys

GOOD TO KNOW

Timing

By 13 June 2026

Accountable: NRA

Involved Stakeholders

Responsible: ENTSO-E, ACER, EU DSO, NRA

15.4 Paragraph 4

Any information related to benchmarking analysis shall be handled and processed pursuant to data classification requirements of this Regulation, the minimum cybersecurity controls and the cross-border electricity cybersecurity risk assessment report. The benchmarking analysis referred to in paragraphs 2 and 3 shall not be made public.

Relevant NCCS Articles

- Article 13(2)
- Article 13(3)

Other NCCS Articles

- Article 23(3)
- Article 23(4)
- Article 46
- Article 47

Input

- Cybersecurity controls

Output

- Benchmarking analys

Accountable: NRA

Involved Stakeholders

Responsible: ENTSO-E, ACER, EU DSO, NRA

15.5 Paragraph 5

Without prejudice to the confidentiality requirements in Article 47 and to the need to protect the security of entities subject to the provisions of this Regulation, the benchmarking analysis referred in paragraphs 2 and 3 of this Article shall be shared with all NRAs, all competent authorities, ACER, ENISA and the Commission.

Relevant NCCS Articles

- Article 13(2)
- Article 13(3)
- Article 47

Other NCCS Articles

- Article 46

Input

- Cybersecurity controls
- Information sharing guidence

Output

- Benchmarking analys

Accountable: NRA

Involved Stakeholders

Responsible: NRA

Informed: EC, ACER, ENISA

Chapter 16

Article 14: Agreements with TSOs from outside the Union

16.1 Paragraph 1

Within 18 months after the entry into force of this Regulation, TSOs of a system operation region that is neighbouring to a third country shall endeavour to conclude agreements with TSOs of the neighbouring third country that are in accordance with relevant Union law and that set out the basis for cooperation on cybersecurity protection and the cybersecurity cooperation arrangements with those TSOs.

Output

- Agreement with the neighbourghoud TSOs

GOOD TO KNOW

Timing

By 13 December 2025

Accountable: TSO

Involved Stakeholders

Responsible: TSO

16.2 Paragraph 2

TSOs shall inform the competent authority of the agreements concluded pursuant to paragraph 1.

Relevant NCCS Articles

- Article 14(1)

Accountable: TSO

Involved Stakeholders

Responsible: TSO

Informed: NCA

Chapter 17

Article 15: Legal representative

17.1 Paragraph 1

Entities who do not have an establishment in the Union, but who deliver services to entities in the Union and have been notified as being high-impact or critical-impact entities in accordance with Article 24(6), shall, within three months after the notification, designate, in writing, a representative in the Union and inform the notifying competent authority accordingly.

Relevant NCCS Articles

- Article 24(6)

Output

- Appointing a legal representative

GOOD TO KNOW

Timing

By 13 September 2028

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: NCA

17.2 Paragraph 2

This representative shall be mandated for the purpose of being addressed by any competent authority or a CSIRT in the Union in addition to or instead of the high-impact or critical-impact entity with regard to the obligations of the entity under this Regulation. The high-impact or critical-impact entity shall provide their legal representative with the necessary powers and sufficient resources to guarantee their efficient and timely cooperation with the relevant competent authorities or CSIRTs.

Other NCCS Articles

- Article 15(1)

Output

- Appointing a legal representative in the E

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: NCA

17.3 Paragraph 3

The representative shall be established in one of the Member States where the entity offers its services. The entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. High-impact or critical-impact entities shall notify the name, postal address, email address and telephone number of their legal representative to the competent authority in the Member State where that legal representative resides or is established.

Other NCCS Articles

- Article 15(1)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: NCA

17.4 Paragraph 4

It shall be possible for the designated legal representative to be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the high-impact or critical- impact entity itself.

Other NCCS Articles

- Article 15(1)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

17.5 Paragraph 5

In the absence of a representative within the Union designated under this Article, any Member State in which the entity provides services may take legal action against the entity for non-compliance with the obligations under this Regulation.

Other NCCS Articles

- Article 15(1)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

17.6 Paragraph 6

The designation of a legal representative within the Union pursuant to paragraph 1 shall not constitute an establishment in the Union.

Other NCCS Articles

- Article 15(1)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Chapter 18

Article 16: Cooperation between the ENTSO for Electricity and the EU DSO Entity

18.1 Paragraph 1 (/1)

The ENTSO for Electricity and the EU DSO entity shall cooperate in performing cybersecurity risk assessments pursuant to Article 19 and Article 21, and in particular the following tasks:

a. development of the cybersecurity risk assessment methodologies pursuant to Article 18(1);

b. development of the Comprehensive Cross-border electricity cybersecurity risk assessment report pursuant to Article 23;

c. development of the common electricity cybersecurity framework pursuant to Chapter III;

d. development of the cybersecurity procurement recommendation pursuant to Article 35;

e. development of the cyber-attacks classification scale methodology pursuant to Article 37(8);

f. development of the provisional electricity cybersecurity impact index (‘ECII’) electricity cybersecurity impact index pursuant to Article 48(1) point (a);

g. development of the consolidated provisional list of high-impact and critical-impact entities pursuant to Article 48(3);

h. development of the provisional list of Union-wide high-impact and critical-impact processes pursuant to Article 48(4);

i. development of the provisional list of European and international standards and controls pursuant to Article 48(6);

j. performance of the Union-wide cybersecurity risk assessment pursuant to Article 19;

k. performance of the regional cybersecurity risk assessments pursuant to Article 21;

l. definition of the regional cybersecurity risk mitigation plans pursuant to Article 22;

m. development of guidance on European cybersecurity certification schemes for ICT products, ICT services, and ICT processes in accordance with Article 36;

Relevant NCCS Articles

- Article 19
- Article 21
- Article 18(1)
- Article 23
- term:aIII chapter[Article III. chapter]
- Article 35
- Article 37(8)
- Article 48(1)
- Article 48(3)
- Article 48(4)
- Article 48(6)
- Article 22
- Article 36

Output

- Cybersecurity risk assessment methods
- Comprehensive cybersecurity risk assessment report for the electricity sector
- Common cybersecurity framework for the electricity sector
- Cybersecurity procurement recommendation
- Methodology for classifying cyberattacks
- Provisional ECII
- Provisional list of identified organizations
- Provisional list of EU-wide high-impact and critical-impact processes
- Provisional list of European and international standards
- EU-level cybersecurity risk assessment report
- Regional cybersecurity risk assessment report
- Regional cybersecurity risk mitigation plans
- Guidance on cybersecurity certification schemes
- Implementation guidelines

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

18.2 Paragraph 1 (/2)

(n) development of guidelines for the implementation of this Regulation in consultation with ACER and ENISA.

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: ACER, ENISA

18.3 Paragraph 2

The cooperation between the ENTSO for Electricity and the EU DSO entity may take the form of a cybersecurity risk working group.

Other NCCS Articles

- Article 16(1)

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

18.4 Paragraph 3

The ENTSO for Electricity and the EU DSO entity shall regularly inform ACER, ENISA, the NIS Cooperation Group and the Electricity Coordination Group on the progress in implementing the Union-wide and regional cybersecurity risk assessments pursuant to Article 19 and Article 21.

Relevant NCCS Articles

- Article 19
- Article 21

Other NCCS Articles

- Article 16(1)

Input

- Union wide risk assessment report
- Regional risk assessment report

Output

- EU-level cybersecurity risk assessment report
- Regional cybersecurity risk assessment report

Accountable: ENTSO-E, EU DSO

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: ACER, ENISA, NIS CG, ECG

Chapter 19

Article 17: Cooperation between ACER and the competent authorities

19.1 Paragraph 1 (/1)

ACER, in cooperation with each competent authority, shall: (1) monitor the implementation of cybersecurity risk management measures pursuant to Article 12(2) point (a) and reporting obligations pursuant to Article 27 and Article 39; and

Relevant NCCS Articles

- Article 12(2)
- Article 27
- Article 39

Input

- ACER monitoring report
- Member state risk assessment report
- Infromation sharing about cyber attack

Output

- ACER monitoring report

Accountable: ACER

Involved Stakeholders

Responsible: ACER

19.2 Paragraph 1 (/2)

(2) monitor the adoption process and the implementation of the terms and conditions, methodologies or plans pursuant to Article 6(2) and (3). The cooperation between ACER, ENISA and each competent authority may take the form of a cybersecurity risk monitoring body.

Relevant NCCS Articles

- Article 6(2)

- Article 6(3)

Input

- Cybersecurity risk assessment methods (draft)
- Comprehensive cybersecurity risk assessment report for the electricity sector (draft)
- Common cybersecurity framework for the electricity sector (draft)
- Cybersecurity procurement recommendation (draft)
- Methodology for classifying cyberattacks (draft)
- Provisional ECII (draft)
- Provisional list of identified organizations (draft)
- Provisional list of EU-wide high-impact and critical-impact processes (draft)
- Provisional list of European and international standards (draft)
- EU-level cybersecurity risk assessment report (draft)
- Regional cybersecurity risk assessment report (adraft)
- Regional cybersecurity risk mitigation plans (draft)
- Guidance on cybersecurity certification schemes (draft)
- Implementation guidelines (draft)

Output

- Cybersecurity risk assessment methods (approved)
- Comprehensive cybersecurity risk assessment report for the electricity sector (approved)
- Common cybersecurity framework for the electricity sector (approved)
- Cybersecurity procurement recommendation (approved)
- Methodology for classifying cyberattacks (approved)
- Provisional ECII (approved)

- Provisional list of identified organizations (approved)
- Provisional list of EU-wide high-impact and critical-impact processes (approved)
- Provisional list of European and international standards (approved)
- EU-level cybersecurity risk assessment report (approved)
- Regional cybersecurity risk assessment report (approved)
- Regional cybersecurity risk mitigation plans (approved)
- Guidance on cybersecurity certification schemes (approved)
- Implementation guidelines (approved)

Accountable: ACER

Involved Stakeholders

Responsible: ACER, ENISA, NCA

Chapter 20

Article 18: Cybersecurity risk assessment methodologies

20.1 Paragraph 1 (/3)

By 13 March 2025, the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and following a consultation with the NIS Cooperation Group, shall submit a proposal for the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level.

Other NCCS Articles

- Article 6(2)
- Article 18(1)
- Article 18(2)
- Article 18(3)
- Article 18(4)

Input

- Provisional ECII

Output

- Risk assessment methodologies
- Risk impact matrix

> 
>
> GOOD TO KNOW
>
> **Timing**
>
> By 13 March 2025

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG

20.2 Paragraph 2

The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall include:

a. a list of cyber threats to be considered, including at least the following supply chain threats:
    a. a severe and unexpected corruption of the supply chain;
    b. the unavailability of ICT products, ICT services, or ICT processes from the supply chain;
    c. cyber-attacks initiated through actors in the supply chain;
    d. leaking of sensitive information through the supply chain, including supply chain tracking;
    e. the introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain;
b. the criteria to evaluate the impact of cybersecurity risks as high or critical, using defined thresholds for consequences and likelihood;
c. an approach to analyse the cybersecurity risks coming from legacy systems, the cascading effects of cyber-attacks and the real-time nature of systems operating the grid;
d. an approach to analyse the cybersecurity risks coming from the dependency on a single supplier of ICT products, ICT services or ICT processes.

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG

20.3 Paragraph 3

The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall assess cybersecurity risks using the same risk impact matrix. The risk impact matrix shall:

a. measure the consequences of cyber-attacks based on the following criteria:
    a. loss of load;
    b. reduction of power generation;
    c. loss of capacity in the primary frequency reserve;
    d. loss of capacity for restoration of an electric grid to operation without relying on the external transmission network to recover after a total or partial shutdown (also called 'black start');
    e. the expected duration of an electricity outage affecting customers in combination with the scale of the outage in customer numbers; and
    f. any other quantitative or qualitative criteria that could reasonably act as an indicator of the effect of a cyber- attack on cross-border electricity flows;
b. measure the likelihood of an incident as the frequency of cyber-attacks per year.

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG

20.4 Paragraph 4

The cybersecurity risk assessment methodologies at Union level shall describe how the ECII values for high-impact and critical-impact thresholds will be defined. The ECII shall enable entities to estimate with the help of the criteria referred to in paragraph 2 point (b), the impact of the risks on their business process during the business impact assessments they perform pursuant to Article 26(4) point (c)(i).

Relevant NCCS Articles

- Article 26(4)
- Article 18(2)

Other NCCS Articles

- Article 19(3)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG

20.5 Paragraph 5

The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the Electricity Coordination Group on the proposals for the cybersecurity risk assessment methodologies that are developed pursuant to paragraph 1.

Relevant NCCS Articles

- Article 18(1)

Input

- Risk assessment methodologies

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: ECG

Chapter 21

Article 19: Union-wide cybersecurity risk assessment

21.1 Paragraph 1

Within 9 months after the approval of the cybersecurity risk assessment methodologies pursuant to Article 8 and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall, without prejudice to Article 22 of Directive (EU) 2022/2555 [a], perform a Union-wide cybersecurity risk assessment and draw up a draft Union-wide cybersecurity risk assessment report. For this purpose, they will use the methodologies developed pursuant to Article 18, and approved pursuant to Article 8, to identify, analyse, and evaluate the possible consequences of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The Union-wide cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_22

Relevant NCCS Articles

- Article 8
- Article 18

Other NCCS Articles

- Article 19(2)

Output

- Union wide cybersecurity risk assessment report

GOOD TO KNOW

Timing

Within 9 months after the approval of cybersecurity risk assessment methodologies

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: NIS CG

21.2 Paragraph 2

The Union-wide cybersecurity risk assessment report shall include the following elements:

a. the Union-wide high-impact processes and the Union-wide critical-impact processes;

b. a risk impact matrix that entities and the competent authorities shall use to assess the cybersecurity risk identified in the cybersecurity risk assessment at Member State level performed pursuant to Article 20 and in the cybersecurity risk assessment at entity level pursuant to Article 26(2) point (b).

Relevant NCCS Articles

- Article 20
- Article 26(2)

Other NCCS Articles

- Article 19(3)

Input

- Union-wide provisional process list

Output

- Risk impact matrix
- Union-wide process list

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: NIS CG

21.3 Paragraph 3

With respect to the Union-wide high-impact processes and the Union-wide critical-impact processes, the Union- wide cybersecurity risk assessment report shall include:

a. an assessment of the possible consequences of a cyber-attack using the metrics defined in the cybersecurity risk assessment methodology developed pursuant to Article 18(2), (3) and (4), and approved pursuant to Article 8;

b. the ECII and high-impact and critical-impact thresholds that the competent authorities shall use pursuant to Article 24(1) and (2) to identify high-impact and critical-impact entities involved in the Union-wide high-impact processes and in the Union-wide critical-impact processes.

Relevant NCCS Articles

- Article 18(2)
- Article 18(3)
- Article 18(4)
- Article 24(1)
- Article 24(2)

Input

- Union-wide process list
- Risk assessment methodologies

Output

- ECII

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: NIS CG

21.4 Paragraph 4 (/1)

The ENTSO for Electricity, in cooperation with the EU DSO entity, shall submit the draft of the Union-wide cybersecurity risk assessment report with the results of the Union-wide cybersecurity risk assessment to ACER for opinion.

Other NCCS Articles

- Article 19(1)

Input

- Union wide risk assessment report (draft)

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: ACER

21.5 Paragraph 4 (/2)

ACER shall issue an opinion on the draft report within three months after its receipt. The ENTSO for Electricity and the EU DSO entity shall take utmost account of ACER's opinion when finalising that report.

Input

- Union wide risk assessment report (draft)

Output

- Acer opinion

GOOD TO KNOW

Timing

Within three months from receiving the draft report

Accountable: ACER

Involved Stakeholders

Responsible: ENTSO-E, ACER, EU DSO

21.6 Paragraph 5

Within three months after receipt of ACER's opinion, the ENTSO for Electricity, in cooperation with the EU DSO entity shall notify the final Union-wide cybersecurity risk assessment report to ACER, the Commission, ENISA and the competent authorities.

Other NCCS Articles

- Article 19(4)

Input

- ACER opinion

Output

- Union wide risk assessment report (draft)

GOOD TO KNOW

Timing

Within three months from receiving the opinion of ACER

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: EC, ACER, ENISA, NCA

Chapter 22

Article 20: Member State cybersecurity risk assessment

22.1 Paragraph 1

Each competent authority shall perform a Member State cybersecurity risk assessment on all high-impact and critical-impact entities in its Member State using the methodologies developed pursuant to Article 18 and approved pursuant to Article 8. The Member State cybersecurity risk assessment shall identify and analyse the risks of cyber-attacks affecting the operational security of the electricity system disrupting cross-border electricity flows. The Member State cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.

Relevant NCCS Articles

- Article 18
- Article 8

Other NCCS Articles

- Article 19(2)

Input

- Risk assessment methodologies

Accountable: NCA

Involved Stakeholders

Responsible: NCA

22.2 Paragraph 2

Within 21 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and every three years after that date, and after consulting the CS-NCA responsible for electricity, each competent authority, supported by the CSIRT, shall provide a Member State cybersecurity risk assessment report to the ENTSO for Electricity and the EU DSO entity, containing the following information for each high-impact and critical-impact business process:

a. the implementation status of the minimum and advanced cybersecurity controls pursuant to Article 29;

b. a list of all cyber-attacks reported in the previous three years pursuant to Article 38(3);

c. a summary of the cyber threat information reported in the previous three years pursuant to Article 38(6);

d. for each Union-wide high-impact or critical-impact process, an estimate of the risks of a compromise of the confidentiality, integrity and availability for information and relevant assets;

e. where necessary, a list of additional entities identified as high-impact or critical-impact pursuant to Article 24(1), (2), (3), and (5).

Relevant NCCS Articles

- Article 24(6)
- Article 29
- Article 38
- Article 38(3)
- Article 38(6)
- Article 24(1)
- Article 24(2)
- Article 24(3)
- Article 24(5)

Other NCCS Articles

- Article 20(3)

Input

- Entitiy level risk assessment

Output

- Member state level risk assessment

GOOD TO KNOW

Recurrence

3 yeras

GOOD TO KNOW

Timing

By 13 March 2030

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Consulted: CS NCA

Informed: ENTSO-E, EU DSO

22.3 Paragraph 3

The Member State cybersecurity risk assessment report shall take into account the Member State's risk preparedness plan established pursuant to Article 10 of Regulation (EU) 2019/941 [a].

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Consulted: CS NCA

Informed: ENTSO-E, EU DSO

22.4 Paragraph 4

The information contained in the Member State cybersecurity risk assessment report pursuant to paragraph 2 points (a) to (d) shall not be linked to specific entities or assets. The Member State cybersecurity risk assessment report shall also include a risk assessment of the temporary derogations issued by the competent authorities in the Member States pursuant to Article 30.

Relevant NCCS Articles

- Article 20(2)
- Article 30

Input

- Risk assessment of the temporary derogations

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Consulted: CS NCA

Informed: ENTSO-E, EU DSO

22.5 Paragraph 5

The ENTSO for Electricity and the EU DSO entity may request additional information from the competent authorities in relation to the tasks specified in subparagraph 2 points (a) and (c).

Relevant NCCS Articles

- term:a20p2 a and c[Article 20(2) a) and c)]

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO, NCA

22.6 Paragraph 6

The competent authorities shall ensure that the information they provide is accurate and correct.

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Chapter 23

Article 21: Regional cybersecurity risk assessments

23.1 Paragraph 1

The ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the relevant Regional Coordination Centre, shall perform a regional cybersecurity risk assessment for each system operation region using the methodologies developed pursuant to Article 19, and approved pursuant to Article 8, to identify, analyse, and evaluate the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The regional cybersecurity risk assessments shall not consider the legal, financial or reputational damage of cyber- attacks.

Relevant NCCS Articles

- Article 18
- Article 8

Input

- Risk assessment methodologies

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: RCC

23.2 Paragraph 2

Within 30 months after the notification of the high-impact and critical-impact entities pursuant to Article 24(6), and every three years after that, the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall draw up a regional cybersecurity risk assessment report for each system operation region.

Relevant NCCS Articles

- Article 24(6)

Other NCCS Articles

- Article 21(3)
- Article 21(4)

Output

- Regional level risk assessment

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

By 13 December 2030

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: NIS CG

23.3 Paragraph 3

> The regional cybersecurity risk assessment report shall take into account the relevant information contained in the Union-wide cybersecurity risk assessment reports and in the Member State cybersecurity risk assessments reports.

Input

- Union wide risk assessment
- Member state level risk assessment

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

23.4 Paragraph 4

The regional cybersecurity risk assessment shall consider the regional electricity crisis scenarios related to cybersecurity identified pursuant to Article 6 of the Regulation (EU) 2019/941. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941#d1e698-1-1

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Chapter 24

Article 22: Regional cybersecurity risk mitigation plans

24.1 Paragraph 1

Within 36 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and no later than 13 June 2031, and every three years after that date, the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the Regional Coordination Centres and the NIS Cooperation Group, shall develop a regional cybersecurity risk mitigation plan for each system operation region.

Relevant NCCS Articles

- Article 24(6)

Other NCCS Articles

- Article 22(2)

Output

- Regional risk mitigation plan (draft)

GOOD TO KNOW

Recurrence

3 yeras

GOOD TO KNOW

Timing

By 13 June 2031

A

Accountable: TSO

Involved Stakeholders

R

Responsible: ENTSO-E, TSO, EU DSO

Consulted: RCC

24.2 Paragraph 2

The regional cybersecurity risk mitigation plans shall include:

a. the minimum and advanced cybersecurity controls that high-impact and critical-impact entities shall apply in the system operation region;

b. the residual cybersecurity risks in the system operation regions after applying the controls referred to in point (a).

Output

- Minimum and advanced controls
- Residual risks

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: RCC

24.3 Paragraph 3

The ENTSO for Electricity shall submit the regional risk mitigation plans to the relevant transmission system operators, to the competent authorities, and to the Electricity Coordination Group. The Electricity Coordination Group may recommend amendments.

Input

- Regional risk mitigation plan

Output

- Request of modification

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, ECG

Informed: TSO, NCA

24.4 Paragraph 4

The TSOs, with the assistance of the ENTSO for Electricity in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group shall update the regional risk mitigation plans every three years, unless circumstances warrant more frequent updates.

Input

- Regional risk mitigation plan

Output

- Regional risk mitigation plan

GOOD TO KNOW

Recurrence

at least 3 years

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG, RCC

Chapter 25

Article 23: Comprehensive cross-border electricity cybersecurity risk assessment report

25.1 Paragraph 1

Within 40 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and every three years thereafter, TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall provide to the Electricity Coordination Group a report on the outcome of the assessment of cybersecurity risks with regard to cross-border electricity flows (the 'comprehensive cross-border electricity cybersecurity risk assessment report')

Relevant NCCS Articles

- Article 24(6)

Other NCCS Articles

- Article 23(2)

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

By 13 October 2031

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG

Informed: ECG

25.2 Paragraph 2

The comprehensive cross-border electricity cybersecurity risk assessment report shall be based on the Union-wide cybersecurity risk assessment report, on the Member State cybersecurity risk assessment reports and on the regional cybersecurity risk assessment reports and include the following information:

a. the list of Union-wide high-impact and critical-impact processes identified in the Union-wide cybersecurity risk assessment report in accordance with Article 19(2) point (a) including the estimation of likelihood and impact of cybersecurity risks evaluated during the regional cybersecurity risk assessment reports pursuant to Article 21(2) and Article 19(3) point (a);

b. current cyber threats, with a specific focus on emerging threats and risks for the electricity system;

c. cyber-attacks for the previous period at Union level, providing a critical overview of how such cyber-attacks may have had an impact on electricity cross-border flows;

d. overall status of implementation of the cybersecurity measures;

e. status of implementation of the information flows pursuant to Articles 37 and 38;

f. list of information or specific criteria for classification of information pursuant to Article 46;

g. identified and highlighted risks that may derive from insecure supply chain management;

h. results and accumulated experiences from regional and cross-regional cybersecurity exercises organised pursuant to Article 44;

i. an analysis of the development of the overall cross-border cybersecurity risks in the electricity sector since the last regional cybersecurity risk assessments;

j. any other information that may be useful to identify possible improvements of this Regulation or the need for a revision of this Regulation or any of its tools; and

k. aggregated and anonymised information of derogations granted pursuant to Article 30(3).

Relevant NCCS Articles

- Article 19(2)
- Article 19(3)
- Article 21(2)
- Article 37
- Article 38
- Article 44
- Article 30(3)

Other NCCS Articles

- Article 46

Input

- Union wide risk assessment report
- Member state level risk assessment
- Regional risk assessment

Output

- Comprehensive cross-border electricity cybersecurity risk assessment report

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG

25.3 Paragraph 3

The entities listed in Article 2(1) may contribute to the development of the comprehensive cross-border electricity cybersecurity risk assessment report, respecting the confidentiality of information in accordance with Article 47. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall consult these entities from an early stage.

Relevant NCCS Articles

- Article 47
- Article 2(1)

Accountable: TSO

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, EU DSO

25.4 Paragraph 4 (/1)

The comprehensive cross-border electricity cybersecurity risk assessment report shall be subject to the rules on protection of exchange of information pursuant to Article 46. Without prejudice to Article 10(4) and Article 47(4), the ENTSO for Electricity and the EU DSO entity shall release a public version of that report which shall not contain information that can cause damage to entities listed in Article 2(1).

Relevant NCCS Articles

- Article 46
- Article 20(4)
- Article 47(4)
- Article 2(1)

Input

- Comprehensive cross-border electricity cybersecurity risk assessment report

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG

25.5 Paragraph 4 (/2)

The public version of this report shall only be released with the agreement of the NIS Cooperation Group and the Electricity Coordination Group. The ENTSO for Electricity in coordination with the EU DSO entity shall be responsible for the compilation and the release of the public version of the report.

Output

- Comprehensive cross-border electricity cybersecurity risk assessment report (published)

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO, NIS CG, ECG

Chapter 26

Article 24: Identification of high-impact and critical-impact entities

26.1 Paragraph 1

Each competent authority shall identify, by using the ECII and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3), point (b), the high-impact and critical- impact entities in its Member State that are involved in the Union-wide high-impact and critical-impact processes. The competent authorities can request information from an entity in their Member State to determine the ECII values for that entity. If the determined ECII of an entity is above the high-impact or critical-impact threshold, the identified entity shall be listed in the Member State cybersecurity risk assessment report referred to in Article 20(2).

Relevant NCCS Articles

- Article 19(3)
- Article 20(2)

Input

- Union wide risk assessment report
- ECII
- Union wide high impact and critical impact processes

Output

- Identified organizations

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

26.2 Paragraph 2

Each competent authority shall identify, by using the ECII and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3), point (b), the high-impact and critical- impact entities not established in the Union in so far they are active within the Union. The competent authority may request information from an entity not established in the Union to determine the ECII values for the entity.

Relevant NCCS Articles

- Article 19(3)

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

26.3 Paragraph 3

Each competent authority may identify additional entities in its Member State as high-impact or critical-impact entities if the following criteria are met:

a. the entity is part of a group of entities for which there is a significant risk that they will be affected simultaneously by a cyber-attack;

b. the ECII aggregated over the group of entities is above the high-impact or critical-impact threshold.

Input

- Grouping criteria

Output

- Identified entities

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

26.4 Paragraph 4

If a competent authority identifies additional entities in accordance with paragraph 3, all processes at these entities for which the ECII aggregated over the group are above the high-impact threshold shall be considered high-impact processes, and all processes at these entities for which the ECII aggregated over the group are above the critical-impact thresholds shall be considered critical-impact processes.

Relevant NCCS Articles

- Article 24(3)

Input

- Union wide risk assessment report
- ECII
- Union wide high impact and critical impact processes

Output

- Entity level high and critical processes

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

26.5 Paragraph 5 (/1)

If a competent authority identifies entities referred to in paragraph 3 point (a) in more than one Member State, it shall inform the other competent authorities, the ENTSO for Electricity and the EU DSO entity.

Relevant NCCS Articles

- Article 24(3)

Other NCCS Articles

- Article 47

Input

- Identified entities

Output

- Information sharing

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

Informed: ENTSO-E, EU DSO

26.6 Paragraph 5 (/2)

The ENTSO for Electricity in cooperation with the EU DSO entity, based on the information received from all competent authorities, shall provide to the competent authorities an analysis of the aggregation of entities in more than one Member State that can create a distributed disturbance to the cross-border electricity flows, and can result in a cyber-attack.

Other NCCS Articles

- Article 19

Input

- Information sharing

Output

- Union wide cybersecurity risk assessment report

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: NCA

26.7 Paragraph 5 (/3)

Where a group of entities in several Member States is identified as an aggregation whose ECII is above the high-impact or critical-impact threshold, all concerned competent authorities shall identify the entities in such group as high-impact or critical-impact entities for their respective Member State, based on the aggregated ECII for the group of the entities, and the identified entities shall be listed in the Union-wide cybersecurity risk assessment report.

Accountable: NCA

Involved Stakeholders

Responsible: NCA

26.8 Paragraph 6

Each competent authority shall, within nine months after being notified by ENTSO for Electricity and EU DSO entity of the Union-wide cybersecurity risk assessment report pursuant to Article 19(5) and in any case no later than 13 June 2028, notify to the entities on the list that they have been identified as a high-impact or critical-impact entity in its Member State.

Relevant NCCS Articles

- Article 19(5)

Input

- Union wide risk assessment report
- ECII
- Union wide high impact and critical impact processes

Output

- Identified entities

> GOOD TO KNOW
>
> **Timing**
>
> By 13 June 2028

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: HIE, CIE

26.9 Paragraph 7 (/1)

When a service provider is reported to a competent authority as being a critical ICT service provider pursuant to Article 27 point (c),

Relevant NCCS Articles

- Article 27

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: NCA, CRITICAL ICT

26.10 Paragraph 7 (/2)

that competent authority shall notify it to the competent authorities of the Member States in whose territories the seat or representative is situated. The latter competent authority shall notify the service provider that it has been identified as being a critical service provider.

Input

- Identified critical IKT providers

Output

- Information sharing

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

Informed: CRITICAL ICT

Chapter 27

Article 25: National verification schemes

27.1 Paragraph 1

The competent authorities may establish a national verification scheme to verify that critical-impact entities identified pursuant to Article 24(1) have implemented the national legislative framework that is included in the mapping matrix referred to in Article 34. The national verification scheme may be based on an inspection carried out by the competent authority, independent security audits, or on mutual peer reviews by critical-impact entities in the same Member State supervised by the competent authority.

Relevant NCCS Articles

- Article 24(1)
- Article 34

Input

- Identified entities
- Mapping matrix
- National verification scheme

Output

- Verified entities

Accountable: NCA

Involved Stakeholders

Responsible: NCA

27.2 Paragraph 2

If a competent authority decides to establish a national verification scheme, that competent authority shall ensure that the verification is performed in accordance with the following requirements:

a. any party performing the peer review, audit or inspection shall be independent from the critical-impact entity being verified, and shall have no conflicts of interest;

b. the staff performing the peer review, audit or inspection shall have demonstrable knowledge of:

    a. cybersecurity in the electricity sector;
    b. cybersecurity management systems;
    c. the principles of auditing;
    d. cybersecurity risk assessment;
    e. the common electricity cybersecurity framework;

f. the national legislative and regulatory framework and European and international standards in scope of the verification;

g. the critical-impact processes in scope of the verification;

c. the party performing the peer review, audit or inspection shall be allowed sufficient time to perform these activities;

d. the party performing the peer review, audit or inspection shall take the appropriate measures to protect the information they collect during the verification, in line with its confidentiality level; and

e. peer reviews, audits or inspections shall be performed at least once every year and cover the full verification scope at least every three years.

GOOD TO KNOW

Recurrence

1 and 3 years

Accountable: NCA

Involved Stakeholders

Responsible: NCA

27.3 Paragraph 3

If a competent authority decides to establish a national verification scheme, it shall report to ACER on an annual basis how frequently it has carried out inspections under that scheme.

Input

- National verification sceme

Output

- Report to ACER

GOOD TO KNOW

Recurrence

1 years

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: ACER

Chapter 28

Article 26: Cybersecurity risk management at entity level

28.1 Paragraph 1

Each high-impact and critical-impact entity as identified by the competent authorities pursuant to Article 24(1) shall perform cybersecurity risk management for all its assets in its high-impact and critical-impact perimeters. Each high-impact and critical-impact entity shall perform risk management containing the phases in paragraph 2 every three years.

Relevant NCCS Articles

- Article 24(1)
- Article 26(2)

Other NCCS Articles

- Article 23
- Article 19(2)
- Article 19(3)
- Article 26(3)
- Article 28(1)

Input

- Union wide high impact and critical impact processes
- Risk matrix
- Comprehensive cross-border electricity cybersecurity risk assessment report
- ECII
- Risk acceptance criteria
- Cybersecurity controls
- Cybersecurity framework

Output

- Entitiy level risk assessment report
- Asset inventory

GOOD TO KNOW

Recurrence

> 3 years

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

28.2 Paragraph 2

> Each high-impact and critical-impact entity shall base its cybersecurity risk management on an approach that aims to protect their network and information systems and that comprises the following phases:
>
> a. context establishment;
> b. cybersecurity risk assessment at entity level;
> c. cybersecurity risk treatment;
> d. cybersecurity risk acceptance.

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

28.3 Paragraph 3

During the context establishment phase, each high-impact and critical-impact entity shall:

a. define the scope of the cybersecurity risk assessment including the high-impact and critical-impact processes identified by the ENTSO for Electricity and the EU DSO entity, and other processes that may be targets of cyber- attacks with a high-impact or critical-impact on cross-border electricity flows; and

b. define the criteria for risk evaluation and for risk acceptance in accordance with the risk impact matrix that entities and the competent authorities shall use to assess the cybersecurity risks in the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by the ENTSO for Electricity and the EU DSO entity in accordance with Article 19(2).

Relevant NCCS Articles

- Article 19(2)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

28.4 Paragraph 4

During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

a. identify cybersecurity risks by taking into account:
    a. all assets supporting the Union-wide high-impact and critical-impact processes with an assessment of the possible impact on cross-border electricity flows if the asset is compromised;
    b. possible cyber threats taking into account the cyber threats identified in the latest Comprehensive cross- border electricity cybersecurity risk assessment report referred to in Article 23 and supply chain threats;
    c. vulnerabilities, including vulnerabilities in legacy systems;
    d. possible cyber-attack scenarios, including cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows;
    e. relevant risk evaluations and assessments carried out at Union level, including coordinated risk assessments of critical supply chains in accordance with Article 22 of Directive (EU) 2022/2555 [a]; and
    f. existing implemented controls;
b. analyse the likelihood and consequences of the cybersecurity risks identified in point (a) and determine the cybersecurity risk level using the risk impact matrix used to assess cybersecurity risks in cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity in accordance with Article 19(2);
c. classify assets according to the possible consequences when cybersecurity is compromised and determine the high- impact and critical-impact perimeter using the following steps:
    a. perform, for all processes covered by the cybersecurity risk assessment, a business impact assessment using the ECII;
    b. classify a process as high-impact or critical-impact if its ECII is above the high-impact or critical-impact threshold respectively;
    c. determine all high-impact and critical-impact assets as the assets needed for the high-impact and critical- impact processes respectively;
    d. define the high-impact and critical-impact perimeters containing all high-impact and critical-impact assets respectively, so that access to the perimeters may be controlled;
d. evaluate cybersecurity risks by prioritising them through risk evaluation criteria and risk acceptance criteria referred to in paragraph 3 point (b).

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_22

Relevant NCCS Articles

- Article 23
- Article 19(2)
- Article 26(3)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

28.5 Paragraph 5

During the cybersecurity risk treatment phase, each high-impact and critical-impact entity shall establish an entity- level risk mitigation plan by selecting risk treatment options appropriate to manage the risks and identify the residual risks.

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

28.6 Paragraph 6

During the cybersecurity risk acceptance phase, each high-impact and critical-impact entity shall decide whether to accept the residual risk based on the risk acceptance criteria established in paragraph 3 point (b).

Relevant NCCS Articles

- Article 26(3)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

28.7 Paragraph 7

Each high-impact and critical-impact entity shall register the assets identified in paragraph 1 in an asset inventory. That asset inventory shall not be part of the risk assessment report.

Relevant NCCS Articles

- Article 26(1)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

28.8 Paragraph 8

The competent authority may inspect the assets in the inventory during inspections.

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

Chapter 29

Article 27: Reporting on the risk assessment at entity level

29.1 Paragraph 1 (/1)

Each high-impact and critical-impact entity shall, within 12 months after the notification of the high-and critical-impact entities pursuant to Article 24(6), and every three years thereafter, provide to the competent authority a report containing the following information: (1) a list of controls selected for the entity-level risk mitigation plan pursuant to Article 26(5) with the current implementation status of each control; (2) for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity, and availability of information and relevant assets. The estimate of this risk shall be given in accordance with the risk impact matrix in Article 19(2); (3) a list of critical ICT service providers for their critical-impact processes.

Relevant NCCS Articles

- Article 24(6)
- Article 26(5)
- Article 19(2)

Output

- Entity level risk assessment

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

No later than June 2030

A

Accountable: HIE, CIE, TSO

Involved Stakeholders

R

Responsible: HIE, CIE, TSO

I

Informed: NCA

Chapter 30

Article 28: Composition, functioning and review of the common electricity cybersecurity framework

30.1 Paragraph 1 (/2)

The common electricity cybersecurity framework shall be composed of the following controls and cybersecurity management system:

a. the minimum cybersecurity controls, developed in accordance with Article 29;

b. the mapping matrix, developed in accordance with Article 34, that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks;

c. the cybersecurity management system established pursuant to Article 32.

Relevant NCCS Articles

- Article 29
- Article 34

- Article 32

Accountable: HIE, NCA

Involved Stakeholders

Responsible: HIE, NCA

30.2 Paragraph 1 (/3)

The common electricity cybersecurity framework shall be composed of the following controls and cybersecurity management system:

a. the minimum cybersecurity controls, developed in accordance with Article 29;

b. the advanced cybersecurity controls, developed in accordance with Article 29;

c. the mapping matrix, developed in accordance with Article 34, that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks;

d. the cybersecurity management system established pursuant to Article 32.

Relevant NCCS Articles

- Article 29
- Article 34

- Article 32

Accountable: CIE, TSO, NCA

Involved Stakeholders

Responsible: CIE, TSO, NCA

30.3 Paragraph 2

All high-impact entities shall apply the minimum cybersecurity controls pursuant to paragraph 1 point (a) within their high-impact perimeter.

Relevant NCCS Articles

- Article 28(1)

Accountable: HIE

Involved Stakeholders

Responsible: HIE

30.4 Paragraph 3

All critical-impact entities shall apply the minnimal and advanced cybersecurity controls pursuant to paragraph 1 point (b) within their critical-impact perimeter.

Relevant NCCS Articles

- Article 28(1)

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

30.5 Paragraph 4

Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the common electricity cybersecurity framework referred to in paragraph 1 shall be supplemented by the minimum and advanced cybersecurity controls in the supply chain developed pursuant to Article 33.

Relevant NCCS Articles

- Article 19(4)
- Article 28(1)
- Article 33

Output

- Unios wide risk assessment with supply chain controls

GOOD TO KNOW

Timing

Not later than October 2026

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Chapter 31

Article 29: Minimum and advanced cybersecurity controls

31.1 Paragraph 1

Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall develop a proposal for minimum and advanced cybersecurity controls.

Relevant NCCS Articles

- Article 19(4)

Other NCCS Articles

- Article 46

Input

- Union wide risk assessment
- Controls about information security

Output

- Minimum and advanced controls (draft)

> GOOD TO KNOW
>
> **Timing**
>
> Not later than October 2026

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

31.2 Paragraph 2

Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall propose an amendment to the competent authority for the minimum and advanced cybersecurity controls. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Relevant NCCS Articles

- Article 21(2)
- Article 8(10)

Input

- Regional level risk assessment

Output

- Minimum and advanced controls

GOOD TO KNOW

Timing

No later than June 2031

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: NCA

31.3 Paragraph 3

The minimum and advanced cybersecurity controls shall be verifiable by taking part in a national verification scheme in accordance with the procedure set out in Article 31 or by undergoing independent third-party security audits performed according to the requirements listed in Article 25(2).

Relevant NCCS Articles

- Article 31
- Article 25(2)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

31.4 Paragraph 4

The initial minimum and advanced cybersecurity controls developed pursuant to paragraph (1) shall be based on the risks that are identified in the Union-wide cybersecurity risk assessment report referred to in Article 19(5). The amended minimum and advanced cybersecurity controls developed pursuant to paragraph (2) shall be based on the regional cybersecurity risk assessment report referred to in Article 21(2).

Relevant NCCS Articles

- Article 29(1)
- Article 19(5)
- Article 29(2)
- Article 21(2)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

31.5 Paragraph 5

The minimum cybersecurity controls shall include controls to protect the information exchanged pursuant to Article 46.

Relevant NCCS Articles

- Article 46

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: NCA

31.6 Paragraph 6 (/1)

Within 12 months after the approval of the minimum and advanced cybersecurity controls pursuant to Article 8(5), or after each update pursuant to Article 8(10), the entities listed in Article 2(1) and identified as critical-impact and high- impact entities pursuant to Article 24 shall, during the establishment of the entity-level risk mitigation plan pursuant to Article 26(5), apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Relevant NCCS Articles

- Article 8(5)
- Article 8(10)
- Article 2(1)
- Article 24
- Article 26(5)

Input

- Minimum controls

Output

- Minimum and advanced controls

GOOD TO KNOW

Timing

12 months

Accountable: HIE

Involved Stakeholders

Responsible: HIE

31.7 Paragraph 6 (/2)

Within 12 months after the approval of the minimum and advanced cybersecurity controls pursuant to Article 8(5), or after each update pursuant to Article 8(10), the entities listed in Article 2(1) and identified as critical-impact and high- impact entities pursuant to Article 24 shall, during the establishment of the entity-level risk mitigation plan pursuant to Article 26(5), apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Relevant NCCS Articles

- Article 8(5)
- Article 8(10)

- Article 2(1)
- Article 24
- Article 26(5)

Input

- Minimum and advanced controls

Output

- Advanced controls

> 
> GOOD TO KNOW
>
> **Timing**
>
> 12 months

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

Chapter 32

Article 30: Derogations from the minimum and advanced cybersecurity controls

32.1 Paragraph 1 (/1)

The entities listed in Article 2(1) may request the respective competent authority to grant a derogation from their obligation to apply the minimum and advanced cybersecurity controls referred to in Article 29(6).

Relevant NCCS Articles

- Article 2(1)
- Article 29(6)

Other NCCS Articles

- Article 29(3)

Input

- Derogation from controls

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

32.2 Paragraph 1 (/2)

The entities listed in Article 2(1) may request the respective competent authority to grant a derogation from their obligation to apply the minimum and advanced cybersecurity controls referred to in Article 29(6). The competent authority may grant such a derogation on one of the following grounds:

a. in exceptional circumstances, where the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefits. ACER and the ENTSO for Electricity in cooperation with the DSO entity may jointly develop a guidance for estimating the costs of cybersecurity controls to help the entities;

b. where the entity provides an entity-level risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable in accordance with to

the risk acceptance criteria referred to Article 26(3), point (b).

Relevant NCCS Articles

- Article 26(3)

Accountable: NCA

Involved Stakeholders

Responsible: NCA

32.3 Paragraph 2

Within three months from the receipt of the request referred to in paragraph 1, each competent authority shall decide whether a derogation from the minimum and advanced cybersecurity controls is to be granted. Derogations from the minimum or advanced cybersecurity controls shall be granted for a maximum of three years, with the possibility of renewal.

Relevant NCCS Articles

- Article 30(1)

Output

- Authorization for deviation from controls

> GOOD TO KNOW
>
> **Recurrence**
>
> 3 years

> GOOD TO KNOW
>
> **Timing**
>
> 3 months

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: HIE, CIE, TSO

32.4 Paragraph 3

Aggregated and anonymised information for the derogations granted shall be included as an annex to the comprehensive cross-border electricity cybersecurity risk assessment report referred to in Article 23. The ENTSO for Electricity and the EU DSO entity shall jointly update the list, where necessary.

Relevant NCCS Articles

- Article 23

Input

- Authorization for deviation from controls

Output

- Common cybersecurity risk assessment of the electrical energy sector

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Chapter 33

Article 31: Verification of the common electricity cybersecurity framework

33.1 Paragraph 1

No later than 24 months after the adoption of the controls referred to in points (a), (b) and (c) of Article 28(1) and the establishment of the cybersecurity management system referred to in point (d) of that Article, each critical-impact entity identified in accordance with Article 24(1) shall be able to demonstrate its compliance with the cybersecurity management system and the minimum or advanced cybersecurity controls at the request of the competent authority.

Relevant NCCS Articles

- Article 28(1)
- Article 24(1)

Output

- Verification of compliance with controls

GOOD TO KNOW

Timing

24 months

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO, NCA

33.2 Paragraph 2

Each critical-impact entity shall fulfil the obligation referred to in paragraph 1 by undergoing independent third- party security audits in accordance with the requirements listed in Article 25(2) or by taking part in a national verification scheme in accordance with Article 25(1).

Relevant NCCS Articles

- Article 25(2)
- Article 25(1)
- Article 31(1)

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

Informed: NCA

33.3 Paragraph 3

The verification that a critical-impact entity complies with the cybersecurity management system and the minimum or advanced cybersecurity controls shall cover all assets within the critical-impact perimeter of the critical-impact entity.

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

Informed: NCA

33.4 Paragraph 4

The verification that a critical-impact entity complies with the cybersecurity management system and the minimum or advanced cybersecurity controls shall be regularly repeated at the latest 36 months after the end of the first verification, and every 3 years thereafter.

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

36 months

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

Informed: NCA

33.5 Paragraph 5

Each critical-impact entity defined in accordance with Article 24 shall demonstrate its compliance with the controls referred to in points (a), (b) and (c) of Article 28(1) and the establishment of the cybersecurity management system referred to in point (d) of that Article by reporting on the outcome of the compliance verification to the competent authority.

Relevant NCCS Articles

- Article 24
- Article 28(1)

Output

- Report on audit results

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

Informed: NCA

Chapter 34

Article 32: Cybersecurity management system

34.1 Paragraph 1

Within 24 months after being notified by the competent authority that they have been identified as a high-impact or critical-impact entity in accordance with Article 24(6), each high-impact and critical-impact entity shall establish a cybersecurity management system, and review it every three years thereafter, to:

a. determine the scope of the cybersecurity management system considering interfaces and dependencies with other entities;

b. ensure that all its senior management is informed of relevant legal obligations and actively contributes to the implementation of the cybersecurity management system through timely decisions and prompt reactions;

c. ensure that the resources needed for the cybersecurity management system are available;

d. establish a cybersecurity policy that shall be documented and communicated within the entity and to parties affected by the security risks;

e. assign and communicate responsibilities for roles relevant to cybersecurity;

f. perform cybersecurity risk management at entity level as defined in Article 26;

g. determine and provide the resources required for the implementation, maintenance and continual improvement of the cybersecurity management system, taking into account the necessary competence and awareness of cybersecurity resources;

h. determine the internal and external communication that is relevant to cybersecurity;

i. create, update and control documented information related to the cybersecurity management system;

j. evaluate the performance and effectiveness of the cybersecurity management system;

k. conduct internal audits at planned intervals to ensure that the cybersecurity management system is effectively implemented and maintained;

l. review the implementation of the cybersecurity management system at planned intervals; and control and correct non-compliance of the resources and activities with the policies, procedures, guidelines in the cybersecurity management system.

Relevant NCCS Articles

- Article 24(6)
- Article 26

Input

- International standards

Output

- Cybersecurity framework

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

24 months

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

34.2 Paragraph 2

The scope of the cybersecurity management system shall include all assets within the high-impact perimeter of the high-impact entity.

Accountable: HIE

Involved Stakeholders

Responsible: HIE

34.3 Paragraph 3

The competent authorities shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or international standards and specifications related to management systems and relevant to the security of network and information systems.

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

Chapter 35

Article 33: Minimum and advanced cybersecurity controls in the supply chain

35.1 Paragraph 1

Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop a proposal for minimum and advanced cybersecurity controls in the supply chain that mitigate the supply chain risks identified in the Union-wide cybersecurity risk assessments, supplementing the minimum and advanced cybersecurity controls developed pursuant to Article 29. The minimum and advanced cybersecurity controls in the supply chain shall be developed together with the minimum and advanced cybersecurity controls pursuant to Article 29. The minimum and advanced cybersecurity controls in the supply chain shall cover the entire lifecycle of all ICT products, ICT services and ICT processes inside the high-impact or critical-impact perimeters of a high-impact or critical-impact entity. The NIS Cooperation Group shall be consulted when developing the proposal for minimum and advanced cybersecurity controls in the supply chain.

Relevant NCCS Articles

- Article 19(4)
- Article 29

Input

- Minimum and advanced cybersecurity controls

Output

- Minimum and advanced cybersecurity controls in supply chain (draft)

> 
> GOOD TO KNOW
>
> **Timing**
>
> Within 7 months after submitting the first draft of the EU-wide cybersecurity risk assessment report

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: NIS CG

35.2 Paragraph 2

The minimum cybersecurity controls in the supply chain shall consist of controls for high-impact and critical-impact entities that:

a. include recommendations for the procurement of ICT products, ICT services, and ICT processes referring to cybersecurity specifications, covering at least:

   i. the background verification checks of the staff of the supplier involved in the supply chain and dealing with sensitive information or with access to the high-impact or critical-impact assets of the entity. Background verification check may include a verification of the identity and background of staff or contractors of an entity in accordance with national law and procedures and relevant and applicable Union law, including Regulation (EU) 2016/679 [a] and Directive (EU) 2016/680 of the European Parliament and of the Council(18) [b]. Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the entity concerned. They need to be proportional to business requirements, the classification of the information to be accessed and the perceived risks, and may be performed by the entity itself, by an external company performing a screening, or through a government clearing;

   ii. the processes for secure and controlled design, development and production of ICT products, ICT services and ICT processes, promoting the design and development of ICT products, ICT services, and ICT processes, which include appropriate technical measures to ensure cybersecurity;

   iii. design of network and information systems in which devices are not trusted even when they are within a secure perimeter, require verification of all requests they receive and apply the least privilege principle;

   iv. the access of the supplier to the assets of the entity;

   v. the contractual obligations on the supplier to protect and restrict access to the entity's sensitive information;

   vi. the underpinning cybersecurity procurement specifications to subcontractors of the supplier;

   vii. the traceability of the application of the cybersecurity specifications from the development through production until delivery of ICT products, ICT services or ICT processes;

   viii. the support for security updates throughout the entire lifetime of ICT products, ICT services or ICT processes;

   ix. the right to audit cybersecurity in the design, development and production processes of the supplier; and

   x. the assessment of the risk profile of the supplier;

a. require such entities to take into account the procurement recommendations referred to in subparagraph (a) when concluding contracts with suppliers, collaboration partners

and other parties in the supply chain, covering ordinary deliveries of ICT products, ICT services and ICT processes as well as unsolicited events and circumstances like termination and transition of contracts in cases of negligence of the contractual partner;

b. require such entities to take into account the results of relevant coordinated security risk assessments of critical

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO, CRITICAL ICT

35.3 Paragraph 3 (/1)

For the cybersecurity specifications in the cybersecurity procurement recommendation referred to in paragraph 2, point (a), high-impactentities shall use the principles of procurement pursuant to Directive 2014/24/EU of the European Parliament and of the Council(19) [a], in accordance with Article 35(4), or define their own specifications based on the results of the cybersecurity risk assessment at entity level.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0024#d1e3478-65-1

Relevant NCCS Articles

- Article 33(2)

- Article 35(4)

Accountable: HIE

Involved Stakeholders

Responsible: HIE

35.4 Paragraph 3 (/2)

For the cybersecurity specifications in the cybersecurity procurement recommendation referred to in paragraph 2, point (a), critical entities shall use the principles of procurement pursuant to Directive 2014/24/EU of the European Parliament and of the Council(19) [a], in accordance with Article 35(4), or define their own specifications based on the results of the cybersecurity risk assessment at entity level.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0024#d1e3478-65-1

Relevant NCCS Articles

- Article 33(2)
- Article 35(4)

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

35.5 Paragraph 4

The advanced cybersecurity controls in the supply chain shall include controls for critical-impact entities to verify, during procurement, that ICT products, ICT services and ICT processes that will be used as critical-impact assets satisfy the cybersecurity specifications. The ICT product, ICT service or ICT process shall be verified either through a European cybersecurity certification scheme referred to in Article 31 or through verification activities selected and organised by the entity. The depth and coverage of the verification activities shall be sufficient to provide assurance that the ICT product, ICT service or ICT process can be used to mitigate the risks identified in the risk assessment at entity level. The critical-impact entity shall document the steps taken to reduce the risks identified.

Relevant NCCS Articles

- Article 36

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

35.6 Paragraph 5 (/1)

The minimum cybersecurity controls in the supply chain shall apply to the procurement of relevant ICT product, ICT services and ICT processes. The minimum cybersecurity controls of the supply chain will apply to procurement processes in the entities identified as high-impact entities pursuant to Article 24 that starts six months after the adoption or update of the minimum cybersecurity controls referred to in Article 29.

Relevant NCCS Articles

- Article 24
- Article 29

Input

- Minimum and advanced cybersecurity controls

Output

- Minimum and advanced cybersecurity controls applied

GOOD TO KNOW

Timing

> Six months after the adoption or update of minimum and advanced cybersecurity controls

Accountable: HIE

Involved Stakeholders

Responsible: HIE

35.7 Paragraph 5 (/2)

The minimum and advanced cybersecurity controls in the supply chain shall apply to the procurement of relevant ICT product, ICT services and ICT processes. The minimum and advanced cybersecurity controls of the supply chain will apply to procurement processes in the entities identified as critical-impact entities pursuant to Article 24 that starts six months after the adoption or update of the minimum and advanced cybersecurity controls referred to in Article 29.

Relevant NCCS Articles

- Article 24
- Article 29

Input

- Minimum and advanced cybersecurity controls

Output

- Minimum and advanced cybersecurity controls in supply chain

> GOOD TO KNOW
>
> **Timing**
>
> Six months after the adoption or update of minimum and advanced cybersecurity controls

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

35.8 Paragraph 6

Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall propose an amendment to the competent authority for the minimum and advanced cybersecurity controls in the supply chain. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Relevant NCCS Articles

- Article 21(2)
- Article 8(10)

Input

- Minimum and advanced cybersecurity controls

Output

- minimum and advanced cybersecurity controls (modified)

GOOD TO KNOW

Timing

Within 6 months after the preparation of regional cybersecurity risk assessment report

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: NCA

Chapter 36

Article 34: Mapping matrix for electricity cybersecurity controls against standards

36.1 Paragraph 1 (/1)

Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity and in consultation with ENISA, shall develop a proposal for a matrix to map the controls set out in Article 28(1), points (a) and (b) against selected European and international standards as well as relevant technical specifications ('the mapping matrix'). The ENTSO for Electricity and the EU DSO entity shall document the equivalence of the different controls with the controls set out in Article 28(1), points (a) and (b).

Relevant NCCS Articles

- Article 19(4)
- Article 28(1)

Input

- National standars and controls
- Temporary list of European and international standards and controls

Output

- Mapping matrix (draft)

GOOD TO KNOW

Timing

Within 7 months after submitting the first draft of the cybersecurity risk assessment report

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: ENISA

36.2 Paragraph 1 (/2)

The ENTSO for Electricity and the EU DSO entity shall document the equivalence of the different controls with the controls set out in Article 28(1), points (a) and (b).

Relevant NCCS Articles

- Article 28(1)

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

36.3 Paragraph 2 (/1)

The competent authorities may provide to the ENTSO for Electricity and the EU DSO entity a mapping of the controls set out in Article 28(1), points (a) and (b) with a reference to the related national legislative or regulatory frameworks, including relevant national standards of Member States pursuant to Article 25 of Directive (EU) 2022/2555 [a]. If the competent authority of a Member State provides such a mapping,

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1733994458451#art_25

Relevant NCCS Articles

- Article 28(1)

Accountable: NCA

Involved Stakeholders

Responsible: ENTSO-E, EU DSO, NCA

36.4 Paragraph 2 (/2)

the ENTSO for Electricity and the EU DSO entity shall integrate this national mapping into the mapping-matrix.

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO, NCA

36.5 Paragraph 3

Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity and in consultation with ENISA, shall propose an amendment to the competent authority for mapping matrix. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Relevant NCCS Articles

- Article 21(2)
- Article 8(10)

Output

- Mapping matrix (suggestion for modification)

GOOD TO KNOW

Timing

Within 6 months after the preparation of regional cybersecurity risk assessment reports

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: ENISA

Informed: NCA

Chapter 37

Article 35: Cybersecurity procurement recommendations

37.1 Paragraph 1

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop, in a work programme to be established and updated each time a regional cybersecurity risk assessment report is adopted, sets of non-binding cybersecurity procurement recommendations that high-impact and critical-impact entities may use as a basis for the procurement of ICT products, ICT services and ICT processes in the high-impact and critical-impact perimeters. This work programme shall include the following:

a. a description and classification of the types of ICT products, ICT services and ICT processes used by high-impact and critical-impact entities in the high-impact and critical-impact perimeter;

b. a list of the types of ICT products, ICT services, and ICT processes for which a set of non-binding cybersecurity recommendations shall be developed based on the relevant regional cybersecurity risk assessment reports and on the priorities of high-impact and critical-impact entities.

Input

- Provisional list of European and international standards and controls
- Regional cybersecurity risk assessment report

Output

- Recommendations for cybersecurity procurement

> GOOD TO KNOW
>
> **Timing**
>
> 6 months after the approval or update of the regional cybersecurity risk assessment report

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Informed: HIE, CIE

37.2 Paragraph 2

The ENTSO for Electricity, in cooperation with the EU DSO entity, shall, within 6 months after the adoption or update of the regional cybersecurity risk assessment report provide ACER with a summary of that work programme.

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: ACER

37.3 Paragraph 3

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall endeavour to ensure that the non-binding cybersecurity procurement recommendations developed based on the relevant regional cybersecurity risk assessment are similar or comparable across system operation regions. The sets of cybersecurity procurement recommendations shall cover at least the specifications referred to in Article 33(2), point (a). Where possible, the specifications shall be selected from European and international standards.

Relevant NCCS Articles

- Article 33(2)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

37.4 Paragraph 4

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall ensure that the sets of cybersecurity procurement recommendations:

a. comply with the principles of procurement pursuant to Directive 2014/24/EU; and

b. are compatible with and take into account the most recent available European cybersecurity certification schemes relevant to the ICT product, ICT service, or ICT process.

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Chapter 38

Article 36: Guidance on use of European cybersecurity certification schemes for procurement of ICT products, ICT services and ICT processes

38.1 Paragraph 1

The non-binding cybersecurity procurement recommendations developed pursuant to Article 35 may include sector-specific guidance on the use of European cybersecurity certification schemes, whenever a suitable scheme is available for a type of ICT product, ICT service or ICT process used by critical-impact entities, without prejudice to the framework for the establishment of European cybersecurity certification schemes pursuant to Article 46 of Regulation (EU) 2019/881. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881#d1e3205-15-1

Relevant NCCS Articles

- Article 35

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

38.2 Paragraph 2

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall closely cooperate with ENISA in providing the sector-specific guidance included in non-binding cybersecurity procurement recommendations pursuant to paragraph 1.

Relevant NCCS Articles

- Article 36(1)

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, ENISA, EU DSO

Chapter 39

Article 37: Rules on information sharing

39.1 Paragraph 1 (/1)

If a competent authority receives information related to a reportable cyber-attack, that competent authority: (a) shall assess the level of confidentiality of that information and inform the entity about the outcome of its assessment without undue delay and not later than within 24 hours of receipt of the information;

Input

- Cyberattack classification scale
- Detected cyberattack

Output

- Assessed information related to cyberattacks

GOOD TO KNOW

Timing

No later than 24 hours after notification

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: HIE, CIE, ENISA, CSIRT, CS NCA

39.2 Paragraph 1 (/2)

(b) shall attempt to find any other similar cyber-attack in the Union reported to other competent authorities, in order to correlate the information received in the context of the reportable cyber-attack with information provided in the context of other cyber-attacks and enrich existing information, strengthen and coordinate cybersecurity responses;

Accountable: NCA

Involved Stakeholders

Responsible: NCA

39.3 Paragraph 1 (/3)

(c) shall be responsible for the removal of business secrets and the anonymisation of the information in accordance with the relevant national and Union rules;

Accountable: NCA

Involved Stakeholders

Responsible: NCA

39.4 Paragraph 1 (/4)

(d) shall share the information with the national single points of contact, CSIRTs and all competent authorities designated pursuant to Article 4 in other Member States without undue delay and no later than 24 hours after the reception of a reportable cyber-attack and provide updated information on a regular basis to those authorities or bodies;

Relevant NCCS Articles

- Article 4

Input

- Assessed information related to cyberattacks

Output

- Sharing information related to cyberattacks

GOOD TO KNOW

Timing

No later than 24 hours after notification

Accountable: NCA

Involved Stakeholders

Responsible: NCA

39.5 Paragraph 1 (/5)

(e) shall disseminate the information of the cyber-attack, after anonymisation and removal of business secrets pursuant to paragraph 1(c), to critical-impact and high-impact entities in its Member State without undue delay and no later than 24 hours after receiving information according to paragraph 1(a), and provide updated information on a regular basis allowing the entities to organise their defence effectively;

Relevant NCCS Articles

- Article 37(1)

Input

- Assessed information related to cyberattacks

Output

- Sharing information related to cyberattacks

GOOD TO KNOW

Timing

No later than 24 hours after notification

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: HIE, CIE

39.6 Paragraph 1 (/6)

(f) may request the reporting high-impact or critical-impact entity to further disseminate the reportable cyber-attack information in a secure manner to other entities that may be affected, with the aim to generate situational awareness by the electricity sector and to prevent the materialisation of a risk that may escalate in a cross-border cybersecurity electricity incident;

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

39.7 Paragraph 1 (/7)

(g) shall share with ENISA a summary report, after anonymisation and removal of business secrets, with the information of the cyber-attack.

Input

- Assessed information related to cyberattacks

Output

- Sharing information related to cyberattacks

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: ENISA

39.8 Paragraph 2

If a CSIRT becomes aware of an unpatched actively exploited vulnerability, it shall:

a. share it with ENISA via an appropriate secure information exchange channel without delay, unless otherwise specified in other Union law;

b. support the concerned entity to receive from the manufacturer or provider an effective, coordinated and rapid management of the unpatched actively exploited vulnerability or of effective and efficient mitigation measures;

c. share available information with the vendor and request the manufacturer or provider, where possible, to identify a list of CSIRTs in Member States concerned by the unpatched actively exploited vulnerability and that shall be informed;

d. share available information with the CSIRTs identified under the previous point, based on need-to-know principle;

e. share, where they exist, mitigation strategies and measures to the reported unpatched actively exploited vulnerability.

Input

- Detected unpatched, actively exploited vulnerability

Output

- Sharing information related to unpatched, actively exploited vulnerabilities

GOOD TO KNOW

Timing

Immediately

Accountable: CSIRT

Involved Stakeholders

Responsible: CSIRT

Informed: HIE, CIE, ENISA, CRITICAL ICT

39.9 Paragraph 3

If a competent authority becomes aware of an unpatched actively exploited vulnerability, that competent authority shall:

a. share, where they exist, mitigation strategies and measures to the reported unpatched actively exploited vulnerability, in coordination with the CSIRTs in its Member State;

b. shall share the information with a CSIRT in the Member State where the unpatched actively exploited vulnerability has been reported.

Input

- Detected unpatched, actively exploited vulnerability

Output

- Sharing information related to unpatched, actively exploited vulnerabilities

GOOD TO KNOW

Timing

Immediately

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: CSIRT

39.10 Paragraph 4

If the competent authority becomes aware of an unpatched vulnerability, without evidence of yet being actively exploited, it shall without undue delay coordinate with the CSIRT for the purposes of coordinated vulnerability disclosure as laid down in Article 12(1) of Directive (EU) 2022/2555. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_12

Input

- Detected unpatched, actively exploited vulnerability

Output

- Sharing information related to unpatched, actively exploited vulnerabilities

GOOD TO KNOW

Timing

Immediately

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: CSIRT

39.11 Paragraph 5

If a CSIRT receives information related to cyber threats from one or several high-impact or critical-impact entities pursuant to Article 38(6), it shall disseminate that information or any other information of importance for preventing, detecting, responding to or mitigating the related risk to critical-impact and high-impact entities in its Member State and, where appropriate, to all concerned CSIRTs and to its national single point of contact without undue delay and no later than four hours after receiving information.

Relevant NCCS Articles

- Article 38(6)

Input

- Cyberattack classification scale
- Detected cyberattack

Output

- Sharing information related to cyberattacks

GOOD TO KNOW

Timing

Within 4 hours after a cyberattack

Involved Stakeholders

Responsible: HIE, CIE, TSO

Consulted: CSIRT

39.12 Paragraph 6

If a competent authority becomes aware of information related to cyber threats from one or several high-impact or critical-impact entities, it shall forward this information to the CSIRT for the purpose of paragraph 5.

Relevant NCCS Articles

- Article 37(5)

Input

- Cyberattack classification scale
- Detected cyberattack

Output

- Sharing information related to cyberattacks

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: CSIRT

39.13 Paragraph 7

The competent authorities may delegate in full or in part the responsibilities under paragraphs 3 and 4 concerning one or more high-impact or critical-impact entities that operate in more than one Member State to another competent authority in one of those Member States, following an agreement among the concerned competent authorities.

Relevant NCCS Articles

- Article 37(3)
- Article 37(4)

Accountable: NCA

Involved Stakeholders

Responsible: NCA

39.14 Paragraph 8

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall develop a cyber-attack classification scale methodology by 13 June 2025. The TSOs, with the assistance of the ENTSO for Electricity and the EU DSO entity may request the competent authorities to consult ENISA and their competent authorities responsible for cybersecurity for assistance in the development of such classification scale. The methodology shall provide the classification for the gravity of a cyber-attack according to five levels, the two highest levels being 'high' and 'critical'. The classification shall be based on the assessment of the following parameters:

a. the potential impact considering the assets and perimeters exposed determined in accordance with Article 26(4), point (c); and

b. the severity of the cyber-attack.

Relevant NCCS Articles

- Article 26(4)

Output

- Cyberattack classification scale

GOOD TO KNOW

Timing

By 13 June 2025

Accountable: TSO

Involved Stakeholders

Responsible: ENTSO-E, TSO, EU DSO

Consulted: ENISA

39.15 Paragraph 9

By 13 June 2026, the ENTSO for Electricity, in collaboration with the EU DSO entity, shall perform a feasibility study to assess the possibility and the financial costs necessary to develop a common tool enabling all entities to share information with relevant national authorities.

Output

- Feasibility study of an information-sharing tool

GOOD TO KNOW

Timing

> By June 2026

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

39.16 Paragraph 10

The feasibility study shall address the possibility for such a common tool to:

a. support critical-impact and high-impact entities with relevant security related information for operations of cross- border electricity flows, such as near real-time reporting of cyber-attacks, early alerts related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system;

b. be maintained in a suitable and highly trustable environment;

c. allow for data collection from critical-impact and high-impact entities and facilitate removal of confidential information and anonymisation of the data and their prompt dissemination to critical-impact and high-impact entities.

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

39.17 Paragraph 11

The ENTSO for Electricity, in cooperation with the EU DSO entity, shall:

a. consult ENISA and the NIS Cooperation Group, the national single points of contact and the representatives of main stakeholders when assessing the feasibility;

b. present the results of the feasibility study to ACER and the NIS Cooperation Group.

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: ENISA, NCA, NIS CG

Informed: ACER

39.18 Paragraph 12

The ENTSO for Electricity, in cooperation with the EU DSO entity may analyse and facilitate initiatives proposed by critical-impact and high-impact entities to evaluate and test such tools for information sharing.

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Chapter 40

Article 38: Role of high-impact and critical-impact entities as regards information sharing

40.1 Paragraph 1

Each high-impact and critical-impact entity shall: (a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

a. ensure that the relevant network and information systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on cyber-attacks;

b. conduct security monitoring, including detecting intrusions and assessing vulnerabilities of network and information systems;

c. analyse and, if necessary, take all actions required under its responsibility and capacity to protect the entity;

d. participate in the information collection and sharing described in this Article;

    a. have the right to procure all or parts of these capabilities pursuant to point (a) through MSSPs. Critical-impact and high-impact entities shall remain responsible for MSSPs and supervise their efforts;

    b. designate a single point of contact at entity level for the purpose of information sharing.

Relevant NCCS Articles

- Article 26(4)

Output

- Established CSOC capability

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

40.2 Paragraph 2

ENISA may issue non-binding guidance on establishing such capabilities or subcontracting the service to MSSPs, as part of the task defined in Article 6(2) of Regulation (EU) 2019/881. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Accountable: ENISA

Involved Stakeholders

Responsible: ENISA

40.3 Paragraph 3

Each critical-impact and high-impact entity shall share relevant information related to a reportable cyber-attack with its CSIRTs and its competent authority without undue delay and no later than four hours of becoming aware that the incident is reportable.

Input

- Cyberattack classification scale
- Detected cyberattack

Output

- Sharing information related to cyberattacks

GOOD TO KNOW

Timing

Within 4 hours after a cyberattack

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: NCA

40.4 Paragraph 4

Information related to a cyber-attack shall be considered reportable when the cyber-attack is assessed by the affected entity resulting in a criticality ranging from 'high' to 'critical' following the cyber-attack classification scale methodology pursuant to Article 37(8). The single point of contact at entity level designated pursuant to paragraph 1 point (c) shall communicate the incident classification.

Relevant NCCS Articles

- Article 37
- Article 38

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

40.5 Paragraph 5

Where critical-impact and high-impact entities notify relevant information related to unpatched actively exploited vulnerabilities to a CSIRT, the latter may forward this information to its competent authority. In light of the level of sensitivity of the notified information, the CSIRT may withhold the information or delay its forwarding based on justified cybersecurity-related grounds.

Input

- Detected unpatched, actively exploited vulnerability

Output

- Detected unpatched, actively exploited vulnerability

GOOD TO KNOW

Timing

NIS 2

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: NCA

40.6 Paragraph 6

Each critical-impact and high-impact entity shall provide without undue delay to its CSIRTs any information related to a reportable cyber threat that may have a cross-border effect. Information related to a cyber threat shall be considered reportable when at least one of the following conditions is met:

a. it provides relevant information for other critical-impact and high-impact entity for preventing, detecting, responding or mitigating the impact of the risk;

b. the identified techniques, tactics and procedures used in the context of an attack lead to information such as compromised URL or IP addresses, hashes or any other attribute useful to contextualise and correlate the attack;

c. a cyber threat may be further assessed and contextualised with additional information provided by service providers or third parties not subject to this Regulation.

Input

- Detected cybersecurity threat

Output

- Sharing information related to cybersecurity threats

GOOD TO KNOW

Timing

Immediately

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

40.7 Paragraph 7

Each critical-impact entity and high-impact entity shall, when sharing information pursuant to this Article, specify the following:

a. that the information is submitted pursuant to this Regulation;

b. whether the information concerns:

i. a reportable cyber-attack referred to in paragraph 3;

ii. unpatched actively exploited vulnerabilities not publicly known referred to in paragraph 4;

iii. a reportable cyber threat referred to in paragraph 5;

a. in the case of a reportable cyber-attack, the level of the cyber-attack according to the cyber-attack classification scale methodology referred to in Article 37(8) and information leading to this classification including at least the criticality of the cyber-attack.

Relevant NCCS Articles

- Article 38(3)
- Article 38(4)
- Article 38(5)
- Article 37(8)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

40.8 Paragraph 8

When a critical or high-impact entity notifies a significant incident pursuant to Article 23 of Directive (EU) 2022/2555 and the incident reporting under that Article contains relevant information as required under paragraph 3 of this Article, the reporting of the entity under Article 23(1) [a] of that Directive shall constitute reporting of information under paragraph 3 of this Article.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#tit_1

Relevant NCCS Articles

- Article 38(3)
- Article 23(1)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

40.9 Paragraph 9

Each critical-impact and high-impact entity shall report to its competent authority or CSIRT by clearly identifying specific information that shall only be shared with the competent authority or CSIRT in cases where the information sharing could be source of a cyber-attack. Each critical-impact and high-impact entity shall have the right to provide a non-confidential version of the information to the competent CSIRT.

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: NCA

Chapter 41

Article 39: Detection of cyber-attacks and handling of related information

41.1 Paragraph 1 (/1)

Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical- impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555 [a]. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_11

Input

- Cyber attack classification scale

Output

- Entity level procedures for handling cyberattacks

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, EU DSO, NCA

41.2 Paragraph 1 (/2)

If a cyber-attack has an effect on cross-border electricity flows, the single points of contact at entity level of affected critical-impact and high-impact entities shall cooperate to share information among them,

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

41.3 Paragraph 2

coordinated by the competent authority of the Member State in which the cyber-attack was first reported.

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

41.4 Paragraph 3

Critical-impact and high-impact entities shall:

a. ensure that their own single point of contact at entity level has access on a need-to-know basis to the information they received from the national single point of contact through their competent authority;

b. unless already done pursuant to Article 3(4) of Directive (EU) 2022/2555, notify the competent authority of the Member State in which they are established and the national single point of contact with a list of their cybersecurity single points of contact at entity level:

    a. from which that competent authority and national single point of contact may expect to receive information about reportable cyber-attacks;

    b. to which competent authorities and national single points of contact may have to provide information;

c. establish cyber-attack management procedures for cyber-attacks, including roles and responsibilities, tasks and reactions based on the observable evolution of the cyber-attack within the critical-impact and high-impact perimeters;

d. test the overall cyber-attack management procedures at least every year by testing at least one scenario affecting directly or indirectly cross-border electricity flows. That annual test may be conducted by critical-impact and high- impact entities during the regular exercises referred to in Article 43. Any live cyber-attack response activity with a consequence classified at least Scale 2, according to the cyber-attack classification scale methodology referred to in Article 37(8) and with a cybersecurity root cause, may serve as an annual test of the cyber-attack response plan.

Relevant NCCS Articles

- Article 43
- Article 37(8)

GOOD TO KNOW

Recurrence

1 year

Accountable: HIE, CIE

Involved Stakeholders

Responsible: HIE, CIE

Informed: NCA

41.5 Paragraph 4

The tasks referred to in paragraph 1 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1

Relevant NCCS Articles

- Article 39(1)

Accountable: MS

Involved Stakeholders

Responsible: MS, RCC

Chapter 42

Article 40: Crisis management

42.1 Paragraph 1

When the competent authority establishes that an electricity crisis is related to a cyber-attack which has an impact on more than one Member State, the competent authorities from the affected Member States, the CS-NCAs, the RP-NCA and the NIS cyber crisis management authorities from the affected Member States shall jointly create an ad hoc cross-border crisis coordination group.

Output

- Ad hoc cross-border crisis coordination group

Accountable: NCA

Involved Stakeholders

Responsible: NCA, RP NCA, CS NCA

42.2 Paragraph 2

The ad hoc cross-border crisis coordination group shall:

a. coordinate the efficient retrieval and further dissemination of all relevant cybersecurity information to the entities involved in the crisis management process;

b. organise the communication between all the entities impacted by the crisis and the competent authorities, in order to reduce overlaps and increase the efficiency in the analyses and technical responses to remedy the simultaneous electricity crises with a cybersecurity root cause;

c. provide, in cooperation with the competent CSIRTs, the expertise required, including operational advice on the implementation of possible mitigation measures to the entities impacted by the incident;

d. notify and provide regular updates on the state of the incident to the Commission and the Electricity Coordination Group, following the protection principles laid down in Article 46;

e. seek advice from relevant authorities, agencies or entities that might be of help to mitigate the electricity crisis.

Relevant NCCS Articles

- Article 46

Involved Stakeholders

Responsible: NCA, RP NCA, CS NCA

Informed: EC, ECG

42.3 Paragraph 3

Where the cyber-attack qualifies or is expected to qualify as a large-scale cybersecurity incident, the ad hoc cross- border crisis coordination group shall immediately inform the national cyber crisis management authorities in accordance with Article 9(1) of Directive (EU) 2022/2555 [a] in the Member States affected by the incident, as well as the Commission and the EU CyCLONe. In such situation, the ad hoc cross-border crisis coordination group shall support the EU CyCLONe concerning sectoral specificities.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_9

Involved Stakeholders

Informed: EC, CS NCA

42.4 Paragraph 4

Critical-impact and high-impact entities shall develop and have at their disposal capabilities, internal guidelines, preparedness plans, and staff to take part in the detection and mitigation of cross-border crisis. The critical-impact or high- impact entity impacted by a simultaneous electricity crisis shall investigate the root cause of such crisis in cooperation with its competent authority to determine the extent to which the crisis is related to a cyber-attack.

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA

42.5 Paragraph 5

The tasks in paragraph 4 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1

Relevant NCCS Articles

- Article 40(4)

Accountable: MS

Involved Stakeholders

Responsible: MS

Chapter 43

Article 41: Cybersecurity Crisis management and response plans

43.1 Paragraph 1

Within 24 months after the notification to ACER of the Union-wide risk assessment report, ACER shall in close cooperation with ENISA, the ENTSO for Electricity, the EU DSO entity, CS-NCAs, competent authorities, RP-NCAs, the NRAs and the NIS national cyber crisis management authorities, develop a Union-level cybersecurity crisis management and response plan for the electricity sector.

Output

- Member state level crisis management and response plan (modified)

GOOD TO KNOW

Timing

Within 24 months after submitting the EU-wide risk assessment report

Accountable: ACER

Involved Stakeholders

Responsible: ENTSO-E, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, NIS CG, CS NCA

43.2 Paragraph 2

Within 12 months after the development by ACER of the Union-level cybersecurity crisis management and response plan for the electricity sector pursuant to paragraph 1, each competent authority shall develop a national cybersecurity crisis management and response plan for cross-border electricity flows taking into account the Union-level cybersecurity crisis management plan and the national risk preparedness plan established in accordance with Article 10 of Regulation (EU) 2019/941 [a]. This plan shall be consistent with the large-scale cybersecurity incident and crisis response plan pursuant to Article 9(4) of Directive (EU) 2022/2555. [b] The competent authority shall coordinate with the critical-impact and high- impact entities and with the RP-NCA in its Member State.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941#d1e928-1-1
[b] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022L2555#art_9

Relevant NCCS Articles

- Article 41(1)

Output

- Union level crisis management and response plan (modified)

GOOD TO KNOW

Timing

Within 12 months after the development of the EU-level cybersecurity crisis management and response plan

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, TSO, NCA, CS NCA

43.3 Paragraph 3

The national large-scale cybersecurity incident and crisis response plan required pursuant to Article 9(4) of Directive (EU) 2022/2555 [a] shall be considered as a national cybersecurity crisis management plan under this Article if it includes crisis management and response provisions for the cross-border electricity flows.

[a] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022L2555#art_9

Accountable: NCA

Involved Stakeholders

Responsible: NCA

43.4 Paragraph 4

The tasks listed in at paragraphs 1 and 2 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943. [a]

[a] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019R0943#d1e3462-54-1

Relevant NCCS Articles

- Article 41(1)
- Article 41(2)

Accountable: MS

Involved Stakeholders

Responsible: MS, RCC

43.5 Paragraph 5

Critical-impact and high-impact entities shall ensure that their cybersecurity-related crisis management processes:

a. have compatible cross-border cybersecurity incident handling procedures as defined in Article 6(8) of Directive (EU) 2022/2555 [a] formally incorporated in their crisis management plans;

b. are part of the general crisis management activities.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_6

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

43.6 Paragraph 6

Within 12 months after the notification of the high-and critical-impact entities pursuant to Article 24(6), and every three years thereafter, critical impact and high-impact entities shall develop a crisis management plan at entity level for a cybersecurity related crisis which shall be included into their general crisis management plans. This plan shall include at least the following:

a. rules of declaration of the crisis as set out in Article 14(2) and (3) of the Regulation (EU) 2019/941; [a]

b. clear roles and responsibilities for crisis management, including the role of other relevant critical-impact and high- impact entities;

c. up-to-date contact information as well as rules for communication and information sharing during a crisis situation including the connection to the CSIRTs.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941#d1e1185-1-1

Relevant NCCS Articles

- Article 24(6)

Output

- Entitiy level crisis management and response plan (included business continuity plan)

GOOD TO KNOW

Recurrence

3 yeras

GOOD TO KNOW

Timing

12 months after identification

A

Accountable: HIE, CIE, TSO

Involved Stakeholders

R

Responsible: HIE, CIE, TSO

43.7 Paragraph 7

The measures for crisis management pursuant to Article 21(2), point (c) of Directive (EU) 2022/2555 [a] shall be considered as a crisis management plan at entity level for the electricity sector under this Article if it includes all requirements listed in paragraph 6.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_21

Relevant NCCS Articles

- Article 41(6)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

43.8 Paragraph 8

The crisis management plans shall be tested during the cybersecurity exercises referred to in Articles 43, 44 and 45.

Relevant NCCS Articles

- Article 43
- Article 44
- Article 45

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

43.9 Paragraph 9

The critical-impact and high-impact entities shall include their crisis management plans at entity level into their business continuity plans for the critical-impact and high-impact processes. The crisis management plans at entity level shall include:

a. processes depending on availability, integrity and reliability of IT services;

b. all business continuity locations including the locations for hardware and software;

c. all internal roles and responsibilities connected to business continuity processes.

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

43.10 Paragraph 10

The critical-impact and high-impact entities shall update their crisis management plans at entity level at least every three years and whenever necessary.

Output

- Entitiy crisis management and response plan (modified)

GOOD TO KNOW

Recurrence

3 years

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

43.11 Paragraph 11

ACER shall update the Union-level cybersecurity crisis management and response plan for the electricity sector developed pursuant to paragraph (1) at least every three years and whenever necessary.

Relevant NCCS Articles

- Article 4(1)

Output

- Union level crisis management and response plan (modified)

GOOD TO KNOW

Recurrence

3 years

Accountable: ACER

Involved Stakeholders

Responsible: ACER

43.12 Paragraph 12

Each competent authority shall update the national cybersecurity crisis management and response plan for cross- border electricity flows developed pursuant to paragraph (2) at least every three years and whenever necessary.

Relevant NCCS Articles

- Article 4(2)

Output

- National cybersecurity crisis management and response plan (modified)

GOOD TO KNOW

Recurrence

3 years

Accountable: NCA

Involved Stakeholders

Responsible: NCA

43.13 Paragraph 13

The critical-impact and high-impact entities shall test their business continuity plans at least once every three years or after major changes in a critical-impact process. The outcome of the business continuity plan tests shall be documented. The critical-impact and high-impact entities may include the test of their business continuity plan in the cybersecurity exercises.

Output

- Business continuity plan (modification)

GOOD TO KNOW

Recurrence

3 years

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

43.14 Paragraph 14

The critical-impact and high-impact entities shall update their business continuity plan when-

ever necessary and at least once every three years taking into account the outcome of the test.

Output

- Test of business continuity plan

GOOD TO KNOW

Recurrence

3 years

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

43.15 Paragraph 15

If a test identifies deficiencies in the business continuity plan, the critical-impact and high-impact entity shall correct those deficiencies within 180 calendar days after the testing and shall conduct a new test to provide evidence that the corrective measures are effective.

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

Entity-level cybersecurity exercise + 180 days

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

43.16 Paragraph 16

Where a critical-impact or high-impact entity cannot correct the deficiencies within 180 calendar days, it shall include the reasons in the report to be provided to its competent authority in accordance with Article 27.

Relevant NCCS Articles

- Article 27

Output

- Entitiy level risk assessment report

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: NCA

Chapter 44

Article 42: Cybersecurity early alert capabilities for the electricity sector

44.1 Paragraph 1 (/1)

The competent authorities shall cooperate with ENISA to develop Electricity Cybersecurity Early Alert Capabilities (ECEAC) as part as the assistance to Member States pursuant to Articles 6(2) and (7) of Regulation (EU) 2019/881. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Accountable: ENISA

Involved Stakeholders

Responsible: ENISA, NCA

44.2 Paragraph 1 (/2)

The ECEAC shall enable ENISA when carrying out the tasks listed in Article 7(7) of Regulation (EU) 2019/881 to:

a. collect voluntary shared information from:
    i. CSIRTs, competent authorities;
    ii. the entities listed in Article 2 of this Regulation;
    iii. any other entity that wants to share relevant information on a voluntary basis;

Relevant NCCS Articles

- Article 2

Output

- ECEAC

Accountable: NCA

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

44.3 Paragraph 1 (/3)

b. assess and classify collected information;

c. assess the information ENISA has access to for identifying cyber risk conditions and relevant indicators for aspects of cross-border electricity flows;

d. identify conditions and indicators that frequently correlate with cyber-attacks within the electricity sector;

e. define whether further analysis and preventive actions shall be taken through assessment and identification of risk factors;

Accountable: ENISA

Involved Stakeholders

Responsible: ENISA

44.4 Paragraph 1 (/4)

f. inform the competent authorities on the identified risks and recommended preventive actions specific to the entities concerned;

g. inform all relevant entities listed in Article 2 on the results of the information assessed in accordance with points (b), (c) and (d) of this paragraph;

Relevant NCCS Articles

- Article 2

Accountable: ENISA

Involved Stakeholders

Responsible: ENISA

Informed: HIE, CIE, ENTSO-E, TSO, ACER, NCA, NRA, RP NCA, CS NCA

44.5 Paragraph 2

h. periodically include the relevant information in the situational awareness report, issued in accordance with Article 7(6) of Regulation (EU) 2019/881; [a]

i. derive, where possible, applicable data that indicates that a potential security breach or cyber-attack ('indicators of compromise') from the collected information.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Accountable: ENISA

Involved Stakeholders

Responsible: ENISA, EU DSO, CS NCA

44.6 Paragraph 3

The CSIRTs shall disseminate the information received from ENISA to the entities concerned without delay, within their tasks defined in Article 11(3), point (b) of Directive (EU) 2022/2555. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_11

Accountable: CSIRT

Involved Stakeholders

Responsible: ENISA, RP NCA, CSIRT, CS NCA

Informed: HIE, CIE, ENTSO-E, TSO, ACER, EU DSO, NCA, NRA

44.7 Paragraph 4 (/1)

ACER shall monitor the effectiveness of the ECEAC. ENISA shall assist ACER by providing all necessary information, pursuant to Articles 6(2) and 7(1) of Regulation (EU) 2019/881.

Accountable: ENISA

Involved Stakeholders

Responsible: ENISA

44.8 Paragraph 4 (/2)

The analysis of this monitoring activity shall be part of the monitoring pursuant to Article 12 [a] of this Regulation.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Relevant NCCS Articles

- Article 12

Accountable: ACER

Involved Stakeholders

Responsible: ACER

Informed: ENISA

Chapter 45

Article 43: Cybersecurity exercises at entity and Member State levels

45.1 Paragraph 1

By 31 December of the year after the notification of critical-impact entities, and every three years thereafter, each critical-impact entity shall perform a cybersecurity exercise including one or more scenarios with cyber-attacks affecting cross-border electricity flows directly or indirectly and related to the risks identified during the cybersecurity risk assessments at Member State and entity levels in accordance with Article 20 and Article 27.

Relevant NCCS Articles

- Article 20
- Article 27

Input

- Member state level risk assessment
- Entitiy level risk assessment

Output

- Entitiy level level exercise

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

By 31 December 2029

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, TSO

45.2 Paragraph 2

By derogation from paragraph 1, the RP-NCA, after consulting the competent authority and the relevant cyber crisis management authority as designated or established in Directive (EU) 2022/2555 under Article 9 [a] may decide to organise a cybersecurity exercise at Member State level as described in paragraph 1 instead of performing the cybersecurity exercise at entity level. In this regard, the competent authority shall inform:

a. all critical-impact entities of its Member State, the NRA, CSIRTs and the CS-NCA at the latest by 30 June of the year preceding the cybersecurity exercise at entity level;

b. each entity that shall participate in the cybersecurity exercise at Member State level at the latest 6 months before the exercise is to take place.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_9

Relevant NCCS Articles

- Article 43(1)

Output

- Member state level exercise

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

6 months before the national-level exercise

Accountable: RP NCA

Involved Stakeholders

Responsible: NCA, RP NCA

Consulted: CS NCA

Informed: CIE

45.3 Paragraph 3

The RP-NCA with the technical support of its CSIRTs, shall organise the cybersecurity exercise described in paragraph 2 at Member State level independently or in the context of a different cybersecurity exercise in that Member State. In order to be able to group these exercises, RP-NCA may postpone the cybersecurity exercise at Member State level referred to in paragraph 1 by one year.

Relevant NCCS Articles

- Article 43(2)
- Article 43(1)

Accountable: RP NCA

Involved Stakeholders

Responsible: CIE, TSO, RP NCA, CSIRT

45.4 Paragraph 4

The cybersecurity exercises at entity level and at Member State level shall be consistent with the national cybersecurity crisis management frameworks in accordance with Article 9(4), point (d) of Directive (EU) 2022/2555. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_9

Accountable: CIE, TSO, RP NCA

Involved Stakeholders

Responsible: CIE, TSO, RP NCA

45.5 Paragraph 5

By 31 December 2026, and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall make available an exercise scenario template to perform the cybersecurity exercises at entity and Member State level referred to in paragraphs 1. This template shall take into account the results of the most recently performed cybersecurity risk assessment at entity and Member State levels and shall include key success criteria. The ENTSO for Electricity and the EU DSO entity shall involve ACER and ENISA in the development of such template.

Relevant NCCS Articles

- Article 43(1)

Input

- Member state level risk assesement report
- Succes critera

Output

- Member state level excercise template
- Entity level excercise template

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

By 31 December 2026

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, ACER, ENISA, EU DSO

Informed: CIE

Chapter 46

Article 44: Regional or cross regional cybersecurity exercises

46.1 Paragraph 1

By 31 December 2029, and every three years thereafter, in each system operation region, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall organise a regional cybersecurity exercise. The critical-impact entities in the system operation region shall participate in the regional cybersecurity exercise. The ENTSO for Electricity, in cooperation with the EU DSO entity, may organise, instead of a regional cybersecurity exercise, a cross regional cybersecurity exercise in more than one system operating regions in the same timeframe. The exercise should take into account other existing cybersecurity risk assessments and scenarios developed at Union level.

Output

- Regional cybersecurity excercise

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

By 31 December 2029

Accountable: ENTSO-E

Involved Stakeholders

Responsible: CIE, ENTSO-E, TSO, EU DSO

46.2 Paragraph 2

ENISA shall support the ENTSO for Electricity and the EU DSO entity in the preparation and organisation of the cybersecurity exercise at regional or at cross-regional level.

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, ENISA, EU DSO

46.3 Paragraph 3

The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the critical-impact entities that shall participate in the regional or cross regional cybersecurity exercise six months before the exercise takes place.

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

6 months before the regional-level exercise

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: CIE

46.4 Paragraph 4

The organiser of a regular cybersecurity exercise at Union level pursuant to Article 7(5) of Regulation (EU) 2019/881 [a], or of any mandatory cybersecurity exercise related to the electricity sector within the same geographic perimeter, may invite the ENTSO for Electricity and the EU DSO entity to participate. In such cases, the obligation in paragraph 1 does not apply, provided that all critical-impact entities in the system operation region take part in the same exercise.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Relevant NCCS Articles

- Article 44(1)

Accountable: ENISA

Involved Stakeholders

Responsible: CIE, ENTSO-E, TSO, ENISA, EU DSO

46.5 Paragraph 5

If the ENTSO for Electricity and the EU DSO entity participate in a cybersecurity exercise referred to in paragraph 4, they may postpone the regional or cross-regional cybersecurity exercise referred to in paragraph 1 by one year.

Relevant NCCS Articles

- Article 44(1)
- Article 44(4)

Accountable: ENTSO-E

Involved Stakeholders

Responsible: CIE, ENTSO-E, TSO, EU DSO

46.6 Paragraph 6

By 31 December 2027, and every three years after that date, the ENTSO for Electricity, in co-ordination with the EU DSO entity, shall make available an exercise template to perform the regional and cross regional cybersecurity exercises. This template shall take into account the results of the most recently performed cybersecurity risk assessment at regional level and shall include key success criteria. The ENTSO for Electricity shall consult the Commission and may seek advice from ACER, ENISA and the Joint Research Centre on the organisation and execution of the regional and cross regional cybersecurity exercises.

Output

- Regional level exercise template

GOOD TO KNOW

Recurrence

3 years

GOOD TO KNOW

Timing

By 31 December 2027

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: EC, ACER, ENISA

Chapter 47

Article 45: Outcome of cybersecurity exercises at entity, Member State, regional or cross regional levels

47.1 Paragraph 1

Upon request from a critical-impact entity, critical service providers shall participate in the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) when they provide services for the critical-impact entity in the area corresponding with the scope of the relevant cybersecurity exercise.

Relevant NCCS Articles

- Article 43(1)
- Article 43(2)
- Article 44(1)

Input

- Union wide high level and critical level processes

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, ENTSO-E, TSO, ENISA, CRITICAL ICT

47.2 Paragraph 2

The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1), with the advice of ENISA if requested by them and pursuant to Article 7(5) of Regulation (EU) 2019/881 [a], shall analyse and finalise the relevant cybersecurity exercise through a report summarising the lessons, addressed to all participants. The report shall include:

a. the exercise scenarios, meeting reports, main positions, successes and lessons learnt at any level of the electricity value chain;

b. whether the key success criteria were met;

c. a list of recommendations for entities participating in the relevant cybersecurity exercise to correct, adapt or change cybersecurity crisis processes, procedures, associated governance models and any existing contractual engagements with critical service providers.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881#d1e1398-15-1

Relevant NCCS Articles

- Article 43(1)
- Article 43(2)
- Article 44(1)

Output

- Report about cybersecurity exercise

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, ENTSO-E, TSO

Consulted: ENISA

Informed: NCA

47.3 Paragraph 3

If requested by the CSIRTs network or the NIS Cooperation Group or the EU CyCLONe, the organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) shall share the outcome of the relevant cybersecurity exercise. The organisers shall share with each entity participating in the exercises the information referred to in paragraph 2, points (a) and (b) of this Article. The organisers shall share the list of recommendations referred to in that paragraph, point (c) exclusively with the entities addressed in the recommendations.

Relevant NCCS Articles

- Article 43(1)
- Article 43(2)
- Article 44(1)
- term:a45, cikk 2[Article 45, cikk 2]

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, ENTSO-E, TSO, NCA, NIS CG, CSIRT

47.4 Paragraph 4

The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) shall follow up regularly with the entities participating in the exercises on the implementation of the recommendations pursuant to paragraph 2, point (c) of this Article.

Relevant NCCS Articles

- Article 43(1)
- Article 43(2)
- Article 44(1)
- Article 45(2)

Accountable: CIE, TSO

Involved Stakeholders

Responsible: CIE, ENTSO-E, TSO

Chapter 48

Article 46: Principles for the protection of exchanged information

48.1 Paragraph 1

The entities listed in Article 2(1) shall ensure that information provided, received, exchanged or transmitted under this Regulation is accessible only on a need-to-know basis and in accordance with relevant Union and national rules on security of information.

Relevant NCCS Articles

- Article 2(1)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

48.2 Paragraph 2

The entities listed in Article 2(1) shall ensure that information provided, received, exchanged or transmitted under this Regulation is handled and tracked during the entire life-cycle of that information and that it may be released at the end of its life-cycle only after being anonymised.

Relevant NCCS Articles

- Article 2(1)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

48.3 Paragraph 3

The entities listed in Article 2(1) shall ensure that all necessary protection measures of organisational and technical nature are in place to safeguard and protect the confidentiality, integrity, availability and non-repudiation of information provided, received, exchanged or transmitted under this Regulation, independently from the means used. The protection measures shall:

a. be proportionate;

b. take into consideration cybersecurity risks related to known past and emerging threats to which such information may be subject in the context of this Regulation;

c. to the extent possible, be based on national, European or international standards and best practices;

d. be documented.

Relevant NCCS Articles

- Article 2(1)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

48.4 Paragraph 4

The entities listed in Article 2(1) shall ensure that any individual who is granted access to information provided, received, exchanged or transmitted under this Regulation is briefed on the security rules applicable at entity level and on the measures and procedures relevant to the protection of information. Those entities shall ensure that the concerned individual

acknowledges the responsibility to protect the information as instructed during the briefing.

Relevant NCCS Articles

- Article 2(1)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

48.5 Paragraph 5

The entities listed in Article 2(1) shall ensure that access to information provided, received, exchanged or transmitted under this Regulation is limited to individuals:

a. who are authorised to access that information based on their functions and limited to the execution of the tasks assigned;

b. for whom the entity was able to assess ethical and integrity principles, as well as for whom there is no evidence of negative outcome from a background verification check to evaluate reliability of the individual in accordance with the best practices and standard security requirements of the entity, and, where necessary, with the national laws and regulations.

Relevant NCCS Articles

- Article 2(1)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

48.6 Paragraph 6

The entities listed in Article 2(1) shall have the written agreement of the natural or legal person that originally created or provided the information, prior to providing that information to a third party that falls outside the scope of this Regulation.

Relevant NCCS Articles

- Article 2(1)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

48.7 Paragraph 7

An entity listed in Article 2(1) may consider that this information shall be shared without complying with paragraphs 1 and 4 of this Article in order to prevent a simultaneous electricity crisis with a cybersecurity root cause or any cross-border crisis within the Union in another sector. In that case, it shall:

a. consult and be authorised by the competent authority to share such information;

b. anonymise such information without losing the elements necessary to inform the public of an imminent and serious risk to cross-border electricity flows and the possible mitigation measures;

c. safeguard the identity of the originator and of the entities that have been processing such information under this Regulation.

Relevant NCCS Articles

- Article 2(1)
- Article 46(1)
- Article 46(4)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Consulted: NCA

48.8 Paragraph 8

By derogation from paragraph 6 of this Article, the competent authorities may provide information provided, received, exchanged or transmitted under this Regulation to a third party not listed in Article 2(1) without a written prior consent of the originator of the information but informing the latter at the earliest time possible. Before disclosing any information provided, received, exchanged or transmitted under this Regulation to a third party not listed in Article 2(1), the concerned competent authority shall reasonably ensure that the concerned third party is aware of the security rules in force and shall receive reasonable assurance that the concerned third party can protect the received information in compliance with paragraphs 1 to 5 of this Article. The competent authority shall anonymise such information without losing the elements necessary to inform the public of an imminent and serious risk to cross-border electricity flows and possible mitigations measures and safeguard the identity of the originator of the information. In this case, the third party not listed in Article 2(1) shall protect the received information in accordance with provisions already in force at entity level, or where this is not possible, with the provisions and instructions provided by

the relevant competent authority.

Relevant NCCS Articles

- Article 46(6)
- Article 2(1)
- Article 46(1)
- Article 46(2)
- Article 46(3)
- Article 46(4)
- Article 46(5)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

48.9 Paragraph 9

This Article does not apply to entities not listed in Article 2(1) that are provided with information pursuant to paragraph 6 of this Article. In this case paragraph 7 of this Article shall be applied, or the competent authority may provide that entity with written provisions to apply in cases where information is received pursuant to this Regulation.

Relevant NCCS Articles

- Article 2(1)
- Article 46(6)
- Article 46(7)

Other NCCS Articles

- Article 47

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Chapter 49

Article 47: Confidentiality of information

49.1 Paragraph 1

Any information provided, received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraphs 2 to 5 of this Article of this Regulation and requirements as laid down in Article 65 of Regulation (EU) 2019/943 [a]. Any information provided, received, exchanged or transmitted among entities listed in Article 2 of this Regulation, for the purposes of implementing this Regulation, shall be protected, considering the confidentiality level of the information applied by the originator.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943#d1e5115-54-1

Relevant NCCS Articles

- Article 47(2)
- Article 47(3)
- Article 47(4)
- Article 47(5)

- Article 2

Accountable: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.2 Paragraph 2

The obligation of professional secrecy shall apply to the entities listed in Article 2.

Relevant NCCS Articles

- Article 2

Accountable: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.3 Paragraph 3

The CS-NCAs, the NRAs, the RP-NCAs and the CSIRTs shall exchange all necessary information to carry out their tasks.

Accountable: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.4 Paragraph 4

Any information received, exchanged or transmitted among entities listed in Article 2(1), for the purposes of implementing Article 23, shall be anonymised and aggregated.

Relevant NCCS Articles

- Article 2(1)
- Article 23

Accountable: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, CS NCA

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, CS NCA

49.5 Paragraph 5

Information received by any entity or authority subject to this Regulation in the course of their duties may not be disclosed to any other entity or authority, without prejudice to cases covered by national law, other provisions of this Regulation or other relevant Union legislation.

Accountable: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.6 Paragraph 6

Without prejudice to national or Union legislation, an authority, entity or natural person who receives information pursuant to this Regulation may not use it for any other purpose than carrying out its duties under this Regulation.

Accountable: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

49.7 Paragraph 7

ACER, after consulting ENISA, all competent authorities, ENTSO for Electricity and the EU-DSO Entity, shall by 13 June 2025 issue guidelines addressing mechanisms for all entities listed in Article 2(1) to exchange information, and in particular envisaged communication flows, and methods to anonymise and to aggregate information for the purpose of implementation of this Article.

Relevant NCCS Articles

- Article 2(1)

Output

- Guideline about information flow

GOOD TO KNOW

Timing

By 13 June 2025

Accountable: ACER

Involved Stakeholders

Responsible: ACER

Consulted: ENTSO-E, ENISA, EU DSO

Informed: HIE, CIE, NCA, NRA, RP NCA, CS NCA

49.8 Paragraph 8

Information that is confidential pursuant to Union and national rules shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Regulation. The information exchanged shall be limited to that which is necessary and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of critical-impact or high-impact entities.

Accountable: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Involved Stakeholders

Responsible: HIE, CIE, ENTSO-E, TSO, ACER, ENISA, EU DSO, NCA, NRA, RP NCA, CS NCA

Informed: EC

Chapter 50

Article 48: Temporary provisions

50.1 Paragraph 1

Until the approval of the terms and conditions or methodologies referred to in Article 6(2) or plans referred to in Article 6(3), the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop non-binding guidance on the following issues:

a. a provisional electricity cybersecurity impact index (‘ECII’) pursuant to paragraph 2 of this Article;

b. a provisional list of Union-wide high-impact and critical-impact processes pursuant to paragraph 4 of this Article; and

c. a provisional list of European and international standards and controls required by national legislation

Relevant NCCS Articles

- Article 6(2)
- Article 6(3)
- Article 48(2)

- Article 48(4)
- Article 48(6)

Output

- Provisional ECII
- Provisional list of Union-wide high-impact and critical-impact processes
- Provisional list of European and international standards and controls

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

50.2 Paragraph 2

By 13 October 2024, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a recommendation for a provisional ECII. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall notify the recommended provisional ECII to the competent authorities.

Output

- Provisional ECII

GOOD TO KNOW

Timing

By 13 October 2024

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: NCA

50.3 Paragraph 3 (/1)

Four months of receipt of the recommended provisional ECII, or the latest by 13 February 2025, the competent authorities shall identify candidates for high-impact and critical-impact entities in their Member State based on the recommended ECII and shall develop a provisional list of high-impact and critical-impact entities.

Output

- Notification of provisional identified entities

GOOD TO KNOW

Timing

By 13 February 2025

Accountable: NCA

Involved Stakeholders

Responsible: NCA

50.4 Paragraph 3 (/2)

The high-impact and critical-impact entities identified in the provisional list may voluntarily fulfil their obligations as laid down in this Regulation based on a precautionary principle. By 13 March 2025, the competent authorities shall notify the entities identified in the provisional list that they have been identified as a high-impact or critical-impact entity.

Output

- List of provisional identified entities

GOOD TO KNOW

Timing

By 13 March 2025

Accountable: NCA

Involved Stakeholders

Responsible: NCA

Informed: HIE, CIE

50.5 Paragraph 4 (/1)

By 13 December 2024, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a provisional list of Union-wide high-impact and critical-impact processes.

Output

- Provisional list of high impact and critical impact processes

GOOD TO KNOW

Timing

By 13 December 2024

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Informed: NCA

50.6 Paragraph 4 (/2)

The entities notified pursuant to paragraph (3) that voluntarily decide to fulfil their obligations as laid down in this Regulation based on a precautionary principle shall use the provisional list of high-impact and critical-impact processes to determine the provisional high-impact and critical-impact perimeters and to determine which assets are to be included in the first cybersecurity risk assessment at entity level.

Relevant NCCS Articles

- Article 48(3)

Output

- Entity level risk assessment report

GOOD TO KNOW

Timing

12 months after notification

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Informed: ENTSO-E, ACER, NCA

50.7 Paragraph 5

By 13 September 2024, each competent authority according to Article 4 (1) shall provide a list of its national legislation with relevance for cybersecurity aspects of cross-border electricity flows to the ENTSO for Electricity and the EU DSO entity.

Relevant NCCS Articles

- Article 4(1)

Output

- List of national legislation

GOOD TO KNOW

Timing

By 13 September 2024

A

Accountable: NCA

Involved Stakeholders

R

Responsible: NCA

I

Informed: ENTSO-E, EU DSO

50.8 Paragraph 6

By 13 June 2025, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall prepare a provisional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows, taking into account the information provided by the competent authorities.

Output

- Provisional list of European and international standards and controls"

GOOD TO KNOW

Timing

By 13 June 2025

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO, NCA

50.9 Paragraph 7

The provisional list of European and international standards and controls shall include:

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO, NCA

50.10 Paragraph 8

The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by ENISA and ACER when finalising the provisional list of standards. The ENTSO for Electricity and the EU DSO entity shall publish the transitional list of European and international standards and controls on their websites.

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, ACER, ENISA, EU DSO

50.11 Paragraph 9

The ENTSO for Electricity and the EU DSO entity shall consult ENISA and ACER on the proposals for non-binding guidance developed pursuant to paragraph 1.

Relevant NCCS Articles

- Article 48(1)

Accountable: ENTSO-E

Involved Stakeholders

Responsible: ENTSO-E, EU DSO

Consulted: ACER, ENISA

50.12 Paragraph 10

Until the minimum and advanced cybersecurity controls are developed pursuant to Article 29 and adopted pursuant to Article 8, all entities listed in Article 2(1) shall strive to progressively apply the non-binding guidance developed pursuant to paragraph 1.

Relevant NCCS Articles

- Article 29
- Article 8
- Article 2
- Article 48(1)

Accountable: HIE, CIE, TSO

Involved Stakeholders

Responsible: HIE, CIE, TSO

Glossary

Agency for the Cooperation of Energy Regulators (ACER)

The Agency for the Cooperation of Energy Regulators

A specialized agency of the European Union responsible for facilitating the integration and efficient functioning of EU energy markets.

https://www.acer.europa.eu/ [1]

REGULATION (EU) 2019/942 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [2]

Article 10

ACER, in close cooperation with ENTSO for Electricity and the EU DSO entity, shall organise stakeholder involvement, including regular meetings with stakeholders to identify problems and propose improvements related to the implementation of this Regulation.

Article 11

1. The costs borne by TSOs and DSOs subject to network tariff regulation and stemming from the obligations laid down in this Regulation, including the costs borne by the ENTSO for Electricity and the EU DSO entity, shall be assessed by the relevant NRA of each Member State.
2. Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms, as determined by the relevant NRA.
3. If requested by the relevant NRAs, TSOs and DSOs referred to in paragraph 1 shall, within a reasonable period determined by the NRA, provide the information necessary to facilitate the assessment of the costs incurred.

Article 11(1)

[1] https://www.acer.europa.eu/
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942

The costs borne by TSOs and DSOs subject to network tariff regulation and stemming from the obligations laid down in this Regulation, including the costs borne by the ENTSO for Electricity and the EU DSO entity, shall be assessed by the relevant NRA of each Member State.

Article 11(2)

Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms, as determined by the relevant NRA.

Article 11(3)

If requested by the relevant NRAs, TSOs and DSOs referred to in paragraph 1 shall, within a reasonable period determined by the NRA, provide the information necessary to facilitate the assessment of the costs incurred.

Article 12

1. ACER shall monitor the implementation of this Regulation in accordance with Article 32(1) of Regulation (EU) 2019/943 [3] and Article 4(2) of Regulation (EU) 2019/942 [4]. In carrying out this monitoring, ACER may cooperate with ENISA and request support from the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group and the NIS Cooperation Group on the implementation of this Regulation.
2. ACER shall publish a report at least every three years after the entry into force of this Regulation to:

a. review the status of implementation of the applicable cybersecurity risk management measures with regard to the high-impact and critical-impact entities;

b. identify whether additional rules on common requirements, planning, monitoring, reporting and crisis management may be necessary to prevent risks for the electricity sector; and

c. identify areas of improvement for the revision of this Regulation, or determine uncovered areas and new priorities that may emerge due to technological developments.

1. By 13 June 2025, ACER, in cooperation with ENISA and after consultation of the ENTSO for Electricity and the EU DSO entity, may issue guidance on the relevant information to be communicated to ACER for the monitoring purposes as well as the process and frequency for the collection, based on the performance indicators defined in accordance with paragraph 5.
2. The competent authorities may have access to the relevant information held by ACER, which it has collected in accordance with this Article.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943&qid=1733993709560#d1e3462-54-1

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942#d1e519-22-1

3. ACER in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity, shall issue non-binding performance indicators for the assessment of operational reliability that are related to cybersecurity aspects of cross-border electricity flows.
4. The entities listed in Article 2(1) of this Regulation shall submit to ACER the information required for ACER to perform the tasks listed in paragraph 2.

Article 12(1)

ACER shall monitor the implementation of this Regulation in accordance with Article 32(1) of Regulation (EU) 2019/943 [5] and Article 4(2) of Regulation (EU) 2019/942 [6]. In carrying out this monitoring, ACER may cooperate with ENISA and request support from the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group and the NIS Cooperation Group on the implementation of this Regulation.

Article 12(2)

ACER shall publish a report at least every three years after the entry into force of this Regulation to:

a. review the status of implementation of the applicable cybersecurity risk management measures with regard to the high-impact and critical-impact entities;
b. identify whether additional rules on common requirements, planning, monitoring, reporting and crisis management may be necessary to prevent risks for the electricity sector; and
c. identify areas of improvement for the revision of this Regulation, or determine uncovered areas and new priorities that may emerge due to technological developments.

Article 12(3)

By 13 June 2025, ACER, in cooperation with ENISA and after consultation of the ENTSO for Electricity and the EU DSO entity, may issue guidance on the relevant information to be communicated to ACER for the monitoring purposes as well as the process and frequency for the collection, based on the performance indicators defined in accordance with paragraph 5.

Article 12(4)

The competent authorities may have access to the relevant information held by ACER, which it has collected in accordance with this Article.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943&qid=1733993709560#d1e3462-54-1

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942#d1e519-22-1

Article 12(5)

ACER in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity, shall issue non-binding performance indicators for the assessment of operational reliability that are related to cybersecurity aspects of cross-border electricity flows.

Article 12(6)

The entities listed in Article 2(1) of this Regulation shall submit to ACER the information required for ACER to perform the tasks listed in paragraph 2.

Article 13

1. By 13 June 2025, ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide. The guide shall explain to NRAs the principles of benchmarking of the implemented cybersecurity controls pursuant to paragraph 2 of this Article, taking into consideration the costs of implementing the controls and the effectiveness of the function played by processes, products, services, systems and solutions used to implement such controls. ACER shall take into account existing benchmarking reports when establishing the non-binding cybersecurity benchmarking guide. ACER shall submit the non-binding cybersecurity benchmarking guide to the NRAs for information.
2. Within 12 months after the establishment of the benchmarking guide pursuant to paragraph 1, the NRAs shall carry out a benchmarking analysis to assess whether current investments in cybersecurity:

a. mitigate risks having an impact on cross-border electricity flows;

b. provide the desired results and engender efficiency gains for the development of the electricity systems;

c. are efficient and integrated into the overall procurement of assets and services.

    1. For the benchmarking analysis, the NRAs may take into account the non-binding cybersecurity benchmarking guide established by ACER, and shall assess in particular:

a. the average expenditure related to cybersecurity for mitigating risks having an impact on electricity cross-border flows, especially with respect to the high-impact and critical-impact entities;

b. in cooperation with the ENTSO for Electricity and the EU DSO entity, the average prices of cybersecurity services, systems and products that contribute to a large extent to the enhancement and maintenance of the cybersecurity risk-management measures in the different system operation regions;

c. the existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of this Regulation, identifying possible measures necessary to foster efficiency in spending, particularly where cybersecurity technological investments may be needed.

1. Any information related to benchmarking analysis shall be handled and processed pursuant to data classification requirements of this Regulation, the minimum cybersecurity controls and the cross-border electricity cybersecurity risk assessment report. The benchmarking analysis referred to in paragraphs 2 and 3 shall not be made public.
2. Without prejudice to the confidentiality requirements in Article 47 and to the need to protect the security of entities subject to the provisions of this Regulation, the benchmarking analysis referred in paragraphs 2 and 3 of this Article shall be shared with all NRAs, all competent authorities, ACER, ENISA and the Commission.

Article 13(1)

By 13 June 2025, ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide. The guide shall explain to NRAs the principles of benchmarking of the implemented cybersecurity controls pursuant to paragraph 2 of this Article, taking into consideration the costs of implementing the controls and the effectiveness of the function played by processes, products, services, systems and solutions used to implement such controls. ACER shall take into account existing benchmarking reports when establishing the non-binding cybersecurity benchmarking guide. ACER shall submit the non-binding cybersecurity benchmarking guide to the NRAs for information.

Article 13(2)

Within 12 months after the establishment of the benchmarking guide pursuant to paragraph 1, the NRAs shall carry out a benchmarking analysis to assess whether current investments in cybersecurity:

a. mitigate risks having an impact on cross-border electricity flows;

b. provide the desired results and engender efficiency gains for the development of the electricity systems;

c. are efficient and integrated into the overall procurement of assets and services.

Article 13(3)

For the benchmarking analysis, the NRAs may take into account the non-binding cybersecurity benchmarking guide established by ACER, and shall assess in particular:

a. the average expenditure related to cybersecurity for mitigating risks having an impact on electricity cross-border flows, especially with respect to the high-impact and critical-impact entities;

b. in cooperation with the ENTSO for Electricity and the EU DSO entity, the average prices of cybersecurity services, systems and products that contribute to a large extent to the enhancement and maintenance of the cybersecurity risk-management measures in the different system operation regions;

c. the existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of this Regulation, identifying possible measures necessary to foster efficiency in spending, particularly where cybersecurity technological investments may be needed.

Article 13(4)

Any information related to benchmarking analysis shall be handled and processed pursuant to data classification requirements of this Regulation, the minimum cybersecurity controls and the cross-border electricity cybersecurity risk assessment report. The benchmarking analysis referred to in paragraphs 2 and 3 shall not be made public.

Article 13(5)

Without prejudice to the confidentiality requirements in Article 47 and to the need to protect the security of entities subject to the provisions of this Regulation, the benchmarking analysis referred in paragraphs 2 and 3 of this Article shall be shared with all NRAs, all competent authorities, ACER, ENISA and the Commission.

Article 14

1. Within 18 months after the entry into force of this Regulation, TSOs of a system operation region that is neighbouring to a third country shall endeavour to conclude agreements with TSOs of the neighbouring third country that are in accordance with relevant Union law and that set out the basis for cooperation on cybersecurity protection and the cybersecurity cooperation arrangements with those TSOs.

2. TSOs shall inform the competent authority of the agreements concluded pursuant to paragraph 1.

Article 14(1)

Within 18 months after the entry into force of this Regulation, TSOs of a system operation region that is neighbouring to a third country shall endeavour to conclude agreements with TSOs of the

neighbouring third country that are in accordance with relevant Union law and that set out the basis for cooperation on cybersecurity protection and the cybersecurity cooperation arrangements with those TSOs.

Article 14(2)

TSOs shall inform the competent authority of the agreements concluded pursuant to paragraph 1.

Article 15

1. Entities who do not have an establishment in the Union, but who deliver services to entities in the Union and have been notified as being high-impact or critical-impact entities in accordance with Article 24(6), shall, within three months after the notification, designate, in writing, a representative in the Union and inform the notifying competent authority accordingly.
2. This representative shall be mandated for the purpose of being addressed by any competent authority or a CSIRT in the Union in addition to or instead of the high-impact or critical-impact entity with regard to the obligations of the entity under this Regulation. The high-impact or critical-impact entity shall provide their legal representative with the necessary powers and sufficient resources to guarantee their efficient and timely cooperation with the relevant competent authorities or CSIRTs.
3. The representative shall be established in one of the Member States where the entity offers its services. The entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. High-impact or critical-impact entities shall notify the name, postal address, email address and telephone number of their legal representative to the competent authority in the Member State where that legal representative resides or is established.
4. It shall be possible for the designated legal representative to be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the high-impact or critical- impact entity itself.
5. In the absence of a representative within the Union designated under this Article, any Member State in which the entity provides services may take legal action against the entity for non-compliance with the obligations under this Regulation.
6. The designation of a legal representative within the Union pursuant to paragraph 1 shall not constitute an establishment in the Union.

Article 15(1)

Entities who do not have an establishment in the Union, but who deliver services to entities in the Union and have been notified as being high-impact or critical-impact entities in accordance

with Article 24(6), shall, within three months after the notification, designate, in writing, a representative in the Union and inform the notifying competent authority accordingly.

Article 15(2)

This representative shall be mandated for the purpose of being addressed by any competent authority or a CSIRT in the Union in addition to or instead of the high-impact or critical-impact entity with regard to the obligations of the entity under this Regulation. The high-impact or critical-impact entity shall provide their legal representative with the necessary powers and sufficient resources to guarantee their efficient and timely cooperation with the relevant competent authorities or CSIRTs.

Article 15(3)

The representative shall be established in one of the Member States where the entity offers its services. The entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. High-impact or critical-impact entities shall notify the name, postal address, email address and telephone number of their legal representative to the competent authority in the Member State where that legal representative resides or is established.

Article 15(4)

It shall be possible for the designated legal representative to be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the high-impact or critical- impact entity itself.

Article 15(5)

In the absence of a representative within the Union designated under this Article, any Member State in which the entity provides services may take legal action against the entity for non-compliance with the obligations under this Regulation.

Article 15(6)

The designation of a legal representative within the Union pursuant to paragraph 1 shall not constitute an establishment in the Union.

Article 16

1. The ENTSO for Electricity and the EU DSO entity shall cooperate in performing cybersecurity risk assessments pursuant to Article 19 and Article 21, and in particular the following tasks:

a. development of the cybersecurity risk assessment methodologies pursuant to Article 18(1);

b. development of the Comprehensive Cross-border electricity cybersecurity risk assessment report pursuant to Article 23;

c. development of the common electricity cybersecurity framework pursuant to Chapter III;

d. development of the cybersecurity procurement recommendation pursuant to Article 35;

e. development of the cyber-attacks classification scale methodology pursuant to Article 37(8);

f. development of the provisional electricity cybersecurity impact index (ECII) electricity cybersecurity impact index pursuant to Article 48(1) point (a);

g. development of the consolidated provisional list of high-impact and critical-impact entities pursuant to Article 48(3);

h. development of the provisional list of Union-wide high-impact and critical-impact processes pursuant to Article 48(4);

i. development of the provisional list of European and international standards and controls pursuant to Article 48(6);

j. performance of the Union-wide cybersecurity risk assessment pursuant to Article 19;

k. performance of the regional cybersecurity risk assessments pursuant to Article 21;

l. definition of the regional cybersecurity risk mitigation plans pursuant to Article 22;

m. development of guidance on European cybersecurity certification schemes for ICT products, ICT services, and ICT processes in accordance with Article 36;

1. (n) development of guidelines for the implementation of this Regulation in consultation with ACER and ENISA.
2. The cooperation between the ENTSO for Electricity and the EU DSO entity may take the form of a cybersecurity risk working group.
3. The ENTSO for Electricity and the EU DSO entity shall regularly inform ACER, ENISA, the NIS Cooperation Group and the Electricity Coordination Group on the progress in implementing the Union-wide and regional cybersecurity risk assessments pursuant to Article 19 and Article 21.

Article 16(1)

The ENTSO for Electricity and the EU DSO entity shall cooperate in performing cybersecurity risk assessments pursuant to Article 19 and Article 21, and in particular the following tasks:

a. development of the cybersecurity risk assessment methodologies pursuant to Article 18(1);

b. development of the Comprehensive Cross-border electricity cybersecurity risk assessment report pursuant to Article 23;

c. development of the common electricity cybersecurity framework pursuant to Chapter III;

d. development of the cybersecurity procurement recommendation pursuant to Article 35;

e. development of the cyber-attacks classification scale methodology pursuant to Article 37(8);

f. development of the provisional electricity cybersecurity impact index ('ECII') electricity cybersecurity impact index pursuant to Article 48(1) point (a);

g. development of the consolidated provisional list of high-impact and critical-impact entities pursuant to Article 48(3);

h. development of the provisional list of Union-wide high-impact and critical-impact processes pursuant to Article 48(4);

i. development of the provisional list of European and international standards and controls pursuant to Article 48(6);

j. performance of the Union-wide cybersecurity risk assessment pursuant to Article 19;

k. performance of the regional cybersecurity risk assessments pursuant to Article 21;

l. definition of the regional cybersecurity risk mitigation plans pursuant to Article 22;

m. development of guidance on European cybersecurity certification schemes for ICT products, ICT services, and ICT processes in accordance with Article 36;

n. development of guidelines for the implementation of this Regulation in consultation with ACER and ENISA.

Article 16(2)

The cooperation between the ENTSO for Electricity and the EU DSO entity may take the form of a cybersecurity risk working group.

Article 16(3)

The ENTSO for Electricity and the EU DSO entity shall regularly inform ACER, ENISA, the NIS Cooperation Group and the Electricity Coordination Group on the progress in implementing the Union-wide and regional cybersecurity risk assessments pursuant to Article 19 and Article 21.

Article 17

1. ACER, in cooperation with each competent authority, shall: (1) monitor the implementation of cybersecurity risk management measures pursuant to Article 12(2) point (a) and reporting obligations pursuant to Article 27 and Article 39; and

2. (2) monitor the adoption process and the implementation of the terms and conditions, methodologies or plans pursuant to Article 6(2) and (3). The cooperation between ACER, ENISA and each competent authority may take the form of a cybersecurity risk monitoring body.

Article 17(1)

ACER, in cooperation with each competent authority, shall:

1. monitor the implementation of cybersecurity risk management measures pursuant to Article 12(2) point (a) and reporting obligations pursuant to Article 27 and Article 39; and
2. monitor the adoption process and the implementation of the terms and conditions, methodologies or plans pursuant to Article 6(2) and (3). The cooperation between ACER, ENISA and each competent authority may take the form of a cybersecurity risk monitoring body.

Article 18

1. By 13 March 2025, the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and following a consultation with the NIS Cooperation Group, shall submit a proposal for the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level.
2. The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall include:

a. a list of cyber threats to be considered, including at least the following supply chain threats:
    a. a severe and unexpected corruption of the supply chain;
    b. the unavailability of ICT products, ICT services, or ICT processes from the supply chain;
    c. cyber-attacks initiated through actors in the supply chain;
    d. leaking of sensitive information through the supply chain, including supply chain tracking;
    e. the introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain;
b. the criteria to evaluate the impact of cybersecurity risks as high or critical, using defined thresholds for consequences and likelihood;
c. an approach to analyse the cybersecurity risks coming from legacy systems, the cascading effects of cyber-attacks and the real-time nature of systems operating the grid;
d. an approach to analyse the cybersecurity risks coming from the dependency on a single supplier of ICT products, ICT services or ICT processes.

1. The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall assess cybersecurity risks using the same risk impact matrix. The risk impact matrix shall:

a. measure the consequences of cyber-attacks based on the following criteria:

    a. loss of load;
    b. reduction of power generation;
    c. loss of capacity in the primary frequency reserve;
    d. loss of capacity for restoration of an electric grid to operation without relying on the external transmission network to recover after a total or partial shutdown (also called black start);
    e. the expected duration of an electricity outage affecting customers in combination with the scale of the outage in customer numbers; and
    f. any other quantitative or qualitative criteria that could reasonably act as an indicator of the effect of a cyber- attack on cross-border electricity flows;

b. measure the likelihood of an incident as the frequency of cyber-attacks per year.

1. The cybersecurity risk assessment methodologies at Union level shall describe how the ECII values for high-impact and critical-impact thresholds will be defined. The ECII shall enable entities to estimate with the help of the criteria referred to in paragraph 2 point (b), the impact of the risks on their business process during the business impact assessments they perform pursuant to Article 26(4) point (c)(i).
2. The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the Electricity Coordination Group on the proposals for the cybersecurity risk assessment methodologies that are developed pursuant to paragraph 1.

Article 18(1)

By 13 March 2025, the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and following a consultation with the NIS Cooperation Group, shall submit a proposal for the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level.

Article 18(2)

The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall include:

a. a list of cyber threats to be considered, including at least the following supply chain threats:

    a. a severe and unexpected corruption of the supply chain;

b. the unavailability of ICT products, ICT services, or ICT processes from the supply chain;
c. cyber-attacks initiated through actors in the supply chain;
d. leaking of sensitive information through the supply chain, including supply chain tracking;
e. the introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain;

b. the criteria to evaluate the impact of cybersecurity risks as high or critical, using defined thresholds for consequences and likelihood;

c. an approach to analyse the cybersecurity risks coming from legacy systems, the cascading effects of cyber-attacks and the real-time nature of systems operating the grid;

d. an approach to analyse the cybersecurity risks coming from the dependency on a single supplier of ICT products, ICT services or ICT processes.

Article 18(3)

The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall assess cybersecurity risks using the same risk impact matrix. The risk impact matrix shall:

a. measure the consequences of cyber-attacks based on the following criteria:
    a. loss of load;
    b. reduction of power generation;
    c. loss of capacity in the primary frequency reserve;
    d. loss of capacity for restoration of an electric grid to operation without relying on the external transmission network to recover after a total or partial shutdown (also called 'black start');
    e. the expected duration of an electricity outage affecting customers in combination with the scale of the outage in customer numbers; and
    f. any other quantitative or qualitative criteria that could reasonably act as an indicator of the effect of a cyber- attack on cross-border electricity flows;

b. measure the likelihood of an incident as the frequency of cyber-attacks per year.

Article 18(4)

The cybersecurity risk assessment methodologies at Union level shall describe how the ECII values for high-impact and critical-impact thresholds will be defined. The ECII shall enable entities to estimate with the help of the criteria referred to in paragraph 2 point (b), the impact of the risks on their business process during the business impact assessments they perform pursuant to Article 26(4) point (c)(i).

Article 18(5)

The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the Electricity Coordination Group on the proposals for the cybersecurity risk assessment methodologies that are developed pursuant to paragraph 1.

Article 19

1. Within 9 months after the approval of the cybersecurity risk assessment methodologies pursuant to Article 8 and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall, without prejudice to Article 22 of Directive (EU) 2022/2555, perform a Union-wide cybersecurity risk assessment and draw up a draft Union-wide cybersecurity risk assessment report. For this purpose, they will use the methodologies developed pursuant to Article 18, and approved pursuant to Article 8, to identify, analyse, and evaluate the possible consequences of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The Union-wide cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.
2. The Union-wide cybersecurity risk assessment report shall include the following elements: (a) the Union-wide high-impact processes and the Union-wide critical-impact processes; (b) a risk impact matrix that entities and the competent authorities shall use to assess the cybersecurity risk identified in the cybersecurity risk assessment at Member State level performed pursuant to Article 20 and in the cybersecurity risk assessment at entity level pursuant to Article 26(2) point (b).
3. With respect to the Union-wide high-impact processes and the Union-wide critical-impact processes, the Union- wide cybersecurity risk assessment report shall include: (a) an assessment of the possible consequences of a cyber-attack using the metrics defined in the cybersecurity risk assessment methodology developed pursuant to Article 18(2), (3) and (4), and approved pursuant to Article 8; (b) the ECII and high-impact and critical-impact thresholds that the competent authorities shall use pursuant to Article 24(1) and (2) to identify high-impact and critical-impact entities involved in the Union-wide high-impact processes and in the Union-wide critical-impact processes.
4. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall submit the draft of the Union-wide cybersecurity risk assessment report with the results of the Union-wide cybersecurity risk assessment to ACER for opinion.
5. ACER shall issue an opinion on the draft report within three months after its receipt. The ENTSO for Electricity and the EU DSO entity shall take utmost account of ACER s opinion when finalising that report.
6. Within three months after receipt of ACER s opinion, the ENTSO for Electricity, in cooperation with the EU DSO entity shall notify the final Union-wide cybersecurity risk assessment report to ACER, the Commission, ENISA and the competent authorities.

Article 19(1)

Within 9 months after the approval of the cybersecurity risk assessment methodologies pursuant to Article 8 and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall, without prejudice to Article 22 of Directive (EU) 2022/2555, perform a Union-wide cybersecurity risk assessment and draw up a draft Union-wide cybersecurity risk assessment report. For this purpose, they will use the methodologies developed pursuant to Article 18, and approved pursuant to Article 8, to identify, analyse, and evaluate the possible consequences of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The Union-wide cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.

Article 19(2)

The Union-wide cybersecurity risk assessment report shall include the following elements:

a. the Union-wide high-impact processes and the Union-wide critical-impact processes;
b. a risk impact matrix that entities and the competent authorities shall use to assess the cybersecurity risk identified in the cybersecurity risk assessment at Member State level performed pursuant to Article 20 and in the cybersecurity risk assessment at entity level pursuant to Article 26(2) point (b).

Article 19(3)

With respect to the Union-wide high-impact processes and the Union-wide critical-impact processes, the Union- wide cybersecurity risk assessment report shall include:

a. an assessment of the possible consequences of a cyber-attack using the metrics defined in the cybersecurity risk assessment methodology developed pursuant to Article 18(2), (3) and (4), and approved pursuant to Article 8;
b. the ECII and high-impact and critical-impact thresholds that the competent authorities shall use pursuant to Article 24(1) and (2) to identify high-impact and critical-impact entities involved in the Union-wide high-impact processes and in the Union-wide critical-impact processes.

Article 19(4)

The ENTSO for Electricity, in cooperation with the EU DSO entity, shall submit the draft of the Union-wide cybersecurity risk assessment report with the results of the Union-wide cybersecurity risk assessment to ACER for opinion.

ACER shall issue an opinion on the draft report within three months after its receipt. The ENTSO for Electricity and the EU DSO entity shall take utmost account of ACER's opinion when finalising that report.

Article 19(5)

Within three months after receipt of ACER's opinion, the ENTSO for Electricity, in cooperation with the EU DSO entity shall notify the final Union-wide cybersecurity risk assessment report to ACER, the Commission, ENISA and the competent authorities.

Article 2

This Regulation applies to cybersecurity aspects of cross-border electricity flows in the activities of the following entities, if they are identified as high-impact or critical-impact entities in accordance with Article 24 [7]:

a. electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944; [8]
b. nominated electricity market operators ('NEMOs') as defined in Article 2(8) of Regulation (EU) 2019/943; [9]
c. organised market places or 'organised markets' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014 [10] (14) that arrange transactions on products relevant to cross-border electricity flows;
d. critical ICT service providers as referred to in Article 3, point (9) of this Regulation [11]
e. the ENTSO for Electricity established pursuant to Article 28 of Regulation (EU) 2019/943 [12]
f. the EU DSO entity established pursuant to Article 52 of Regulation (EU) 2019/943; [13]
g. balancing responsible parties as defined in Article 2, point (14) of Regulation (EU) 2019/943; [14]
h. operators of recharging points as defined in Annex I to Directive (EU) 2022/2555; [15]
i. regional coordination centres ('RCCs') as established pursuant to Article 35 of Regulation (EU) 2019/943; [16]
j. managed security service providers ('MSSP') as defined in Article 6(40) of Directive (EU) 2022/2555; [17]
k. any other entity or third party to whom responsibilities have been delegated or assigned pursuant to this Regulation. [18]

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R1348
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%253A32024R1366
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

1. The following authorities are, as part of their current mandates, responsible to perform tasks assigned in this Regulation [19]:

l. the European Union Agency for the Cooperation of Energy Regulators ('ACER') established by Regulation (EU) 2019/942 of the European Parliament and of the Council [20]

m. national competent authorities responsible for carrying out the tasks assigned to them under this Regulation [21] and designated by Member States pursuant to Article 4, or 'competent authority';

n. national regulatory authorities ('NRAs') designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944; [22]

o. competent authorities for risk preparedness ('RP-NCAs') established pursuant to Article 3 of Regulation (EU) 2019/941; [23]

p. computer security incident response teams ('CSIRTs') as designated or established pursuant to Article 10 of Directive (EU) 2022/2555; [24]

q. competent authorities responsible for cybersecurity ('CS-NCAs') as designated or established pursuant to Article 8 of Directive (EU) 2022/2555; [25]

r. the European Union Agency for Cybersecurity established pursuant to Regulation (EU) 2019/881; [26]

s. any other authorities or third party to whom responsibilities have been delegated or assigned pursuant to https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885 [27]

Article 2(1)

This Regulation applies to cybersecurity aspects of cross-border electricity flows in the activities of the following entities, if they are identified as high-impact or critical-impact entities in accordance with Article 24 [28]:

a. electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944; [29]

b. nominated electricity market operators ('NEMOs') as defined in Article 2(8) of Regulation (EU) 2019/943; [30]

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[24] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[30] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943

c. organised market places or 'organised markets' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014 [31] (14) that arrange transactions on products relevant to cross-border electricity flows;

d. critical ICT service providers as referred to in Article 3, point (9) of this Regulation [32]

e. the ENTSO for Electricity established pursuant to Article 28 of Regulation (EU) 2019/943 [33]

f. the EU DSO entity established pursuant to Article 52 of Regulation (EU) 2019/943; [34]

g. balancing responsible parties as defined in Article 2, point (14) of Regulation (EU) 2019/943; [35]

h. operators of recharging points as defined in Annex I to Directive (EU) 2022/2555; [36]

i. regional coordination centres ('RCCs') as established pursuant to Article 35 of Regulation (EU) 2019/943; [37]

j. managed security service providers ('MSSP') as defined in Article 6(40) of Directive (EU) 2022/2555; [38]

k. any other entity or third party to whom responsibilities have been delegated or assigned pursuant to this Regulation. [39]

Article 2(2)

1. The following authorities are, as part of their current mandates, responsible to perform tasks assigned in this Regulation [40]:

   a. the European Union Agency for the Cooperation of Energy Regulators ('ACER') established by Regulation (EU) 2019/942 of the European Parliament and of the Council [41]

   b. national competent authorities responsible for carrying out the tasks assigned to them under this Regulation [42] and designated by Member States pursuant to Article 4, or 'competent authority';

   c. national regulatory authorities ('NRAs') designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944; [43]

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R1348
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%253A32024R1366
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[34] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[35] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art
[37] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[39] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[40] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[41] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942
[42] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885
[43] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944

d. competent authorities for risk preparedness ('RP-NCAs') established pursuant to Article 3 of Regulation (EU) 2019/941; [44]

e. computer security incident response teams ('CSIRTs') as designated or established pursuant to Article 10 of Directive (EU) 2022/2555; [45]

f. competent authorities responsible for cybersecurity ('CS-NCAs') as designated or established pursuant to Article 8 of Directive (EU) 2022/2555; [46]

g. the European Union Agency for Cybersecurity established pursuant to Regulation (EU) 2019/881; [47]

h. any other authorities or third party to whom responsibilities have been delegated or assigned pursuant to Article 4(3). [48]

Article 20

1. Each competent authority shall perform a Member State cybersecurity risk assessment on all high-impact and critical-impact entities in its Member State using the methodologies developed pursuant to Article 18 and approved pursuant to Article 8. The Member State cybersecurity risk assessment shall identify and analyse the risks of cyber-attacks affecting the operational security of the electricity system disrupting cross-border electricity flows. The Member State cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.

2. Within 21 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and every three years after that date, and after consulting the CS-NCA responsible for electricity, each competent authority, supported by the CSIRT, shall provide a Member State cybersecurity risk assessment report to the ENTSO for Electricity and the EU DSO entity, containing the following information for each high-impact and critical-impact business process: (a) the implementation status of the minimum and advanced cybersecurity controls pursuant to Article 29; (b) a list of all cyber-attacks reported in the previous three years pursuant to Article 38(3); (c) a summary of the cyber threat information reported in the previous three years pursuant to Article 38(6); (d) for each Union-wide high-impact or critical-impact process, an estimate of the risks of a compromise of the confidentiality, integrity and availability for information and relevant assets; (e) where necessary, a list of additional entities identified as high-impact or critical-impact pursuant to Article 24(1), (2), (3), and (5).

3. The Member State cybersecurity risk assessment report shall take into account the Member State s risk preparedness plan established pursuant to Article 10 of Regulation (EU) 2019/941.

4. The information contained in the Member State cybersecurity risk assessment report pursuant to paragraph 2 points (a) to (d) shall not be linked to specific entities or assets. The Member State cybersecurity risk assessment report shall also include a risk assessment of the temporary derogations issued by the competent authorities in the Member States pursuant to Article 30.

[44] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[45] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[46] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[47] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[48] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

5. The ENTSO for Electricity and the EU DSO entity may request additional information from the competent authorities in relation to the tasks specified in subparagraph 2 points (a) and (c).
6. The competent authorities shall ensure that the information they provide is accurate and correct.

Article 20(1)

Each competent authority shall perform a Member State cybersecurity risk assessment on all high-impact and critical-impact entities in its Member State using the methodologies developed pursuant to Article 18 and approved pursuant to Article 8. The Member State cybersecurity risk assessment shall identify and analyse the risks of cyber-attacks affecting the operational security of the electricity system disrupting cross-border electricity flows. The Member State cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.

Article 20(2)

Within 21 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and every three years after that date, and after consulting the CS-NCA responsible for electricity, each competent authority, supported by the CSIRT, shall provide a Member State cybersecurity risk assessment report to the ENTSO for Electricity and the EU DSO entity, containing the following information for each high-impact and critical-impact business process:

a. the implementation status of the minimum and advanced cybersecurity controls pursuant to Article 29;
b. a list of all cyber-attacks reported in the previous three years pursuant to Article 38(3);
c. a summary of the cyber threat information reported in the previous three years pursuant to Article 38(6);
d. for each Union-wide high-impact or critical-impact process, an estimate of the risks of a compromise of the confidentiality, integrity and availability for information and relevant assets;
e. where necessary, a list of additional entities identified as high-impact or critical-impact pursuant to Article 24(1), (2), (3), and (5).

Article 20(3)

The Member State cybersecurity risk assessment report shall take into account the Member State's risk preparedness plan established pursuant to Article 10 of Regulation (EU) 2019/941.

Article 20(4)

The information contained in the Member State cybersecurity risk assessment report pursuant to paragraph 2 points (a) to (d) shall not be linked to specific entities or assets. The Member State cybersecurity risk assessment report shall also include a risk assessment of the temporary derogations issued by the competent authorities in the Member States pursuant to Article 30.

Article 20(5)

The ENTSO for Electricity and the EU DSO entity may request additional information from the competent authorities in relation to the tasks specified in subparagraph 2 points (a) and (c).

Article 20(6)

The competent authorities shall ensure that the information they provide is accurate and correct.

Article 21

1. The ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the relevant Regional Coordination Centre, shall perform a regional cybersecurity risk assessment for each system operation region using the methodologies developed pursuant to Article 19, and approved pursuant to Article 8, to identify, analyse, and evaluate the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The regional cybersecurity risk assessments shall not consider the legal, financial or reputational damage of cyber- attacks.
2. Within 30 months after the notification of the high-impact and critical-impact entities pursuant to Article 24(6), and every three years after that, the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall draw up a regional cybersecurity risk assessment report for each system operation region.
3. The regional cybersecurity risk assessment report shall take into account the relevant information contained in the Union-wide cybersecurity risk assessment reports and in the Member State cybersecurity risk assessments reports.
4. The regional cybersecurity risk assessment shall consider the regional electricity crisis scenarios related to cybersecurity identified pursuant to Article 6 of the Regulation (EU) 2019/941.

Article 21(1)

The ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the relevant Regional Coordination Centre, shall perform a regional cybersecurity risk assessment for each system operation region using the methodologies developed pursuant to Article 19, and approved pursuant to Article 8, to identify, analyse, and evaluate the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity

flows. The regional cybersecurity risk assessments shall not consider the legal, financial or reputational damage of cyber- attacks.

Article 21(2)

Within 30 months after the notification of the high-impact and critical-impact entities pursuant to Article 24(6), and every three years after that, the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall draw up a regional cybersecurity risk assessment report for each system operation region.

Article 21(3)

The regional cybersecurity risk assessment report shall take into account the relevant information contained in the Union-wide cybersecurity risk assessment reports and in the Member State cybersecurity risk assessments reports.

Article 21(4)

The regional cybersecurity risk assessment shall consider the regional electricity crisis scenarios related to cybersecurity identified pursuant to Article 6 of the Regulation (EU) 2019/941.

Article 22

1. Within 36 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and no later than 13 June 2031, and every three years after that date, the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the Regional Coordination Centres and the NIS Cooperation Group, shall develop a regional cybersecurity risk mitigation plan for each system operation region.
2. The regional cybersecurity risk mitigation plans shall include: (a) the minimum and advanced cybersecurity controls that high-impact and critical-impact entities shall apply in the system operation region; (b) the residual cybersecurity risks in the system operation regions after applying the controls referred to in point (a).
3. The ENTSO for Electricity shall submit the regional risk mitigation plans to the relevant transmission system operators, to the competent authorities, and to the Electricity Coordination Group. The Electricity Coordination Group may recommend amendments.
4. The TSOs, with the assistance of the ENTSO for Electricity in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group shall update the regional risk mitigation plans every three years, unless circumstances warrant more frequent updates.

Article 22(1)

Within 36 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and no later than 13 June 2031, and every three years after that date, the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the Regional Coordination Centres and the NIS Cooperation Group, shall develop a regional cybersecurity risk mitigation plan for each system operation region.

Article 22(2)

The regional cybersecurity risk mitigation plans shall include:

a. the minimum and advanced cybersecurity controls that high-impact and critical-impact entities shall apply in the system operation region;

b. the residual cybersecurity risks in the system operation regions after applying the controls referred to in point (a).

Article 22(3)

The ENTSO for Electricity shall submit the regional risk mitigation plans to the relevant transmission system operators, to the competent authorities, and to the Electricity Coordination Group. The Electricity Coordination Group may recommend amendments.

Article 22(4)

The TSOs, with the assistance of the ENTSO for Electricity in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group shall update the regional risk mitigation plans every three years, unless circumstances warrant more frequent updates.

Article 23

1. Within 40 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and every three years thereafter, TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall provide to the Electricity Coordination Group a report on the outcome of the assessment of cybersecurity risks with regard to cross-border electricity flows (the comprehensive cross-border electricity cybersecurity risk assessment report)
2. The comprehensive cross-border electricity cybersecurity risk assessment report shall be based on the Union-wide cybersecurity risk assessment report, on the Member State cybersecurity risk assessment reports and on the regional cybersecurity risk assessment reports and include the following information: (a) the list of Union-wide high-impact and critical-impact processes identified in the Union-wide cybersecurity risk assessment report in accordance

with Article 19(2) point (a) including the estimation of likelihood and impact of cybersecurity risks evaluated during the regional cybersecurity risk assessment reports pursuant to Article 21(2) and Article 19(3) point (a); (b) current cyber threats, with a specific focus on emerging threats and risks for the electricity system; (c) cyber-attacks for the previous period at Union level, providing a critical overview of how such cyber-attacks may have had an impact on electricity cross-border flows; (d) overall status of implementation of the cybersecurity measures; (e) status of implementation of the information flows pursuant to Articles 37 and 38; (f) list of information or specific criteria for classification of information pursuant to Article 46; (g) identified and highlighted risks that may derive from insecure supply chain management; (h) results and accumulated experiences from regional and cross-regional cybersecurity exercises organised pursuant to Article 44; (i) an analysis of the development of the overall cross-border cybersecurity risks in the electricity sector since the last regional cybersecurity risk assessments; (j) any other information that may be useful to identify possible improvements of this Regulation or the need for a revision of this Regulation or any of its tools; and (k) aggregated and anonymised information of derogations granted pursuant to Article 30(3).

3. The entities listed in Article 2(1) may contribute to the development of the comprehensive cross-border electricity cybersecurity risk assessment report, respecting the confidentiality of information in accordance with Article 47. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall consult these entities from an early stage.

4. The comprehensive cross-border electricity cybersecurity risk assessment report shall be subject to the rules on protection of exchange of information pursuant to Article 46. Without prejudice to Article 10(4) and Article 47(4), the ENTSO for Electricity and the EU DSO entity shall release a public version of that report which shall not contain information that can cause damage to entities listed in Article 2(1).

5. The public version of this report shall only be released with the agreement of the NIS Cooperation Group and the Electricity Coordination Group. The ENTSO for Electricity in coordination with the EU DSO entity shall be responsible for the compilation and the release of the public version of the report.

Article 23(1)

Within 40 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and every three years thereafter, TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall provide to the Electricity Coordination Group a report on the outcome of the assessment of cybersecurity risks with regard to cross-border electricity flows (the 'comprehensive cross-border electricity cybersecurity risk assessment report')

Article 23(2)

The comprehensive cross-border electricity cybersecurity risk assessment report shall be based on the Union-wide cybersecurity risk assessment report, on the Member State cybersecurity risk

assessment reports and on the regional cybersecurity risk assessment reports and include the following information:

a. the list of Union-wide high-impact and critical-impact processes identified in the Union-wide cybersecurity risk assessment report in accordance with Article 19(2) point (a) including the estimation of likelihood and impact of cybersecurity risks evaluated during the regional cybersecurity risk assessment reports pursuant to Article 21(2) and Article 19(3) point (a);

b. current cyber threats, with a specific focus on emerging threats and risks for the electricity system;

c. cyber-attacks for the previous period at Union level, providing a critical overview of how such cyber-attacks may have had an impact on electricity cross-border flows;

d. overall status of implementation of the cybersecurity measures;

e. status of implementation of the information flows pursuant to Articles 37 and 38;

f. list of information or specific criteria for classification of information pursuant to Article 46;

g. identified and highlighted risks that may derive from insecure supply chain management;

h. results and accumulated experiences from regional and cross-regional cybersecurity exercises organised pursuant to Article 44;

i. an analysis of the development of the overall cross-border cybersecurity risks in the electricity sector since the last regional cybersecurity risk assessments;

j. any other information that may be useful to identify possible improvements of this Regulation or the need for a revision of this Regulation or any of its tools; and

k. aggregated and anonymised information of derogations granted pursuant to Article 30(3).

Article 23(3)

The entities listed in Article 2(1) may contribute to the development of the comprehensive cross-border electricity cybersecurity risk assessment report, respecting the confidentiality of information in accordance with Article 47. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall consult these entities from an early stage.

Article 23(4)

The comprehensive cross-border electricity cybersecurity risk assessment report shall be subject to the rules on protection of exchange of information pursuant to Article 46. Without prejudice to Article 10(4) and Article 47(4), the ENTSO for Electricity and the EU DSO entity shall release a public version of that report which shall not contain information that can cause damage to entities listed in Article 2(1).

The public version of this report shall only be released with the agreement of the NIS Cooperation Group and the Electricity Coordination Group. The ENTSO for Electricity in coordination with the EU DSO entity shall be responsible for the compilation and the release of the public version of the report.

Article 24

1. Each competent authority shall identify, by using the ECII and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3), point (b), the high-impact and critical- impact entities in its Member State that are involved in the Union-wide high-impact and critical-impact processes. The competent authorities can request information from an entity in their Member State to determine the ECII values for that entity. If the determined ECII of an entity is above the high-impact or critical-impact threshold, the identified entity shall be listed in the Member State cybersecurity risk assessment report referred to in Article 20(2).

2. Each competent authority shall identify, by using the ECII and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3), point (b), the high-impact and critical- impact entities not established in the Union in so far they are active within the Union. The competent authority may request information from an entity not established in the Union to determine the ECII values for the entity.

3. Each competent authority may identify additional entities in its Member State as high-impact or critical-impact entities if the following criteria are met: (a) the entity is part of a group of entities for which there is a significant risk that they will be affected simultaneously by a cyber-attack; (b) the ECII aggregated over the group of entities is above the high-impact or critical-impact threshold.

4. If a competent authority identifies additional entities in accordance with paragraph 3, all processes at these entities for which the ECII aggregated over the group are above the high-impact threshold shall be considered high-impact processes, and all processes at these entities for which the ECII aggregated over the group are above the critical-impact thresholds shall be considered critical-impact processes.

5. If a competent authority identifies entities referred to in paragraph 3 point (a) in more than one Member State, it shall inform the other competent authorities, the ENTSO for Electricity and the EU DSO entity.

6. The ENTSO for Electricity in cooperation with the EU DSO entity, based on the information received from all competent authorities, shall provide to the competent authorities an analysis of the aggregation of entities in more than one Member State that can create a distributed disturbance to the cross-border electricity flows, and can result in a cyber-attack.

7. Where a group of entities in several Member States is identified as an aggregation whose ECII is above the high-impact or critical-impact threshold, all concerned competent authorities shall identify the entities in such group as high-impact or critical-impact entities for their respective Member State, based on the aggregated ECII for the group of the entities, and the identified entities shall be listed in the Union-wide cybersecurity risk assessment report.

8. Each competent authority shall, within nine months after being notified by ENTSO for Electricity and EU DSO entity of the Union-wide cybersecurity risk assessment report pursuant to Article 19(5) and in any case no later than 13 June 2028, notify to the entities on the list that they have been identified as a high-impact or critical-impact entity in its Member State.
9. When a service provider is reported to a competent authority as being a critical ICT service provider pursuant to Article 27 point (c),
10. that competent authority shall notify it to the competent authorities of the Member States in whose territories the seat or representative is situated. The latter competent authority shall notify the service provider that it has been identified as being a critical service provider.

Article 24(1)

Each competent authority shall identify, by using the ECII and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3), point (b), the high-impact and critical- impact entities in its Member State that are involved in the Union-wide high-impact and critical-impact processes. The competent authorities can request information from an entity in their Member State to determine the ECII values for that entity. If the determined ECII of an entity is above the high-impact or critical-impact threshold, the identified entity shall be listed in the Member State cybersecurity risk assessment report referred to in Article 20(2).

Article 24(2)

Each competent authority shall identify, by using the ECII and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3), point (b), the high-impact and critical- impact entities not established in the Union in so far they are active within the Union. The competent authority may request information from an entity not established in the Union to determine the ECII values for the entity.

Article 24(3)

Each competent authority may identify additional entities in its Member State as high-impact or critical-impact entities if the following criteria are met:

a. the entity is part of a group of entities for which there is a significant risk that they will be affected simultaneously by a cyber-attack;
b. the ECII aggregated over the group of entities is above the high-impact or critical-impact threshold.

Article 24(4)

If a competent authority identifies additional entities in accordance with paragraph 3, all processes at these entities for which the ECII aggregated over the group are above the high-impact threshold shall be considered high-impact processes, and all processes at these entities for which the ECII aggregated over the group are above the critical-impact thresholds shall be considered critical-impact processes.

Article 24(5)

If a competent authority identifies entities referred to in paragraph 3 point (a) in more than one Member State, it shall inform the other competent authorities, the ENTSO for Electricity and the EU DSO entity.

The ENTSO for Electricity in cooperation with the EU DSO entity, based on the information received from all competent authorities, shall provide to the competent authorities an analysis of the aggregation of entities in more than one Member State that can create a distributed disturbance to the cross-border electricity flows, and can result in a cyber-attack.

Where a group of entities in several Member States is identified as an aggregation whose ECII is above the high-impact or critical-impact threshold, all concerned competent authorities shall identify the entities in such group as high-impact or critical-impact entities for their respective Member State, based on the aggregated ECII for the group of the entities, and the identified entities shall be listed in the Union-wide cybersecurity risk assessment report.

Article 24(6)

Each competent authority shall, within nine months after being notified by ENTSO for Electricity and EU DSO entity of the Union-wide cybersecurity risk assessment report pursuant to Article 19(5) and in any case no later than 13 June 2028, notify to the entities on the list that they have been identified as a high-impact or critical-impact entity in its Member State.

Article 24(7)

When a service provider is reported to a competent authority as being a critical ICT service provider pursuant to Article 27 point (c),

that competent authority shall notify it to the competent authorities of the Member States in whose territories the seat or representative is situated. The latter competent authority shall notify the service provider that it has been identified as being a critical service provider.

Article 25

1. The competent authorities may establish a national verification scheme to verify that critical-impact entities identified pursuant to Article 24(1) have implemented the national legislative framework that is included in the mapping matrix referred to in Article 34. The national ver-

ification scheme may be based on an inspection carried out by the competent authority, independent security audits, or on mutual peer reviews by critical-impact entities in the same Member State supervised by the competent authority.

2. If a competent authority decides to establish a national verification scheme, that competent authority shall ensure that the verification is performed in accordance with the following requirements: (a) any party performing the peer review, audit or inspection shall be independent from the critical-impact entity being verified, and shall have no conflicts of interest; (b) the staff performing the peer review, audit or inspection shall have demonstrable knowledge of: (i) cybersecurity in the electricity sector; (ii) cybersecurity management systems; (iii) the principles of auditing; (iv) cybersecurity risk assessment; (v) the common electricity cybersecurity framework; (vi) the national legislative and regulatory framework and European and international standards in scope of the verification; (vii) the critical-impact processes in scope of the verification; (c) the party performing the peer review, audit or inspection shall be allowed sufficient time to perform these activities; (d) the party performing the peer review, audit or inspection shall take the appropriate measures to protect the information they collect during the verification, in line with its confidentiality level; and (e) peer reviews, audits or inspections shall be performed at least once every year and cover the full verification scope at least every three years.

3. If a competent authority decides to establish a national verification scheme, it shall report to ACER on an annual basis how frequently it has carried out inspections under that scheme.

Article 25(1)

The competent authorities may establish a national verification scheme to verify that critical-impact entities identified pursuant to Article 24(1) have implemented the national legislative framework that is included in the mapping matrix referred to in Article 34. The national verification scheme may be based on an inspection carried out by the competent authority, independent security audits, or on mutual peer reviews by critical-impact entities in the same Member State supervised by the competent authority.

Article 25(2)

If a competent authority decides to establish a national verification scheme, that competent authority shall ensure that the verification is performed in accordance with the following requirements:

a. any party performing the peer review, audit or inspection shall be independent from the critical-impact entity being verified, and shall have no conflicts of interest;

b. the staff performing the peer review, audit or inspection shall have demonstrable knowledge of:

   i. cybersecurity in the electricity sector;

   ii. cybersecurity management systems;

iii. the principles of auditing;

iv. cybersecurity risk assessment;

v. the common electricity cybersecurity framework;

vi. the national legislative and regulatory framework and European and international standards in scope of the verification;

vii. the critical-impact processes in scope of the verification;

c. the party performing the peer review, audit or inspection shall be allowed sufficient time to perform these activities;

d. the party performing the peer review, audit or inspection shall take the appropriate measures to protect the information they collect during the verification, in line with its confidentiality level; and

e. peer reviews, audits or inspections shall be performed at least once every year and cover the full verification scope at least every three years.

Article 25(3)

If a competent authority decides to establish a national verification scheme, it shall report to ACER on an annual basis how frequently it has carried out inspections under that scheme.

Article 26

1. Each high-impact and critical-impact entity as identified by the competent authorities pursuant to Article 24(1) shall perform cybersecurity risk management for all its assets in its high-impact and critical-impact perimeters. Each high-impact and critical-impact entity shall perform risk management containing the phases in paragraph 2 every three years.

2. Each high-impact and critical-impact entity shall base its cybersecurity risk management on an approach that aims to protect their network and information systems and that comprises the following phases: (a) context establishment; (b) cybersecurity risk assessment at entity level; (c) cybersecurity risk treatment; (d) cybersecurity risk acceptance.

3. During the context establishment phase, each high-impact and critical-impact entity shall: (a) define the scope of the cybersecurity risk assessment including the high-impact and critical-impact processes identified by the ENTSO for Electricity and the EU DSO entity, and other processes that may be targets of cyber- attacks with a high-impact or critical-impact on cross-border electricity flows; and (b) define the criteria for risk evaluation and for risk acceptance in accordance with the risk impact matrix that entities and the competent authorities shall use to assess the cybersecurity risks in the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by the ENTSO for Electricity and the EU DSO entity in accordance with Article 19(2).

4. During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall: (a) identify cybersecurity risks by taking into account: (i) all assets supporting the Union-wide high-impact and critical-impact processes with an assessment of the possible impact on cross-border electricity flows if the asset is compromised; (ii) possible cyber threats taking into account the cyber threats identified in the latest Comprehensive cross-border electricity cybersecurity risk assessment report referred to in Article 23 and supply chain threats; (iii) vulnerabilities, including vulnerabilities in legacy systems; (iv) possible cyber-attack scenarios, including cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows; (v) relevant risk evaluations and assessments carried out at Union level, including coordinated risk assessments of critical supply chains in accordance with Article 22 of Directive (EU) 2022/2555; and (vi) existing implemented controls; (b) analyse the likelihood and consequences of the cybersecurity risks identified in point (a) and determine the cybersecurity risk level using the risk impact matrix used to assess cybersecurity risks in cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity in accordance with Article 19(2); (c) classify assets according to the possible consequences when cybersecurity is compromised and determine the high- impact and critical-impact perimeter using the following steps: (i) perform, for all processes covered by the cybersecurity risk assessment, a business impact assessment using the ECII; (ii) classify a process as high-impact or critical-impact if its ECII is above the high-impact or critical-impact threshold respectively; (iii) determine all high-impact and critical-impact assets as the assets needed for the high-impact and critical- impact processes respectively; (iv) define the high-impact and critical-impact perimeters containing all high-impact and critical-impact assets respectively, so that access to the perimeters may be controlled; (d) evaluate cybersecurity risks by prioritising them through risk evaluation criteria and risk acceptance criteria referred to in paragraph 3 point (b).
5. During the cybersecurity risk treatment phase, each high-impact and critical-impact entity shall establish an entity- level risk mitigation plan by selecting risk treatment options appropriate to manage the risks and identify the residual risks.
6. During the cybersecurity risk acceptance phase, each high-impact and critical-impact entity shall decide whether to accept the residual risk based on the risk acceptance criteria established in paragraph 3 point (b).
7. Each high-impact and critical-impact entity shall register the assets identified in paragraph 1 in an asset inventory. That asset inventory shall not be part of the risk assessment report.
8. The competent authority may inspect the assets in the inventory during inspections.

Article 26(1)

Each high-impact and critical-impact entity as identified by the competent authorities pursuant to Article 24(1) shall perform cybersecurity risk management for all its assets in its high-impact and critical-impact perimeters. Each high-impact and critical-impact entity shall perform risk management containing the phases in paragraph 2 every three years.

Article 26(2)

Each high-impact and critical-impact entity shall base its cybersecurity risk management on an approach that aims to protect their network and information systems and that comprises the following phases:

a. context establishment;

b. cybersecurity risk assessment at entity level;

c. cybersecurity risk treatment;

d. cybersecurity risk acceptance.

Article 26(3)

During the context establishment phase, each high-impact and critical-impact entity shall:

a. define the scope of the cybersecurity risk assessment including the high-impact and critical-impact processes identified by the ENTSO for Electricity and the EU DSO entity, and other processes that may be targets of cyber- attacks with a high-impact or critical-impact on cross-border electricity flows; and

b. define the criteria for risk evaluation and for risk acceptance in accordance with the risk impact matrix that entities and the competent authorities shall use to assess the cybersecurity risks in the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by the ENTSO for Electricity and the EU DSO entity in accordance with Article 19(2).

Article 26(4)

During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

a. identify cybersecurity risks by taking into account:

    i. all assets supporting the Union-wide high-impact and critical-impact processes with an assessment of the possible impact on cross-border electricity flows if the asset is compromised;

    ii. possible cyber threats taking into account the cyber threats identified in the latest Comprehensive cross- border electricity cybersecurity risk assessment report referred to in Article 23 and supply chain threats;

    iii. vulnerabilities, including vulnerabilities in legacy systems;

    iv. possible cyber-attack scenarios, including cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows;

v. relevant risk evaluations and assessments carried out at Union level, including coordinated risk assessments of critical supply chains in accordance with Article 22 of Directive (EU) 2022/2555; and

vi. existing implemented controls;

b. analyse the likelihood and consequences of the cybersecurity risks identified in point (a) and determine the cybersecurity risk level using the risk impact matrix used to assess cybersecurity risks in cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity in accordance with Article 19(2);

c. classify assets according to the possible consequences when cybersecurity is compromised and determine the high- impact and critical-impact perimeter using the following steps:

i. perform, for all processes covered by the cybersecurity risk assessment, a business impact assessment using the ECII;

ii. classify a process as high-impact or critical-impact if its ECII is above the high-impact or critical-impact threshold respectively;

iii. determine all high-impact and critical-impact assets as the assets needed for the high-impact and critical- impact processes respectively;

iv. define the high-impact and critical-impact perimeters containing all high-impact and critical-impact assets respectively, so that access to the perimeters may be controlled;

d. evaluate cybersecurity risks by prioritising them through risk evaluation criteria and risk acceptance criteria referred to in paragraph 3 point (b).

Article 26(5)

During the cybersecurity risk treatment phase, each high-impact and critical-impact entity shall establish an entity- level risk mitigation plan by selecting risk treatment options appropriate to manage the risks and identify the residual risks.

Article 26(6)

During the cybersecurity risk acceptance phase, each high-impact and critical-impact entity shall decide whether to accept the residual risk based on the risk acceptance criteria established in paragraph 3 point (b).

Article 26(7)

Each high-impact and critical-impact entity shall register the assets identified in paragraph 1 in an asset inventory. That asset inventory shall not be part of the risk assessment report.

Article 26(8)

The competent authority may inspect the assets in the inventory during inspections.

Article 27

1. Each high-impact and critical-impact entity shall, within 12 months after the notification of the high-and critical-impact entities pursuant to Article 24(6), and every three years thereafter, provide to the competent authority a report containing the following information: (1) a list of controls selected for the entity-level risk mitigation plan pursuant to Article 26(5) with the current implementation status of each control; (2) for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity, and availability of information and relevant assets. The estimate of this risk shall be given in accordance with the risk impact matrix in Article 19(2); (3) a list of critical ICT service providers for their critical-impact processes.

Article 27(1)

Each high-impact and critical-impact entity shall, within 12 months after the notification of the high-and critical-impact entities pursuant to Article 24(6), and every three years thereafter, provide to the competent authority a report containing the following information:

1. a list of controls selected for the entity-level risk mitigation plan pursuant to Article 26(5) with the current implementation status of each control;
2. for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity, and availability of information and relevant assets. The estimate of this risk shall be given in accordance with the risk impact matrix in Article 19(2);
3. a list of critical ICT service providers for their critical-impact processes.

Article 28

1. The common electricity cybersecurity framework shall be composed of the following controls and cybersecurity management system: (a) the minimum cybersecurity controls, developed in accordance with Article 29; (c) the mapping matrix, developed in accordance with Article 34, that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks; (d) the cybersecurity management system established pursuant to Article 32.
2. The common electricity cybersecurity framework shall be composed of the following controls and cybersecurity management system: (a) the minimum cybersecurity controls, developed in accordance with Article 29; (b) the advanced cybersecurity controls, developed in accordance with Article 29; (c) the mapping matrix, developed in accordance with Article 34,

that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks; (d) the cybersecurity management system established pursuant to Article 32.

3. All high-impact entities shall apply the minimum cybersecurity controls pursuant to paragraph 1 point (a) within their high-impact perimeter.
4. All critical-impact entities shall apply the minnimal and advanced cybersecurity controls pursuant to paragraph 1 point (b) within their critical-impact perimeter.
5. Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the common electricity cybersecurity framework referred to in paragraph 1 shall be supplemented by the minimum and advanced cybersecurity controls in the supply chain developed pursuant to Article 33.

Article 28(1)

The common electricity cybersecurity framework shall be composed of the following controls and cybersecurity management system:

a. the minimum cybersecurity controls, developed in accordance with Article 29;
b. the mapping matrix, developed in accordance with Article 34, that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks;
c. the cybersecurity management system established pursuant to Article 32.

The common electricity cybersecurity framework shall be composed of the following controls and cybersecurity management system:

a. the minimum cybersecurity controls, developed in accordance with Article 29;
b. the advanced cybersecurity controls, developed in accordance with Article 29;
c. the mapping matrix, developed in accordance with Article 34, that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks;
d. the cybersecurity management system established pursuant to Article 32.

Article 28(2)

All high-impact entities shall apply the minimum cybersecurity controls pursuant to paragraph 1 point (a) within their high-impact perimeter.

Article 28(3)

All critical-impact entities shall apply the minnimal and advanced cybersecurity controls pursuant to paragraph 1 point (b) within their critical-impact perimeter.

Article 28(4)

Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the common electricity cybersecurity framework referred to in paragraph 1 shall be supplemented by the minimum and advanced cybersecurity controls in the supply chain developed pursuant to Article 33.

Article 29

1. Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall develop a proposal for minimum and advanced cybersecurity controls.
2. Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall propose an amendment to the competent authority for the minimum and advanced cybersecurity controls. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.
3. The minimum and advanced cybersecurity controls shall be verifiable by taking part in a national verification scheme in accordance with the procedure set out in Article 31 or by undergoing independent third-party security audits performed according to the requirements listed in Article 25(2).
4. The initial minimum and advanced cybersecurity controls developed pursuant to paragraph (1) shall be based on the risks that are identified in the Union-wide cybersecurity risk assessment report referred to in Article 19(5). The amended minimum and advanced cybersecurity controls developed pursuant to paragraph (2) shall be based on the regional cybersecurity risk assessment report referred to in Article 21(2).
5. The minimum cybersecurity controls shall include controls to protect the information exchanged pursuant to Article 46.
6. Within 12 months after the approval of the minimum and advanced cybersecurity controls pursuant to Article 8(5), or after each update pursuant to Article 8(10), the entities listed in Article 2(1) and identified as critical-impact and high- impact entities pursuant to Article 24 shall, during the establishment of the entity-level risk mitigation plan pursuant to Article 26(5), apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

7. Within 12 months after the approval of the minimum and advanced cybersecurity controls pursuant to Article 8(5), or after each update pursuant to Article 8(10), the entities listed in Article 2(1) and identified as critical-impact and high- impact entities pursuant to Article 24 shall, during the establishment of the entity-level risk mitigation plan pursuant to Article 26(5), apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Article 29(1)

Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall develop a proposal for minimum and advanced cybersecurity controls.

Article 29(2)

Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall propose an amendment to the competent authority for the minimum and advanced cybersecurity controls. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Article 29(3)

The minimum and advanced cybersecurity controls shall be verifiable by taking part in a national verification scheme in accordance with the procedure set out in Article 31 or by undergoing independent third-party security audits performed according to the requirements listed in Article 25(2).

Article 29(4)

The initial minimum and advanced cybersecurity controls developed pursuant to paragraph (1) shall be based on the risks that are identified in the Union-wide cybersecurity risk assessment report referred to in Article 19(5). The amended minimum and advanced cybersecurity controls developed pursuant to paragraph (2) shall be based on the regional cybersecurity risk assessment report referred to in Article 21(2).

Article 29(5)

The minimum cybersecurity controls shall include controls to protect the information exchanged pursuant to Article 46.

Article 29(6)

Within 12 months after the approval of the minimum and advanced cybersecurity controls pursuant to Article 8(5), or after each update pursuant to Article 8(10), the entities listed in Article 2(1) and identified as critical-impact and high- impact entities pursuant to Article 24 shall, during the establishment of the entity-level risk mitigation plan pursuant to Article 26(5), apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Within 12 months after the approval of the minimum and advanced cybersecurity controls pursuant to Article 8(5), or after each update pursuant to Article 8(10), the entities listed in Article 2(1) and identified as critical-impact and high- impact entities pursuant to Article 24 shall, during the establishment of the entity-level risk mitigation plan pursuant to Article 26(5), apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Article 30

1. The entities listed in Article 2(1) may request the respective competent authority to grant a derogation from their obligation to apply the minimum and advanced cybersecurity controls referred to in Article 29(6).
2. The entities listed in Article 2(1) may request the respective competent authority to grant a derogation from their obligation to apply the minimum and advanced cybersecurity controls referred to in Article 29(6). The competent authority may grant such a derogation on one of the following grounds: (a) in exceptional circumstances, where the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefits. ACER and the ENTSO for Electricity in cooperation with the DSO entity may jointly develop a guidance for estimating the costs of cybersecurity controls to help the entities; (b) where the entity provides an entity-level risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable in accordance with to the risk acceptance criteria referred to Article 26(3), point (b).
3. Within three months from the receipt of the request referred to in paragraph 1, each competent authority shall decide whether a derogation from the minimum and advanced cybersecurity controls is to be granted. Derogations from the minimum or advanced cybersecurity controls shall be granted for a maximum of three years, with the possibility of renewal.
4. Aggregated and anonymised information for the derogations granted shall be included as an annex to the comprehensive cross-border electricity cybersecurity risk assessment report referred to in Article 23. The ENTSO for Electricity and the EU DSO entity shall jointly update the list, where necessary.

Article 30(1)

The entities listed in Article 2(1) may request the respective competent authority to grant a dero-

gation from their obligation to apply the minimum and advanced cybersecurity controls referred to in Article 29(6).

The entities listed in Article 2(1) may request the respective competent authority to grant a derogation from their obligation to apply the minimum and advanced cybersecurity controls referred to in Article 29(6). The competent authority may grant such a derogation on one of the following grounds:

a. in exceptional circumstances, where the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefits. ACER and the ENTSO for Electricity in cooperation with the DSO entity may jointly develop a guidance for estimating the costs of cybersecurity controls to help the entities;
b. where the entity provides an entity-level risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable in accordance with to the risk acceptance criteria referred to Article 26(3), point (b).

Article 30(2)

Within three months from the receipt of the request referred to in paragraph 1, each competent authority shall decide whether a derogation from the minimum and advanced cybersecurity controls is to be granted. Derogations from the minimum or advanced cybersecurity controls shall be granted for a maximum of three years, with the possibility of renewal.

Article 30(3)

Aggregated and anonymised information for the derogations granted shall be included as an annex to the comprehensive cross-border electricity cybersecurity risk assessment report referred to in Article 23. The ENTSO for Electricity and the EU DSO entity shall jointly update the list, where necessary.

Article 31

1. No later than 24 months after the adoption of the controls referred to in points (a), (b) and (c) of Article 28(1) and the establishment of the cybersecurity management system referred to in point (d) of that Article, each critical-impact entity identified in accordance with Article 24(1) shall be able to demonstrate its compliance with the cybersecurity management system and the minimum or advanced cybersecurity controls at the request of the competent authority.
2. Each critical-impact entity shall fulfil the obligation referred to in paragraph 1 by undergoing independent third- party security audits in accordance with the requirements listed in Article 25(2) or by taking part in a national verification scheme in accordance with Article 25(1).
3. The verification that a critical-impact entity complies with the cybersecurity management system and the minimum or advanced cybersecurity controls shall cover all assets within the critical-impact perimeter of the critical-impact entity.

4. The verification that a critical-impact entity complies with the cybersecurity management system and the minimum or advanced cybersecurity controls shall be regularly repeated at the latest 36 months after the end of the first verification, and every 3 years thereafter.
5. Each critical-impact entity defined in accordance with Article 24 shall demonstrate its compliance with the controls referred to in points (a), (b) and (c) of Article 28(1) and the establishment of the cybersecurity management system referred to in point (d) of that Article by reporting on the outcome of the compliance verification to the competent authority.

Article 31(1)

No later than 24 months after the adoption of the controls referred to in points (a), (b) and (c) of Article 28(1) and the establishment of the cybersecurity management system referred to in point (d) of that Article, each critical-impact entity identified in accordance with Article 24(1) shall be able to demonstrate its compliance with the cybersecurity management system and the minimum or advanced cybersecurity controls at the request of the competent authority.

Article 31(2)

Each critical-impact entity shall fulfil the obligation referred to in paragraph 1 by undergoing independent third- party security audits in accordance with the requirements listed in Article 25(2) or by taking part in a national verification scheme in accordance with Article 25(1).

Article 31(3)

The verification that a critical-impact entity complies with the cybersecurity management system and the minimum or advanced cybersecurity controls shall cover all assets within the critical-impact perimeter of the critical-impact entity.

Article 31(4)

The verification that a critical-impact entity complies with the cybersecurity management system and the minimum or advanced cybersecurity controls shall be regularly repeated at the latest 36 months after the end of the first verification, and every 3 years thereafter.

Article 31(5)

Each critical-impact entity defined in accordance with Article 24 shall demonstrate its compliance with the controls referred to in points (a), (b) and (c) of Article 28(1) and the establishment of the cybersecurity management system referred to in point (d) of that Article by reporting on the outcome of the compliance verification to the competent authority.

Article 32

1. Within 24 months after being notified by the competent authority that they have been identified as a high-impact or critical-impact entity in accordance with Article 24(6), each high-impact and critical-impact entity shall establish a cybersecurity management system, and review it every three years thereafter, to: (a) determine the scope of the cybersecurity management system considering interfaces and dependencies with other entities; (b) ensure that all its senior management is informed of relevant legal obligations and actively contributes to the implementation of the cybersecurity management system through timely decisions and prompt reactions; (c) ensure that the resources needed for the cybersecurity management system are available; (d) establish a cybersecurity policy that shall be documented and communicated within the entity and to parties affected by the security risks; (e) assign and communicate responsibilities for roles relevant to cybersecurity; (f) perform cybersecurity risk management at entity level as defined in Article 26; (g) determine and provide the resources required for the implementation, maintenance and continual improvement of the cybersecurity management system, taking into account the necessary competence and awareness of cybersecurity resources; (h) determine the internal and external communication that is relevant to cybersecurity; (i) create, update and control documented information related to the cybersecurity management system; (j) evaluate the performance and effectiveness of the cybersecurity management system; (k) conduct internal audits at planned intervals to ensure that the cybersecurity management system is effectively implemented and maintained; (l) review the implementation of the cybersecurity management system at planned intervals; and control and correct non-compliance of the resources and activities with the policies, procedures, guidelines in the cybersecurity management system.
2. The scope of the cybersecurity management system shall include all assets within the high-impact perimeter of the high-impact entity.
3. The competent authorities shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or international standards and specifications related to management systems and relevant to the security of network and information systems.

Article 32(1)

Within 24 months after being notified by the competent authority that they have been identified as a high-impact or critical-impact entity in accordance with Article 24(6), each high-impact and critical-impact entity shall establish a cybersecurity management system, and review it every three years thereafter, to:

a. determine the scope of the cybersecurity management system considering interfaces and dependencies with other entities;
b. ensure that all its senior management is informed of relevant legal obligations and actively contributes to the implementation of the cybersecurity management system through timely decisions and prompt reactions;

c. ensure that the resources needed for the cybersecurity management system are available;

d. establish a cybersecurity policy that shall be documented and communicated within the entity and to parties affected by the security risks;

e. assign and communicate responsibilities for roles relevant to cybersecurity;

f. perform cybersecurity risk management at entity level as defined in Article 26;

g. determine and provide the resources required for the implementation, maintenance and continual improvement of the cybersecurity management system, taking into account the necessary competence and awareness of cybersecurity resources;

h. determine the internal and external communication that is relevant to cybersecurity;

i. create, update and control documented information related to the cybersecurity management system;

j. evaluate the performance and effectiveness of the cybersecurity management system;

k. conduct internal audits at planned intervals to ensure that the cybersecurity management system is effectively implemented and maintained;

l. review the implementation of the cybersecurity management system at planned intervals; and control and correct non-compliance of the resources and activities with the policies, procedures, guidelines in the cybersecurity management system.

Article 32(2)

The scope of the cybersecurity management system shall include all assets within the high-impact perimeter of the high-impact entity.

Article 32(3)

The competent authorities shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or international standards and specifications related to management systems and relevant to the security of network and information systems.

Article 33

1. Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop a proposal for minimum and advanced cybersecurity controls in the supply chain that mitigate the supply chain risks identified in the Union-wide cybersecurity risk assessments, supplementing the minimum and advanced

cybersecurity controls developed pursuant to Article 29. The minimum and advanced cybersecurity controls in the supply chain shall be developed together with the minimum and advanced cybersecurity controls pursuant to Article 29. The minimum and advanced cybersecurity controls in the supply chain shall cover the entire lifecycle of all ICT products, ICT services and ICT processes inside the high-impact or critical-impact perimeters of a high-impact or critical-impact entity. The NIS Cooperation Group shall be consulted when developing the proposal for minimum and advanced cybersecurity controls in the supply chain.

2. The minimum cybersecurity controls in the supply chain shall consist of controls for high-impact and critical-impact entities that: (a)include recommendations for the procurement of ICT products, ICT services, and ICT processes referring to cybersecurity specifications, covering at least: (i)the background verification checks of the staff of the supplier involved in the supply chain and dealing with sensitive information or with access to the high-impact or critical-impact assets of the entity. Background verification check may include a verification of the identity and background of staff or contractors of an entity in accordance with national law and procedures and relevant and applicable Union law, including Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council(18). Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the entity concerned. They need to be proportional to business requirements, the classification of the information to be accessed and the perceived risks, and may be performed by the entity itself, by an external company performing a screening, or through a government clearing; (ii)the processes for secure and controlled design, development and production of ICT products, ICT services and ICT processes, promoting the design and development of ICT products, ICT services, and ICT processes, which include appropriate technical measures to ensure cybersecurity; (iii)design of network and information systems in which devices are not trusted even when they are within a secure perimeter, require verification of all requests they receive and apply the least privilege principle; (iv) the access of the supplier to the assets of the entity; (v) the contractual obligations on the supplier to protect and restrict access to the entity s sensitive information; (vi) the underpinning cybersecurity procurement specifications to subcontractors of the supplier; (vii) the traceability of the application of the cybersecurity specifications from the development through production until delivery of ICT products, ICT services or ICT processes; (viii) the support for security updates throughout the entire lifetime of ICT products, ICT services or ICT processes; (ix) the right to audit cybersecurity in the design, development and production processes of the supplier; and (x) the assessment of the risk profile of the supplier; (b) require such entities to take into account the procurement recommendations referred to in subparagraph (a) when concluding contracts with suppliers, collaboration partners and other parties in the supply chain, covering ordinary deliveries of ICT products, ICT services and ICT processes as well as unsolicited events and circumstances like termination and transition of contracts in cases of negligence of the contractual partner; (c) require such entities to take into account the results of relevant coordinated security risk assessments of critical

3. For the cybersecurity specifications in the cybersecurity procurement recommendation referred to in paragraph 2, point (a), high-impactentities shall use the principles of procurement pursuant to Directive 2014/24/EU of the European Parliament and of the Council(19), in accordance with Article 35(4), or define their own specifications based on the results of the cybersecurity risk assessment at entity level.

4. For the cybersecurity specifications in the cybersecurity procurement recommendation re-

ferred to in paragraph 2, point (a), critical entities shall use the principles of procurement pursuant to Directive 2014/24/EU of the European Parliament and of the Council(19), in accordance with Article 35(4), or define their own specifications based on the results of the cybersecurity risk assessment at entity level.

5. The advanced cybersecurity controls in the supply chain shall include controls for critical-impact entities to verify, during procurement, that ICT products, ICT services and ICT processes that will be used as critical-impact assets satisfy the cybersecurity specifications. The ICT product, ICT service or ICT process shall be verified either through a European cybersecurity certification scheme referred to in Article 31 or through verification activities selected and organised by the entity. The depth and coverage of the verification activities shall be sufficient to provide assurance that the ICT product, ICT service or ICT process can be used to mitigate the risks identified in the risk assessment at entity level. The critical- impact entity shall document the steps taken to reduce the risks identified.

6. The minimum cybersecurity controls in the supply chain shall apply to the procurement of relevant ICT product, ICT services and ICT processes. The minimum cybersecurity controls of the supply chain will apply to procurement processes in the entities identified as high-impact entities pursuant to Article 24 that starts six months after the adoption or update of the minimum cybersecurity controls referred to in Article 29.

7. The minimum and advanced cybersecurity controls in the supply chain shall apply to the procurement of relevant ICT product, ICT services and ICT processes. The minimum and advanced cybersecurity controls of the supply chain will apply to procurement processes in the entities identified as critical-impact entities pursuant to Article 24 that starts six months after the adoption or update of the minimum and advanced cybersecurity controls referred to in Article 29.

8. Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall propose an amendment to the competent authority for the minimum and advanced cybersecurity controls in the supply chain. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Article 33(1)

Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop a proposal for minimum and advanced cybersecurity controls in the supply chain that mitigate the supply chain risks identified in the Union-wide cybersecurity risk assessments, supplementing the minimum and advanced cybersecurity controls developed pursuant to Article 29. The minimum and advanced cybersecurity controls in the supply chain shall be developed together with the minimum and advanced cybersecurity controls pursuant to Article 29. The minimum and advanced cybersecurity controls in the supply chain shall cover the entire lifecycle of all ICT products, ICT services and ICT processes inside the high-impact or critical-impact perimeters of a high-impact or critical-impact entity. The NIS Cooperation Group shall be consulted when developing the proposal for minimum and advanced cybersecurity controls in the supply chain.

Article 33(2)

The minimum cybersecurity controls in the supply chain shall consist of controls for high-impact and critical-impact entities that:

i. the background verification checks of the staff of the supplier involved in the supply chain and dealing with sensitive information or with access to the high-impact or critical-impact assets of the entity. Background verification check may include a verification of the identity and background of staff or contractors of an entity in accordance with national law and procedures and relevant and applicable Union law, including Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council(18). Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the entity concerned. They need to be proportional to business requirements, the classification of the information to be accessed and the perceived risks, and may be performed by the entity itself, by an external company performing a screening, or through a government clearing;

ii. the processes for secure and controlled design, development and production of ICT products, ICT services and ICT processes, promoting the design and development of ICT products, ICT services, and ICT processes, which include appropriate technical measures to ensure cybersecurity;

iii. design of network and information systems in which devices are not trusted even when they are within a secure perimeter, require verification of all requests they receive and apply the least privilege principle;

iv. the access of the supplier to the assets of the entity;

v. the contractual obligations on the supplier to protect and restrict access to the entity's sensitive information;

vi. the underpinning cybersecurity procurement specifications to subcontractors of the supplier;

vii. the traceability of the application of the cybersecurity specifications from the development through production until delivery of ICT products, ICT services or ICT processes;

viii. the support for security updates throughout the entire lifetime of ICT products, ICT services or ICT processes;

ix. the right to audit cybersecurity in the design, development and production processes of the supplier; and

x. the assessment of the risk profile of the supplier;

    1. require such entities to take into account the procurement recommendations referred to in subparagraph (a) when concluding contracts with suppliers, collaboration partners and other parties in the supply chain, covering ordinary deliveries of ICT products, ICT services and ICT processes as well as unsolicited events and circumstances like termination and transition of contracts in cases of negligence of the contractual partner;
    2. require such entities to take into account the results of relevant coordinated security risk assessments of critical

Article 33(3)

For the cybersecurity specifications in the cybersecurity procurement recommendation referred to in paragraph 2, point (a), high-impactentities shall use the principles of procurement pursuant to Directive 2014/24/EU of the European Parliament and of the Council(19), in accordance with Article 35(4), or define their own specifications based on the results of the cybersecurity risk assessment at entity level.

For the cybersecurity specifications in the cybersecurity procurement recommendation referred to in paragraph 2, point (a), critical entities shall use the principles of procurement pursuant to Directive 2014/24/EU of the European Parliament and of the Council(19), in accordance with Article 35(4), or define their own specifications based on the results of the cybersecurity risk assessment at entity level.

Article 33(4)

The advanced cybersecurity controls in the supply chain shall include controls for critical-impact entities to verify, during procurement, that ICT products, ICT services and ICT processes that will be used as critical-impact assets satisfy the cybersecurity specifications. The ICT product, ICT service or ICT process shall be verified either through a European cybersecurity certification scheme referred to in Article 31 or through verification activities selected and organised by the entity. The depth and coverage of the verification activities shall be sufficient to provide assurance that the ICT product, ICT service or ICT process can be used to mitigate the risks identified in the risk assessment at entity level. The critical- impact entity shall document the steps taken to reduce the risks identified.

Article 33(5)

The minimum cybersecurity controls in the supply chain shall apply to the procurement of relevant ICT product, ICT services and ICT processes. The minimum cybersecurity controls of the supply chain will apply to procurement processes in the entities identified as high-impact entities pursuant to Article 24 that starts six months after the adoption or update of the minimum cybersecurity controls referred to in Article 29.

The minimum and advanced cybersecurity controls in the supply chain shall apply to the procurement of relevant ICT product, ICT services and ICT processes. The minimum and advanced cybersecurity controls of the supply chain will apply to procurement processes in the entities identified as critical-impact entities pursuant to Article 24 that starts six months after the adoption or update of the minimum and advanced cybersecurity controls referred to in Article 29.

Article 33(6)

Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall propose an amendment to the competent authority for the minimum and

advanced cybersecurity controls in the supply chain. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Article 34

1. Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity and in consultation with ENISA, shall develop a proposal for a matrix to map the controls set out in Article 28(1), points (a) and (b) against selected European and international standards as well as relevant technical specifications (the mapping matrix). The ENTSO for Electricity and the EU DSO entity shall document the equivalence of the different controls with the controls set out in Article 28(1), points (a) and (b).
2. The ENTSO for Electricity and the EU DSO entity shall document the equivalence of the different controls with the controls set out in Article 28(1), points (a) and (b).
3. The competent authorities may provide to the ENTSO for Electricity and the EU DSO entity a mapping of the controls set out in Article 28(1), points (a) and (b) with a reference to the related national legislative or regulatory frameworks, including relevant national standards of Member States pursuant to Article 25 of Directive (EU) 2022/2555. If the competent authority of a Member State provides such a mapping,
4. the ENTSO for Electricity and the EU DSO entity shall integrate this national mapping into the mapping-matrix.
5. Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity and in consultation with ENISA, shall propose an amendment to the competent authority for mapping matrix. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Article 34(1)

Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity and in consultation with ENISA, shall develop a proposal for a matrix to map the controls set out in Article 28(1), points (a) and (b) against selected European and international standards as well as relevant technical specifications (‘the mapping matrix’). The ENTSO for Electricity and the EU DSO entity shall document the equivalence of the different controls with the controls set out in Article 28(1), points (a) and (b).

The ENTSO for Electricity and the EU DSO entity shall document the equivalence of the different controls with the controls set out in Article 28(1), points (a) and (b).

Article 34(2)

The competent authorities may provide to the ENTSO for Electricity and the EU DSO entity a mapping of the controls set out in Article 28(1), points (a) and (b) with a reference to the related national legislative or regulatory frameworks, including relevant national standards of Member States pursuant to Article 25 of Directive (EU) 2022/2555. If the competent authority of a Member State provides such a mapping,

the ENTSO for Electricity and the EU DSO entity shall integrate this national mapping into the mapping-matrix.

Article 34(3)

Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity and in consultation with ENISA, shall propose an amendment to the competent authority for mapping matrix. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Article 35

1. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop, in a work programme to be established and updated each time a regional cybersecurity risk assessment report is adopted, sets of non-binding cybersecurity procurement recommendations that high-impact and critical-impact entities may use as a basis for the procurement of ICT products, ICT services and ICT processes in the high-impact and critical-impact perimeters. This work programme shall include the following: (a) a description and classification of the types of ICT products, ICT services and ICT processes used by high-impact and critical-impact entities in the high-impact and critical-impact perimeter; (b) a list of the types of ICT products, ICT services, and ICT processes for which a set of non-binding cybersecurity recommendations shall be developed based on the relevant regional cybersecurity risk assessment reports and on the priorities of high-impact and critical-impact entities.
2. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall, within 6 months after the adoption or update of the regional cybersecurity risk assessment report provide ACER with a summary of that work programme.
3. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall endeavour to ensure that the non-binding cybersecurity procurement recommendations developed based on the relevant regional cybersecurity risk assessment are similar or comparable across system operation regions. The sets of cybersecurity procurement recommendations shall cover at least the specifications referred to in Article 33(2), point (a). Where possible, the specifications shall be selected from European and international standards.
4. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall ensure that the sets of cybersecurity procurement recommendations: (a) comply with the principles of procurement pursuant to Directive 2014/24/EU; and (b) are

compatible with and take into account the most recent available European cybersecurity certification schemes relevant to the ICT product, ICT service, or ICT process.

Article 35(1)

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop, in a work programme to be established and updated each time a regional cybersecurity risk assessment report is adopted, sets of non-binding cybersecurity procurement recommendations that high-impact and critical-impact entities may use as a basis for the procurement of ICT products, ICT services and ICT processes in the high-impact and critical-impact perimeters. This work programme shall include the following:

a. a description and classification of the types of ICT products, ICT services and ICT processes used by high-impact and critical-impact entities in the high-impact and critical-impact perimeter;
b. a list of the types of ICT products, ICT services, and ICT processes for which a set of non-binding cybersecurity recommendations shall be developed based on the relevant regional cybersecurity risk assessment reports and on the priorities of high-impact and critical-impact entities.

Article 35(2)

The ENTSO for Electricity, in cooperation with the EU DSO entity, shall, within 6 months after the adoption or update of the regional cybersecurity risk assessment report provide ACER with a summary of that work programme.

Article 35(3)

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall endeavour to ensure that the non-binding cybersecurity procurement recommendations developed based on the relevant regional cybersecurity risk assessment are similar or comparable across system operation regions. The sets of cybersecurity procurement recommendations shall cover at least the specifications referred to in Article 33(2), point (a). Where possible, the specifications shall be selected from European and international standards.

Article 35(4)

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall ensure that the sets of cybersecurity procurement recommendations:

a. comply with the principles of procurement pursuant to Directive 2014/24/EU; and

b. are compatible with and take into account the most recent available European cybersecurity certification schemes relevant to the ICT product, ICT service, or ICT process.

Article 36

1. The non-binding cybersecurity procurement recommendations developed pursuant to Article 35 may include sector-specific guidance on the use of European cybersecurity certification schemes, whenever a suitable scheme is available for a type of ICT product, ICT service or ICT process used by critical-impact entities, without prejudice to the framework for the establishment of European cybersecurity certification schemes pursuant to Article 46 of Regulation (EU) 2019/881.
2. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall closely cooperate with ENISA in providing the sector-specific guidance included in non-binding cybersecurity procurement recommendations pursuant to paragraph 1.

Article 36(1)

The non-binding cybersecurity procurement recommendations developed pursuant to Article 35 may include sector-specific guidance on the use of European cybersecurity certification schemes, whenever a suitable scheme is available for a type of ICT product, ICT service or ICT process used by critical-impact entities, without prejudice to the framework for the establishment of European cybersecurity certification schemes pursuant to Article 46 of Regulation (EU) 2019/881.

Article 36(2)

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall closely cooperate with ENISA in providing the sector-specific guidance included in non-binding cybersecurity procurement recommendations pursuant to paragraph 1.

Article 37

1. If a competent authority receives information related to a reportable cyber-attack, that competent authority: (a) shall assess the level of confidentiality of that information and inform the entity about the outcome of its assessment without undue delay and not later than within 24 hours of receipt of the information;
2. (b) shall attempt to find any other similar cyber-attack in the Union reported to other competent authorities, in order to correlate the information received in the context of the reportable cyber-attack with information provided in the context of other cyber-attacks and enrich existing information, strengthen and coordinate cybersecurity responses;

3. (c) shall be responsible for the removal of business secrets and the anonymisation of the information in accordance with the relevant national and Union rules;

4. (d) shall share the information with the national single points of contact, CSIRTs and all competent authorities designated pursuant to Article 4 in other Member States without undue delay and no later than 24 hours after the reception of a reportable cyber-attack and provide updated information on a regular basis to those authorities or bodies;

5. (e) shall disseminate the information of the cyber-attack, after anonymisation and removal of business secrets pursuant to paragraph 1(c), to critical-impact and high-impact entities in its Member State without undue delay and no later than 24 hours after receiving information according to paragraph 1(a), and provide updated information on a regular basis allowing the entities to organise their defence effectively;

6. (f) may request the reporting high-impact or critical-impact entity to further disseminate the reportable cyber-attack information in a secure manner to other entities that may be affected, with the aim to generate situational awareness by the electricity sector and to prevent the materialisation of a risk that may escalate in a cross-border cybersecurity electricity incident;

7. (g) shall share with ENISA a summary report, after anonymisation and removal of business secrets, with the information of the cyber-attack.

8. If a CSIRT becomes aware of an unpatched actively exploited vulnerability, it shall: (a) share it with ENISA via an appropriate secure information exchange channel without delay, unless otherwise specified in other Union law; (b) support the concerned entity to receive from the manufacturer or provider an effective, coordinated and rapid management of the unpatched actively exploited vulnerability or of effective and efficient mitigation measures; (c) share available information with the vendor and request the manufacturer or provider, where possible, to identify a list of CSIRTs in Member States concerned by the unpatched actively exploited vulnerability and that shall be informed; (d) share available information with the CSIRTs identified under the previous point, based on need-to-know principle; (e) share, where they exist, mitigation strategies and measures to the reported unpatched actively exploited vulnerability.

9. If a competent authority becomes aware of an unpatched actively exploited vulnerability, that competent authority shall: (a) share, where they exist, mitigation strategies and measures to the reported unpatched actively exploited vulnerability, in coordination with the CSIRTs in its Member State; (b) shall share the information with a CSIRT in the Member State where the unpatched actively exploited vulnerability has been reported.

10. If the competent authority becomes aware of an unpatched vulnerability, without evidence of yet being actively exploited, it shall without undue delay coordinate with the CSIRT for the purposes of coordinated vulnerability disclosure as laid down in Article 12(1) of Directive (EU) 2022/2555.

11. If a CSIRT receives information related to cyber threats from one or several high-impact or critical-impact entities pursuant to Article 38(6), it shall disseminate that information or any other information of importance for preventing, detecting, responding to or mitigating the related risk to critical-impact and high-impact entities in its Member State and, where appropriate, to all concerned CSIRTs and to its national single point of contact without undue delay and no later than four hours after receiving information.

12. If a competent authority becomes aware of information related to cyber threats from one or several high-impact or critical-impact entities, it shall forward this information to the CSIRT for the purpose of paragraph 5.

13. The competent authorities may delegate in full or in part the responsibilities under paragraphs 3 and 4 concerning one or more high-impact or critical-impact entities that operate in more than one Member State to another competent authority in one of those Member States, following an agreement among the concerned competent authorities.

14. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall develop a cyber-attack classification scale methodology by 13 June 2025. The TSOs, with the assistance of the ENTSO for Electricity and the EU DSO entity may request the competent authorities to consult ENISA and their competent authorities responsible for cybersecurity for assistance in the development of such classification scale. The methodology shall provide the classification for the gravity of a cyber-attack according to five levels, the two highest levels being high and critical . The classification shall be based on the assessment of the following parameters: (a) the potential impact considering the assets and perimeters exposed determined in accordance with Article 26(4), point (c); and (b) the severity of the cyber-attack.

15. By 13 June 2026, the ENTSO for Electricity, in collaboration with the EU DSO entity, shall perform a feasibility study to assess the possibility and the financial costs necessary to develop a common tool enabling all entities to share information with relevant national authorities.

16. The feasibility study shall address the possibility for such a common tool to: (a) support critical-impact and high-impact entities with relevant security related information for operations of cross- border electricity flows, such as near real-time reporting of cyber-attacks, early alerts related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system; (b) be maintained in a suitable and highly trustable environment; (c) allow for data collection from critical-impact and high-impact entities and facilitate removal of confidential information and anonymisation of the data and their prompt dissemination to critical-impact and high-impact entities.

17. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall: (a) consult ENISA and the NIS Cooperation Group, the national single points of contact and the representatives of main stakeholders when assessing the feasibility; (b) present the results of the feasibility study to ACER and the NIS Cooperation Group.

18. The ENTSO for Electricity, in cooperation with the EU DSO entity may analyse and facilitate initiatives proposed by critical-impact and high-impact entities to evaluate and test such tools for information sharing.

Article 37(1)

If a competent authority receives information related to a reportable cyber-attack, that competent authority:

a. shall assess the level of confidentiality of that information and inform the entity about the outcome of its assessment without undue delay and not later than within 24 hours of receipt of the information;

b. shall attempt to find any other similar cyber-attack in the Union reported to other competent authorities, in order to correlate the information received in the context of the reportable cyber-attack with information provided in the context of other cyber-attacks and enrich existing information, strengthen and coordinate cybersecurity responses;

c. shall be responsible for the removal of business secrets and the anonymisation of the information in accordance with the relevant national and Union rules;

d. shall share the information with the national single points of contact, CSIRTs and all competent authorities designated pursuant to Article 4 in other Member States without undue delay and no later than 24 hours after the reception of a reportable cyber-attack and provide updated information on a regular basis to those authorities or bodies;

e. shall disseminate the information of the cyber-attack, after anonymisation and removal of business secrets pursuant to paragraph 1(c), to critical-impact and high-impact entities in its Member State without undue delay and no later than 24 hours after receiving information according to paragraph 1(a), and provide updated information on a regular basis allowing the entities to organise their defence effectively;

f. may request the reporting high-impact or critical-impact entity to further disseminate the reportable cyber-attack information in a secure manner to other entities that may be affected, with the aim to generate situational awareness by the electricity sector and to prevent the materialisation of a risk that may escalate in a cross-border cybersecurity electricity incident;

g. shall share with ENISA a summary report, after anonymisation and removal of business secrets, with the information of the cyber-attack.

Article 37(10)

The feasibility study shall address the possibility for such a common tool to:

a. support critical-impact and high-impact entities with relevant security related information for operations of cross- border electricity flows, such as near real-time reporting of cyber-attacks, early alerts related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system;

b. be maintained in a suitable and highly trustable environment;

c. allow for data collection from critical-impact and high-impact entities and facilitate removal of confidential information and anonymisation of the data and their prompt dissemination to critical-impact and high-impact entities.

Article 37(11)

The ENTSO for Electricity, in cooperation with the EU DSO entity, shall:

a. consult ENISA and the NIS Cooperation Group, the national single points of contact and the representatives of main stakeholders when assessing the feasibility;

b. present the results of the feasibility study to ACER and the NIS Cooperation Group.

Article 37(12)

The ENTSO for Electricity, in cooperation with the EU DSO entity may analyse and facilitate initiatives proposed by critical-impact and high-impact entities to evaluate and test such tools for information sharing.

Article 37(2)

If a CSIRT becomes aware of an unpatched actively exploited vulnerability, it shall:

a. share it with ENISA via an appropriate secure information exchange channel without delay, unless otherwise specified in other Union law;

b. support the concerned entity to receive from the manufacturer or provider an effective, coordinated and rapid management of the unpatched actively exploited vulnerability or of effective and efficient mitigation measures;

c. share available information with the vendor and request the manufacturer or provider, where possible, to identify a list of CSIRTs in Member States concerned by the unpatched actively exploited vulnerability and that shall be informed;

d. share available information with the CSIRTs identified under the previous point, based on need-to-know principle;

e. share, where they exist, mitigation strategies and measures to the reported unpatched actively exploited vulnerability.

Article 37(3)

If a competent authority becomes aware of an unpatched actively exploited vulnerability, that competent authority shall:

a. share, where they exist, mitigation strategies and measures to the reported unpatched actively exploited vulnerability, in coordination with the CSIRTs in its Member State;

b. shall share the information with a CSIRT in the Member State where the unpatched actively exploited vulnerability has been reported.

Article 37(4)

If the competent authority becomes aware of an unpatched vulnerability, without evidence of yet being actively exploited, it shall without undue delay coordinate with the CSIRT for the purposes of coordinated vulnerability disclosure as laid down in Article 12(1) of Directive (EU) 2022/2555.

Article 37(5)

If a CSIRT receives information related to cyber threats from one or several high-impact or critical-impact entities pursuant to Article 38(6), it shall disseminate that information or any other information of importance for preventing, detecting, responding to or mitigating the related risk to critical-impact and high-impact entities in its Member State and, where appropriate, to all concerned CSIRTs and to its national single point of contact without undue delay and no later than four hours after receiving information.

Article 37(6)

If a competent authority becomes aware of information related to cyber threats from one or several high-impact or critical-impact entities, it shall forward this information to the CSIRT for the purpose of paragraph 5.

Article 37(7)

The competent authorities may delegate in full or in part the responsibilities under paragraphs 3 and 4 concerning one or more high-impact or critical-impact entities that operate in more than one Member State to another competent authority in one of those Member States, following an agreement among the concerned competent authorities.

Article 37(8)

The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall develop a cyber-attack classification scale methodology by 13 June 2025. The TSOs, with the assistance of the ENTSO for Electricity and the EU DSO entity may request the competent authorities to consult ENISA and their competent authorities responsible for cybersecurity for assistance in the development of such classification scale. The methodology shall provide the classification for the gravity of a cyber-attack according to five levels, the two highest levels being 'high' and 'critical'. The classification shall be based on the assessment of the following parameters:

a. the potential impact considering the assets and perimeters exposed determined in accordance with Article 26(4), point (c); and
b. the severity of the cyber-attack.

Article 37(9)

By 13 June 2026, the ENTSO for Electricity, in collaboration with the EU DSO entity, shall perform a feasibility study to assess the possibility and the financial costs necessary to develop a common tool enabling all entities to share information with relevant national authorities.

Article 38

1. Each high-impact and critical-impact entity shall: (a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to: (i) ensure that the relevant network and information systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on cyber-attacks; (ii) conduct security monitoring, including detecting intrusions and assessing vulnerabilities of network and information systems; (iii) analyse and, if necessary, take all actions required under its responsibility and capacity to protect the entity; (iv) participate in the information collection and sharing described in this Article; (b) have the right to procure all or parts of these capabilities pursuant to point (a) through MSSPs. Critical-impact and high-impact entities shall remain responsible for MSSPs and supervise their efforts; c) designate a single point of contact at entity level for the purpose of information sharing.
2. ENISA may issue non-binding guidance on establishing such capabilities or subcontracting the service to MSSPs, as part of the task defined in Article 6(2) of Regulation (EU) 2019/881.
3. Each critical-impact and high-impact entity shall share relevant information related to a reportable cyber-attack with its CSIRTs and its competent authority without undue delay and no later than four hours of becoming aware that the incident is reportable.
4. Information related to a cyber-attack shall be considered reportable when the cyber-attack is assessed by the affected entity resulting in a criticality ranging from high to critical following the cyber-attack classification scale methodology pursuant to Article 37(8). The single point of contact at entity level designated pursuant to paragraph 1 point (c) shall communicate the incident classification.
5. Where critical-impact and high-impact entities notify relevant information related to unpatched actively exploited vulnerabilities to a CSIRT, the latter may forward this information to its competent authority. In light of the level of sensitivity of the notified information, the CSIRT may withhold the information or delay its forwarding based on justified cybersecurity-related grounds.
6. Each critical-impact and high-impact entity shall provide without undue delay to its CSIRTs any information related to a reportable cyber threat that may have a cross-border effect. Information related to a cyber threat shall be considered reportable when at least one of the following conditions is met: (a) it provides relevant information for other critical-impact and high-impact entity for preventing, detecting, responding or mitigating the impact of the risk; (b) the identified techniques, tactics and procedures used in the context of an attack lead to information such as compromised URL or IP addresses, hashes or any other attribute useful to contextualise and correlate the attack; (c) a cyber threat may be further assessed and contextualised with additional information provided by service providers or third parties not subject to this Regulation.
7. Each critical-impact entity and high-impact entity shall, when sharing information pursuant to this Article, specify the following: (a) that the information is submitted pursuant to this

Regulation; (b) whether the information concerns: (i) a reportable cyber-attack referred to in paragraph 3; (ii) unpatched actively exploited vulnerabilities not publicly known referred to in paragraph 4; (iii) a reportable cyber threat referred to in paragraph 5; (c) in the case of a reportable cyber-attack, the level of the cyber-attack according to the cyber-attack classification scale methodology referred to in Article 37(8) and information leading to this classification including at least the criticality of the cyber-attack.

8. When a critical or high-impact entity notifies a significant incident pursuant to Article 23 of Directive (EU) 2022/2555 and the incident reporting under that Article contains relevant information as required under paragraph 3 of this Article, the reporting of the entity under Article 23(1) of that Directive shall constitute reporting of information under paragraph 3 of this Article.

9. Each critical-impact and high-impact entity shall report to its competent authority or CSIRT by clearly identifying specific information that shall only be shared with the competent authority or CSIRT in cases where the information sharing could be source of a cyber-attack. Each critical-impact and high-impact entity shall have the right to provide a non-confidential version of the information to the competent CSIRT.

Article 38(1)

Each high-impact and critical-impact entity shall:

a. establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

   i. ensure that the relevant network and information systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on cyber-attacks;

   ii. conduct security monitoring, including detecting intrusions and assessing vulnerabilities of network and information systems;

   iii. analyse and, if necessary, take all actions required under its responsibility and capacity to protect the entity;

   iv. participate in the information collection and sharing described in this Article;

b. have the right to procure all or parts of these capabilities pursuant to point (a) through MSSPs. Critical-impact and high-impact entities shall remain responsible for MSSPs and supervise their efforts;

c. designate a single point of contact at entity level for the purpose of information sharing.

Article 38(2)

ENISA may issue non-binding guidance on establishing such capabilities or subcontracting the service to MSSPs, as part of the task defined in Article 6(2) of Regulation (EU) 2019/881.

Article 38(3)

Each critical-impact and high-impact entity shall share relevant information related to a reportable cyber-attack with its CSIRTs and its competent authority without undue delay and no later than four hours of becoming aware that the incident is reportable.

Article 38(4)

Information related to a cyber-attack shall be considered reportable when the cyber-attack is assessed by the affected entity resulting in a criticality ranging from 'high' to 'critical' following the cyber-attack classification scale methodology pursuant to Article 37(8). The single point of contact at entity level designated pursuant to paragraph 1 point (c) shall communicate the incident classification.

Article 38(5)

Where critical-impact and high-impact entities notify relevant information related to unpatched actively exploited vulnerabilities to a CSIRT, the latter may forward this information to its competent authority. In light of the level of sensitivity of the notified information, the CSIRT may withhold the information or delay its forwarding based on justified cybersecurity-related grounds.

Article 38(6)

Each critical-impact and high-impact entity shall provide without undue delay to its CSIRTs any information related to a reportable cyber threat that may have a cross-border effect. Information related to a cyber threat shall be considered reportable when at least one of the following conditions is met:

a. it provides relevant information for other critical-impact and high-impact entity for preventing, detecting, responding or mitigating the impact of the risk;

b. the identified techniques, tactics and procedures used in the context of an attack lead to information such as compromised URL or IP addresses, hashes or any other attribute useful to contextualise and correlate the attack;

c. a cyber threat may be further assessed and contextualised with additional information provided by service providers or third parties not subject to this Regulation.

Article 38(7)

Each critical-impact entity and high-impact entity shall, when sharing information pursuant to this Article, specify the following:

a. that the information is submitted pursuant to this Regulation;

b. whether the information concerns:

   i. a reportable cyber-attack referred to in paragraph 3;

   ii. unpatched actively exploited vulnerabilities not publicly known referred to in paragraph 4;

   iii. a reportable cyber threat referred to in paragraph 5;

c. in the case of a reportable cyber-attack, the level of the cyber-attack according to the cyber-attack classification scale methodology referred to in Article 37(8) and information leading to this classification including at least the criticality of the cyber-attack.

Article 38(8)

When a critical or high-impact entity notifies a significant incident pursuant to Article 23 of Directive (EU) 2022/2555 and the incident reporting under that Article contains relevant information as required under paragraph 3 of this Article, the reporting of the entity under Article 23(1) of that Directive shall constitute reporting of information under paragraph 3 of this Article.

Article 38(9)

Each critical-impact and high-impact entity shall report to its competent authority or CSIRT by clearly identifying specific information that shall only be shared with the competent authority or CSIRT in cases where the information sharing could be source of a cyber-attack. Each critical-impact and high-impact entity shall have the right to provide a non-confidential version of the information to the competent CSIRT.

Article 39

1. Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical- impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

2. If a cyber-attack has an effect on cross-border electricity flows, the single points of contact at entity level of affected critical-impact and high-impact entities shall cooperate to share information among them,

3. coordinated by the competent authority of the Member State in which the cyber-attack was first reported.

4. Critical-impact and high-impact entities shall: (a) ensure that their own single point of contact at entity level has access on a need-to-know basis to the information they received from the national single point of contact through their competent authority; (b) unless already done pursuant to Article 3(4) of Directive (EU) 2022/2555, notify the competent authority of the Member State in which they are established and the national single point of contact with a list of their cybersecurity single points of contact at entity level: (i) from which that competent authority and national single point of contact may expect to receive information about reportable cyber-attacks; (ii) to which competent authorities and national single points of contact may have to provide information; (c) establish cyber-attack management procedures for cyber-attacks, including roles and responsibilities, tasks and reactions based on the observable evolution of the cyber-attack within the critical-impact and high-impact perimeters; (d) test the overall cyber-attack management procedures at least every year by testing at least one scenario affecting directly or indirectly cross-border electricity flows. That annual test may be conducted by critical-impact and high- impact entities during the regular exercises referred to in Article 43. Any live cyber-attack response activity with a consequence classified at least Scale 2, according to the cyber-attack classification scale methodology referred to in Article 37(8) and with a cybersecurity root cause, may serve as an annual test of the cyber-attack response plan.
5. The tasks referred to in paragraph 1 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.

Article 39(1)

Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical- impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

If a cyber-attack has an effect on cross-border electricity flows, the single points of contact at entity level of affected critical-impact and high-impact entities shall cooperate to share information among them,

Article 39(2)

coordinated by the competent authority of the Member State in which the cyber-attack was first reported.

Article 39(3)

Critical-impact and high-impact entities shall:

a. ensure that their own single point of contact at entity level has access on a need-to-know basis to the information they received from the national single point of contact through their competent authority;

b. unless already done pursuant to Article 3(4) of Directive (EU) 2022/2555, notify the competent authority of the Member State in which they are established and the national single point of contact with a list of their cybersecurity single points of contact at entity level:

   i. from which that competent authority and national single point of contact may expect to receive information about reportable cyber-attacks;

   ii. to which competent authorities and national single points of contact may have to provide information;

c. establish cyber-attack management procedures for cyber-attacks, including roles and responsibilities, tasks and reactions based on the observable evolution of the cyber-attack within the critical-impact and high-impact perimeters;

d. test the overall cyber-attack management procedures at least every year by testing at least one scenario affecting directly or indirectly cross-border electricity flows. That annual test may be conducted by critical-impact and high- impact entities during the regular exercises referred to in Article 43. Any live cyber-attack response activity with a consequence classified at least Scale 2, according to the cyber-attack classification scale methodology referred to in Article 37(8) and with a cybersecurity root cause, may serve as an annual test of the cyber-attack response plan.

Article 39(4)

The tasks referred to in paragraph 1 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.

Article 4

1. As soon as possible and in any event by 13 December 2024, each Member State shall designate a national governmental or regulatory authority responsible for carrying out the tasks assigned to it in this Regulation (competent authority). Until the competent authority has been assigned with carrying out the tasks under this Regulation, the regulatory authority designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944 [49] shall carry out the tasks of the competent authority in accordance with this Regulation.

2. Member States shall, without delay, notify the Commission, ACER, ENISA, the NIS Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 [50] and the Electricity Coordination Group set up under Article 1 of Commission Decision of 15 November 2012 [51] and communicate to them the name and the contact details of their competent authority designated pursuant to paragraph 1 of this article and any subsequent changes thereto.

[49] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02019L0944-20240716#art_57
[50] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_14
[51] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D1117(01)

3. Member States may allow their competent authority to delegate tasks assigned to it in this Regulation to other national authorities with the exception of the tasks listed in Article 5. Each competent authority shall monitor the application of this Regulation by the authorities to whom it has delegated tasks.
4. The competent authority shall communicate the name, contact details, assigned tasks and any subsequent changes thereto of the authorities to whom a task has been delegated to the Commission, to ACER, to the Electricity Coordination Group, to ENISA and to the NIS Cooperation Group.

Article 4(1)

As soon as possible and in any event by 13 December 2024, each Member State shall designate a national governmental or regulatory authority responsible for carrying out the tasks assigned to it in this Regulation ('competent authority'). Until the competent authority has been assigned with carrying out the tasks under this Regulation, the regulatory authority designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944 [52] shall carry out the tasks of the competent authority in accordance with this Regulation.

Article 4(2)

Member States shall, without delay, notify the Commission, ACER, ENISA, the NIS Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 [53] and the Electricity Coordination Group set up under Article 1 of Commission Decision of 15 November 2012 [54] and communicate to them the name and the contact details of their competent authority designated pursuant to paragraph 1 of this article and any subsequent changes thereto.

Article 4(3)

This Regulation shall also apply to all entities who are not established in the Union but who deliver services to entities in the Union, provided they have been identified as high or critical-impact entities by the competent authorities in accordance with https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885 [55]

Article 4(3)

Member States may allow their competent authority to delegate tasks assigned to it in this Regulation to other national authorities with the exception of the tasks listed in Article 5. Each competent authority shall monitor the application of this Regulation by the authorities to whom it has delegated tasks.

[52] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02019L0944-20240716#art_57
[53] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_14
[54] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D1117(01)
[55] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885

The competent authority shall communicate the name, contact details, assigned tasks and any subsequent changes thereto of the authorities to whom a task has been delegated to the Commission, to ACER, to the Electricity Coordination Group, to ENISA and to the NIS Cooperation Group.

Article 40

1. When the competent authority establishes that an electricity crisis is related to a cyber-attack which has an impact on more than one Member State, the competent authorities from the affected Member States, the CS-NCAs, the RP-NCA and the NIS cyber crisis management authorities from the affected Member States shall jointly create an ad hoc cross-border crisis coordination group.
2. The ad hoc cross-border crisis coordination group shall: (a) coordinate the efficient retrieval and further dissemination of all relevant cybersecurity information to the entities involved in the crisis management process; (b) organise the communication between all the entities impacted by the crisis and the competent authorities, in order to reduce overlaps and increase the efficiency in the analyses and technical responses to remedy the simultaneous electricity crises with a cybersecurity root cause; (c) provide, in cooperation with the competent CSIRTs, the expertise required, including operational advice on the implementation of possible mitigation measures to the entities impacted by the incident; (d) notify and provide regular updates on the state of the incident to the Commission and the Electricity Coordination Group, following the protection principles laid down in Article 46; (e) seek advice from relevant authorities, agencies or entities that might be of help to mitigate the electricity crisis.
3. Where the cyber-attack qualifies or is expected to qualify as a large-scale cybersecurity incident, the ad hoc cross- border crisis coordination group shall immediately inform the national cyber crisis management authorities in accordance with Article 9(1) of Directive (EU) 2022/2555 in the Member States affected by the incident, as well as the Commission and the EU CyCLONe. In such situation, the ad hoc cross-border crisis coordination group shall support the EU CyCLONe concerning sectoral specificities.
4. Critical-impact and high-impact entities shall develop and have at their disposal capabilities, internal guidelines, preparedness plans, and staff to take part in the detection and mitigation of cross-border crisis. The critical-impact or high- impact entity impacted by a simultaneous electricity crisis shall investigate the root cause of such crisis in cooperation with its competent authority to determine the extent to which the crisis is related to a cyber-attack.
5. The tasks in paragraph 4 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.

Article 40(1)

When the competent authority establishes that an electricity crisis is related to a cyber-attack which has an impact on more than one Member State, the competent authorities from the affected Member States, the CS-NCAs, the RP-NCA and the NIS cyber crisis management author-

ities from the affected Member States shall jointly create an ad hoc cross-border crisis coordination group.

Article 40(2)

The ad hoc cross-border crisis coordination group shall:

a. coordinate the efficient retrieval and further dissemination of all relevant cybersecurity information to the entities involved in the crisis management process;
b. organise the communication between all the entities impacted by the crisis and the competent authorities, in order to reduce overlaps and increase the efficiency in the analyses and technical responses to remedy the simultaneous electricity crises with a cybersecurity root cause;
c. provide, in cooperation with the competent CSIRTs, the expertise required, including operational advice on the implementation of possible mitigation measures to the entities impacted by the incident;
d. notify and provide regular updates on the state of the incident to the Commission and the Electricity Coordination Group, following the protection principles laid down in Article 46;
e. seek advice from relevant authorities, agencies or entities that might be of help to mitigate the electricity crisis.

Article 40(3)

Where the cyber-attack qualifies or is expected to qualify as a large-scale cybersecurity incident, the ad hoc cross- border crisis coordination group shall immediately inform the national cyber crisis management authorities in accordance with Article 9(1) of Directive (EU) 2022/2555 in the Member States affected by the incident, as well as the Commission and the EU CyCLONe. In such situation, the ad hoc cross-border crisis coordination group shall support the EU CyCLONe concerning sectoral specificities.

Article 40(4)

Critical-impact and high-impact entities shall develop and have at their disposal capabilities, internal guidelines, preparedness plans, and staff to take part in the detection and mitigation of cross-border crisis. The critical-impact or high- impact entity impacted by a simultaneous electricity crisis shall investigate the root cause of such crisis in cooperation with its competent authority to determine the extent to which the crisis is related to a cyber-attack.

Article 40(5)

The tasks in paragraph 4 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.

Article 41

1. Within 24 months after the notification to ACER of the Union-wide risk assessment report, ACER shall in close cooperation with ENISA, the ENTSO for Electricity, the EU DSO entity, CS-NCAs, competent authorities, RP-NCAs, the NRAs and the NIS national cyber crisis management authorities, develop a Union-level cybersecurity crisis management and response plan for the electricity sector.
2. Within 12 months after the development by ACER of the Union-level cybersecurity crisis management and response plan for the electricity sector pursuant to paragraph 1, each competent authority shall develop a national cybersecurity crisis management and response plan for cross-border electricity flows taking into account the Union-level cybersecurity crisis management plan and the national risk preparedness plan established in accordance with Article 10 of Regulation (EU) 2019/941. This plan shall be consistent with the large-scale cybersecurity incident and crisis response plan pursuant to Article 9(4) of Directive (EU) 2022/2555. The competent authority shall coordinate with the critical-impact and high- impact entities and with the RP-NCA in its Member State.
3. The national large-scale cybersecurity incident and crisis response plan required pursuant to Article 9(4) of Directive (EU) 2022/2555 shall be considered as a national cybersecurity crisis management plan under this Article if it includes crisis management and response provisions for the cross-border electricity flows.
4. The tasks listed in at paragraphs 1 and 2 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.
5. Critical-impact and high-impact entities shall ensure that their cybersecurity-related crisis management processes: (a) have compatible cross-border cybersecurity incident handling procedures as defined in Article 6(8) of Directive (EU) 2022/2555 formally incorporated in their crisis management plans; (b) are part of the general crisis management activities.
6. Within 12 months after the notification of the high-and critical-impact entities pursuant to Article 24(6), and every three years thereafter, critical impact and high-impact entities shall develop a crisis management plan at entity level for a cybersecurity related crisis which shall be included into their general crisis management plans. This plan shall include at least the following: (a) rules of declaration of the crisis as set out in Article 14(2) and (3) of the Regulation (EU) 2019/941; (b) clear roles and responsibilities for crisis management, including the role of other relevant critical-impact and high- impact entities; (c) up-to-date contact information as well as rules for communication and information sharing during a crisis situation including the connection to the CSIRTs.
7. The measures for crisis management pursuant to Article 21(2), point (c) of Directive (EU) 2022/2555 shall be considered as a crisis management plan at entity level for the electricity sector under this Article if it includes all requirements listed in paragraph 6.
8. The crisis management plans shall be tested during the cybersecurity exercises referred to in Articles 43, 44 and 45.

9. The critical-impact and high-impact entities shall include their crisis management plans at entity level into their business continuity plans for the critical-impact and high-impact processes. The crisis management plans at entity level shall include: (a) processes depending on availability, integrity and reliability of IT services; (b) all business continuity locations including the locations for hardware and software; (c) all internal roles and responsibilities connected to business continuity processes.
10. The critical-impact and high-impact entities shall update their crisis management plans at entity level at least every three years and whenever necessary.
11. ACER shall update the Union-level cybersecurity crisis management and response plan for the electricity sector developed pursuant to paragraph (1) at least every three years and whenever necessary.
12. Each competent authority shall update the national cybersecurity crisis management and response plan for cross- border electricity flows developed pursuant to paragraph (2) at least every three years and whenever necessary.
13. The critical-impact and high-impact entities shall test their business continuity plans at least once every three years or after major changes in a critical-impact process. The outcome of the business continuity plan tests shall be documented. The critical-impact and high-impact entities may include the test of their business continuity plan in the cybersecurity exercises.
14. The critical-impact and high-impact entities shall update their business continuity plan whenever necessary and at least once every three years taking into account the outcome of the test.
15. If a test identifies deficiencies in the business continuity plan, the critical-impact and high-impact entity shall correct those deficiencies within 180 calendar days after the testing and shall conduct a new test to provide evidence that the corrective measures are effective.
16. Where a critical-impact or high-impact entity cannot correct the deficiencies within 180 calendar days, it shall include the reasons in the report to be provided to its competent authority in accordance with Article 27.

Article 41(1)

Within 24 months after the notification to ACER of the Union-wide risk assessment report, ACER shall in close cooperation with ENISA, the ENTSO for Electricity, the EU DSO entity, CS-NCAs, competent authorities, RP-NCAs, the NRAs and the NIS national cyber crisis management authorities, develop a Union-level cybersecurity crisis management and response plan for the electricity sector.

Article 41(10)

The critical-impact and high-impact entities shall update their crisis management plans at entity level at least every three years and whenever necessary.

Article 41(11)

ACER shall update the Union-level cybersecurity crisis management and response plan for the electricity sector developed pursuant to paragraph (1) at least every three years and whenever necessary.

Article 41(12)

Each competent authority shall update the national cybersecurity crisis management and response plan for cross- border electricity flows developed pursuant to paragraph (2) at least every three years and whenever necessary.

Article 41(13)

The critical-impact and high-impact entities shall test their business continuity plans at least once every three years or after major changes in a critical-impact process. The outcome of the business continuity plan tests shall be documented. The critical-impact and high-impact entities may include the test of their business continuity plan in the cybersecurity exercises.

Article 41(14)

The critical-impact and high-impact entities shall update their business continuity plan whenever necessary and at least once every three years taking into account the outcome of the test.

Article 41(15)

If a test identifies deficiencies in the business continuity plan, the critical-impact and high-impact entity shall correct those deficiencies within 180 calendar days after the testing and shall conduct a new test to provide evidence that the corrective measures are effective.

Article 41(16)

Where a critical-impact or high-impact entity cannot correct the deficiencies within 180 calendar days, it shall include the reasons in the report to be provided to its competent authority in accordance with Article 27.

Article 41(2)

Within 12 months after the development by ACER of the Union-level cybersecurity crisis management and response plan for the electricity sector pursuant to paragraph 1, each competent

authority shall develop a national cybersecurity crisis management and response plan for cross-border electricity flows taking into account the Union-level cybersecurity crisis management plan and the national risk preparedness plan established in accordance with Article 10 of Regulation (EU) 2019/941. This plan shall be consistent with the large-scale cybersecurity incident and crisis response plan pursuant to Article 9(4) of Directive (EU) 2022/2555. The competent authority shall coordinate with the critical-impact and high- impact entities and with the RP-NCA in its Member State.

Article 41(3)

The national large-scale cybersecurity incident and crisis response plan required pursuant to Article 9(4) of Directive (EU) 2022/2555 shall be considered as a national cybersecurity crisis management plan under this Article if it includes crisis management and response provisions for the cross-border electricity flows.

Article 41(4)

The tasks listed in at paragraphs 1 and 2 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.

Article 41(5)

Critical-impact and high-impact entities shall ensure that their cybersecurity-related crisis management processes:

a. have compatible cross-border cybersecurity incident handling procedures as defined in Article 6(8) of Directive (EU) 2022/2555 formally incorporated in their crisis management plans;
b. are part of the general crisis management activities.

Article 41(6)

Within 12 months after the notification of the high-and critical-impact entities pursuant to Article 24(6), and every three years thereafter, critical impact and high-impact entities shall develop a crisis management plan at entity level for a cybersecurity related crisis which shall be included into their general crisis management plans. This plan shall include at least the following:

a. rules of declaration of the crisis as set out in Article 14(2) and (3) of the Regulation (EU) 2019/941;
b. clear roles and responsibilities for crisis management, including the role of other relevant critical-impact and high- impact entities;

c. up-to-date contact information as well as rules for communication and information sharing during a crisis situation including the connection to the CSIRTs.

Article 41(7)

The measures for crisis management pursuant to Article 21(2), point (c) of Directive (EU) 2022/2555 shall be considered as a crisis management plan at entity level for the electricity sector under this Article if it includes all requirements listed in paragraph 6.

Article 41(8)

The crisis management plans shall be tested during the cybersecurity exercises referred to in Articles 43, 44 and 45.

Article 41(9)

The critical-impact and high-impact entities shall include their crisis management plans at entity level into their business continuity plans for the critical-impact and high-impact processes. The crisis management plans at entity level shall include:

a. processes depending on availability, integrity and reliability of IT services;

b. all business continuity locations including the locations for hardware and software;

c. all internal roles and responsibilities connected to business continuity processes.

Article 42

1. The competent authorities shall cooperate with ENISA to develop Electricity Cybersecurity Early Alert Capabilities (ECEAC) as part as the assistance to Member States pursuant to Articles 6(2) and (7) of Regulation (EU) 2019/881.
2. The ECEAC shall enable ENISA when carrying out the tasks listed in Article 7(7) of Regulation (EU) 2019/881 to: (a) collect voluntary shared information from: (i)CSIRTs, competent authorities; (ii)the entities listed in Article 2 of this Regulation; (iii)any other entity that wants to share relevant information on a voluntary basis;
3. (b)assess and classify collected information; (c)assess the information ENISA has access to for identifying cyber risk conditions and relevant indicators for aspects of cross-border electricity flows; (d)identify conditions and indicators that frequently correlate with cyber-attacks within the electricity sector; (e)define whether further analysis and preventive actions shall be taken through assessment and identification of risk factors;

1. (f)inform the competent authorities on the identified risks and recommended preventive actions specific to the entities concerned; (g)inform all relevant entities listed in Article 2 on the results of the information assessed in accordance with points (b), (c) and (d) of this paragraph;

1. (h)periodically include the relevant information in the situational awareness report, issued in accordance with Article 7(6) of Regulation (EU) 2019/881; (i)derive, where possible, applicable data that indicates that a potential security breach or cyber-attack (indicators of compromise) from the collected information.
2. The CSIRTs shall disseminate the information received from ENISA to the entities concerned without delay, within their tasks defined in Article 11(3), point (b) of Directive (EU) 2022/2555.
3. ACER shall monitor the effectiveness of the ECEAC. ENISA shall assist ACER by providing all necessary information, pursuant to Articles 6(2) and 7(1) of Regulation (EU) 2019/881.
4. The analysis of this monitoring activity shall be part of the monitoring pursuant to Article 12 of this Regulation.

Article 42(1)

The competent authorities shall cooperate with ENISA to develop Electricity Cybersecurity Early Alert Capabilities (ECEAC) as part as the assistance to Member States pursuant to Articles 6(2) and (7) of Regulation (EU) 2019/881.

The ECEAC shall enable ENISA when carrying out the tasks listed in Article 7(7) of Regulation (EU) 2019/881 to:

a. collect voluntary shared information from:
    i. CSIRTs, competent authorities;
    ii. the entities listed in Article 2 of this Regulation;
    iii. any other entity that wants to share relevant information on a voluntary basis;
b. assess and classify collected information;
c. assess the information ENISA has access to for identifying cyber risk conditions and relevant indicators for aspects of cross-border electricity flows;
d. identify conditions and indicators that frequently correlate with cyber-attacks within the electricity sector;
e. define whether further analysis and preventive actions shall be taken through assessment and identification of risk factors;
f. inform the competent authorities on the identified risks and recommended preventive actions specific to the entities concerned;
g. inform all relevant entities listed in Article 2 on the results of the information assessed in accordance with points (b), (c) and (d) of this paragraph;

Article 42(2)

(h) periodically include the relevant information in the situational awareness report, issued in accordance with Article 7(6) of Regulation (EU) 2019/881;

(i) derive, where possible, applicable data that indicates that a potential security breach or cyber-attack ('indicators of compromise') from the collected information.

Article 42(3)

The CSIRTs shall disseminate the information received from ENISA to the entities concerned without delay, within their tasks defined in Article 11(3), point (b) of Directive (EU) 2022/2555.

Article 42(4)

ACER shall monitor the effectiveness of the ECEAC. ENISA shall assist ACER by providing all necessary information, pursuant to Articles 6(2) and 7(1) of Regulation (EU) 2019/881.

The analysis of this monitoring activity shall be part of the monitoring pursuant to Article 12 of this Regulation.

Article 43

1. By 31 December of the year after the notification of critical-impact entities, and every three years thereafter, each critical-impact entity shall perform a cybersecurity exercise including one or more scenarios with cyber-attacks affecting cross-border electricity flows directly or indirectly and related to the risks identified during the cybersecurity risk assessments at Member State and entity levels in accordance with Article 20 and Article 27.
2. By derogation from paragraph 1, the RP-NCA, after consulting the competent authority and the relevant cyber crisis management authority as designated or established in Directive (EU) 2022/2555 under Article 9 may decide to organise a cybersecurity exercise at Member State level as described in paragraph 1 instead of performing the cybersecurity exercise at entity level. In this regard, the competent authority shall inform: (a) all critical-impact entities of its Member State, the NRA, CSIRTs and the CS-NCA at the latest by 30 June of the year preceding the cybersecurity exercise at entity level; (b) each entity that shall participate in the cybersecurity exercise at Member State level at the latest 6 months before the exercise is to take place.
3. The RP-NCA with the technical support of its CSIRTs, shall organise the cybersecurity exercise described in paragraph 2 at Member State level independently or in the context of a different cybersecurity exercise in that Member State. In order to be able to group these exercises, RP-NCA may postpone the cybersecurity exercise at Member State level referred to in paragraph 1 by one year.

4. The cybersecurity exercises at entity level and at Member State level shall be consistent with the national cybersecurity crisis management frameworks in accordance with Article 9(4), point (d) of Directive (EU) 2022/2555.

5. By 31 December 2026, and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall make available an exercise scenario template to perform the cybersecurity exercises at entity and Member State level referred to in paragraphs 1. This template shall take into account the results of the most recently performed cybersecurity risk assessment at entity and Member State levels and shall include key success criteria. The ENTSO for Electricity and the EU DSO entity shall involve ACER and ENISA in the development of such template.

Article 43(1)

By 31 December of the year after the notification of critical-impact entities, and every three years thereafter, each critical-impact entity shall perform a cybersecurity exercise including one or more scenarios with cyber-attacks affecting cross-border electricity flows directly or indirectly and related to the risks identified during the cybersecurity risk assessments at Member State and entity levels in accordance with Article 20 and Article 27.

Article 43(2)

By derogation from paragraph 1, the RP-NCA, after consulting the competent authority and the relevant cyber crisis management authority as designated or established in Directive (EU) 2022/2555 under Article 9 may decide to organise a cybersecurity exercise at Member State level as described in paragraph 1 instead of performing the cybersecurity exercise at entity level. In this regard, the competent authority shall inform:

a. all critical-impact entities of its Member State, the NRA, CSIRTs and the CS-NCA at the latest by 30 June of the year preceding the cybersecurity exercise at entity level;

b. each entity that shall participate in the cybersecurity exercise at Member State level at the latest 6 months before the exercise is to take place.

Article 43(3)

The RP-NCA with the technical support of its CSIRTs, shall organise the cybersecurity exercise described in paragraph 2 at Member State level independently or in the context of a different cybersecurity exercise in that Member State. In order to be able to group these exercises, RP-NCA may postpone the cybersecurity exercise at Member State level referred to in paragraph 1 by one year.

Article 43(4)

The cybersecurity exercises at entity level and at Member State level shall be consistent with the national cybersecurity crisis management frameworks in accordance with Article 9(4), point (d) of Directive (EU) 2022/2555.

Article 43(5)

By 31 December 2026, and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall make available an exercise scenario template to perform the cybersecurity exercises at entity and Member State level referred to in paragraphs 1. This template shall take into account the results of the most recently performed cybersecurity risk assessment at entity and Member State levels and shall include key success criteria. The ENTSO for Electricity and the EU DSO entity shall involve ACER and ENISA in the development of such template.

Article 44

1. By 31 December 2029, and every three years thereafter, in each system operation region, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall organise a regional cybersecurity exercise. The critical-impact entities in the system operation region shall participate in the regional cybersecurity exercise. The ENTSO for Electricity, in cooperation with the EU DSO entity, may organise, instead of a regional cybersecurity exercise, a cross regional cybersecurity exercise in more than one system operating regions in the same timeframe. The exercise should take into account other existing cybersecurity risk assessments and scenarios developed at Union level.
2. ENISA shall support the ENTSO for Electricity and the EU DSO entity in the preparation and organisation of the cybersecurity exercise at regional or at cross-regional level.
3. The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the critical-impact entities that shall participate in the regional or cross regional cybersecurity exercise six months before the exercise takes place.
4. The organiser of a regular cybersecurity exercise at Union level pursuant to Article 7(5) of Regulation (EU) 2019/881, or of any mandatory cybersecurity exercise related to the electricity sector within the same geographic perimeter, may invite the ENTSO for Electricity and the EU DSO entity to participate. In such cases, the obligation in paragraph 1 does not apply, provided that all critical-impact entities in the system operation region take part in the same exercise.
5. If the ENTSO for Electricity and the EU DSO entity participate in a cybersecurity exercise referred to in paragraph 4, they may postpone the regional or cross-regional cybersecurity exercise referred to in paragraph 1 by one year.
6. By 31 December 2027, and every three years after that date, the ENTSO for Electricity, in coordination with the EU DSO entity, shall make available an exercise template to perform the regional and cross regional cybersecurity exercises. This template shall take into account the results of the most recently performed cybersecurity risk assessment at regional level and shall include key success criteria. The ENTSO for Electricity shall consult the Commission

and may seek advice from ACER, ENISA and the Joint Research Centre on the organisation and execution of the regional and cross regional cybersecurity exercises.

Article 44(1)

By 31 December 2029, and every three years thereafter, in each system operation region, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall organise a regional cybersecurity exercise. The critical-impact entities in the system operation region shall participate in the regional cybersecurity exercise. The ENTSO for Electricity, in cooperation with the EU DSO entity, may organise, instead of a regional cybersecurity exercise, a cross regional cybersecurity exercise in more than one system operating regions in the same timeframe. The exercise should take into account other existing cybersecurity risk assessments and scenarios developed at Union level.

Article 44(2)

ENISA shall support the ENTSO for Electricity and the EU DSO entity in the preparation and organisation of the cybersecurity exercise at regional or at cross-regional level.

Article 44(3)

The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the critical-impact entities that shall participate in the regional or cross regional cybersecurity exercise six months before the exercise takes place.

Article 44(4)

The organiser of a regular cybersecurity exercise at Union level pursuant to Article 7(5) of Regulation (EU) 2019/881, or of any mandatory cybersecurity exercise related to the electricity sector within the same geographic perimeter, may invite the ENTSO for Electricity and the EU DSO entity to participate. In such cases, the obligation in paragraph 1 does not apply, provided that all critical-impact entities in the system operation region take part in the same exercise.

Article 44(5)

If the ENTSO for Electricity and the EU DSO entity participate in a cybersecurity exercise referred to in paragraph 4, they may postpone the regional or cross-regional cybersecurity exercise referred to in paragraph 1 by one year.

Article 44(6)

By 31 December 2027, and every three years after that date, the ENTSO for Electricity, in coordination with the EU DSO entity, shall make available an exercise template to perform the regional and cross regional cybersecurity exercises. This template shall take into account the results of the most recently performed cybersecurity risk assessment at regional level and shall include key success criteria. The ENTSO for Electricity shall consult the Commission and may seek advice from ACER, ENISA and the Joint Research Centre on the organisation and execution of the regional and cross regional cybersecurity exercises.

Article 45

1. Upon request from a critical-impact entity, critical service providers shall participate in the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) when they provide services for the critical-impact entity in the area corresponding with the scope of the relevant cybersecurity exercise.
2. The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1), with the advice of ENISA if requested by them and pursuant to Article 7(5) of Regulation (EU) 2019/881, shall analyse and finalise the relevant cybersecurity exercise through a report summarising the lessons, addressed to all participants. The report shall include: (a) the exercise scenarios, meeting reports, main positions, successes and lessons learnt at any level of the electricity value chain; (b) whether the key success criteria were met; (c) a list of recommendations for entities participating in the relevant cybersecurity exercise to correct, adapt or change cybersecurity crisis processes, procedures, associated governance models and any existing contractual engagements with critical service providers.
3. If requested by the CSIRTs network or the NIS Cooperation Group or the EU CyCLONe, the organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) shall share the outcome of the relevant cybersecurity exercise. The organisers shall share with each entity participating in the exercises the information referred to in paragraph 2, points (a) and (b) of this Article. The organisers shall share the list of recommendations referred to in that paragraph, point (c) exclusively with the entities addressed in the recommendations.
4. The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) shall follow up regularly with the entities participating in the exercises on the implementation of the recommendations pursuant to paragraph 2, point (c) of this Article.

Article 45(1)

Upon request from a critical-impact entity, critical service providers shall participate in the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) when they provide services for the critical-impact entity in the area corresponding with the scope of the relevant cybersecurity exercise.

Article 45(2)

The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1), with the advice of ENISA if requested by them and pursuant to Article 7(5) of Regulation (EU) 2019/881, shall analyse and finalise the relevant cybersecurity exercise through a report summarising the lessons, addressed to all participants. The report shall include:

a. the exercise scenarios, meeting reports, main positions, successes and lessons learnt at any level of the electricity value chain;

b. whether the key success criteria were met;

c. a list of recommendations for entities participating in the relevant cybersecurity exercise to correct, adapt or change cybersecurity crisis processes, procedures, associated governance models and any existing contractual engagements with critical service providers.

Article 45(3)

If requested by the CSIRTs network or the NIS Cooperation Group or the EU CyCLONe, the organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) shall share the outcome of the relevant cybersecurity exercise. The organisers shall share with each entity participating in the exercises the information referred to in paragraph 2, points (a) and (b) of this Article. The organisers shall share the list of recommendations referred to in that paragraph, point (c) exclusively with the entities addressed in the recommendations.

Article 45(4)

The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) shall follow up regularly with the entities participating in the exercises on the implementation of the recommendations pursuant to paragraph 2, point (c) of this Article.

Article 46

1. The entities listed in Article 2(1) shall ensure that information provided, received, exchanged or transmitted under this Regulation is accessible only on a need-to-know basis and in accordance with relevant Union and national rules on security of information.

2. The entities listed in Article 2(1) shall ensure that information provided, received, exchanged or transmitted under this Regulation is handled and tracked during the entire life-cycle of that information and that it may be released at the end of its life-cycle only after being anonymised.

3. The entities listed in Article 2(1) shall ensure that all necessary protection measures of organisational and technical nature are in place to safeguard and protect the confidentiality, integrity, availability and non-repudiation of information provided, received, exchanged or transmitted under this Regulation, independently from the means used. The protection measures shall: (a) be proportionate; (b) take into consideration cybersecurity risks related to

known past and emerging threats to which such information may be subject in the context of this Regulation; (c) to the extent possible, be based on national, European or international standards and best practices; (d) be documented.

4. The entities listed in Article 2(1) shall ensure that any individual who is granted access to information provided, received, exchanged or transmitted under this Regulation is briefed on the security rules applicable at entity level and on the measures and procedures relevant to the protection of information. Those entities shall ensure that the concerned individual acknowledges the responsibility to protect the information as instructed during the briefing.

5. The entities listed in Article 2(1) shall ensure that access to information provided, received, exchanged or transmitted under this Regulation is limited to individuals: (a) who are authorised to access that information based on their functions and limited to the execution of the tasks assigned; (b) for whom the entity was able to assess ethical and integrity principles, as well as for whom there is no evidence of negative outcome from a background verification check to evaluate reliability of the individual in accordance with the best practices and standard security requirements of the entity, and, where necessary, with the national laws and regulations.

6. The entities listed in Article 2(1) shall have the written agreement of the natural or legal person that originally created or provided the information, prior to providing that information to a third party that falls outside the scope of this Regulation.

7. An entity listed in Article 2(1) may consider that this information shall be shared without complying with paragraphs 1 and 4 of this Article in order to prevent a simultaneous electricity crisis with a cybersecurity root cause or any cross-border crisis within the Union in another sector. In that case, it shall: (a) consult and be authorised by the competent authority to share such information; (b) anonymise such information without losing the elements necessary to inform the public of an imminent and serious risk to cross-border electricity flows and the possible mitigation measures; (c) safeguard the identity of the originator and of the entities that have been processing such information under this Regulation.

8. By derogation from paragraph 6 of this Article, the competent authorities may provide information provided, received, exchanged or transmitted under this Regulation to a third party not listed in Article 2(1) without a written prior consent of the originator of the information but informing the latter at the earliest time possible. Before disclosing any information provided, received, exchanged or transmitted under this Regulation to a third party not listed in Article 2(1), the concerned competent authority shall reasonably ensure that the concerned third party is aware of the security rules in force and shall receive reasonable assurance that the concerned third party can protect the received information in compliance with paragraphs 1 to 5 of this Article. The competent authority shall anonymise such information without losing the elements necessary to inform the public of an imminent and serious risk to cross-border electricity flows and possible mitigations measures and safeguard the identity of the originator of the information. In this case, the third party not listed in Article 2(1) shall protect the received information in accordance with provisions already in force at entity level, or where this is not possible, with the provisions and instructions provided by the relevant competent authority.

9. This Article does not apply to entities not listed in Article 2(1) that are provided with information pursuant to paragraph 6 of this Article. In this case paragraph 7 of this Article shall be applied, or the competent authority may provide that entity with written provisions to apply in cases where information is received pursuant to this Regulation.

Article 46(1)

The entities listed in Article 2(1) shall ensure that information provided, received, exchanged or transmitted under this Regulation is accessible only on a need-to-know basis and in accordance with relevant Union and national rules on security of information.

Article 46(2)

The entities listed in Article 2(1) shall ensure that information provided, received, exchanged or transmitted under this Regulation is handled and tracked during the entire life-cycle of that information and that it may be released at the end of its life-cycle only after being anonymised.

Article 46(3)

The entities listed in Article 2(1) shall ensure that all necessary protection measures of organisational and technical nature are in place to safeguard and protect the confidentiality, integrity, availability and non-repudiation of information provided, received, exchanged or transmitted under this Regulation, independently from the means used. The protection measures shall:

a. be proportionate;
b. take into consideration cybersecurity risks related to known past and emerging threats to which such information may be subject in the context of this Regulation;
c. to the extent possible, be based on national, European or international standards and best practices;
d. be documented.

Article 46(4)

The entities listed in Article 2(1) shall ensure that any individual who is granted access to information provided, received, exchanged or transmitted under this Regulation is briefed on the security rules applicable at entity level and on the measures and procedures relevant to the protection of information. Those entities shall ensure that the concerned individual acknowledges the responsibility to protect the information as instructed during the briefing.

Article 46(5)

The entities listed in Article 2(1) shall ensure that access to information provided, received, exchanged or transmitted under this Regulation is limited to individuals:

a. who are authorised to access that information based on their functions and limited to the execution of the tasks assigned;

b. for whom the entity was able to assess ethical and integrity principles, as well as for whom there is no evidence of negative outcome from a background verification check to evaluate reliability of the individual in accordance with the best practices and standard security requirements of the entity, and, where necessary, with the national laws and regulations.

Article 46(6)

The entities listed in Article 2(1) shall have the written agreement of the natural or legal person that originally created or provided the information, prior to providing that information to a third party that falls outside the scope of this Regulation.

Article 46(7)

An entity listed in Article 2(1) may consider that this information shall be shared without complying with paragraphs 1 and 4 of this Article in order to prevent a simultaneous electricity crisis with a cybersecurity root cause or any cross-border crisis within the Union in another sector. In that case, it shall:

a. consult and be authorised by the competent authority to share such information;

b. anonymise such information without losing the elements necessary to inform the public of an imminent and serious risk to cross-border electricity flows and the possible mitigation measures;

c. safeguard the identity of the originator and of the entities that have been processing such information under this Regulation.

Article 46(8)

By derogation from paragraph 6 of this Article, the competent authorities may provide information provided, received, exchanged or transmitted under this Regulation to a third party not listed in Article 2(1) without a written prior consent of the originator of the information but informing the latter at the earliest time possible. Before disclosing any information provided, received, exchanged or transmitted under this Regulation to a third party not listed in Article 2(1), the concerned competent authority shall reasonably ensure that the concerned third party is aware of the security rules in force and shall receive reasonable assurance that the concerned third party can protect the received information in compliance with paragraphs 1 to 5 of this Article. The competent authority shall anonymise such information without losing the elements necessary to inform the public of an imminent and serious risk to cross-border electricity flows and possible mitigations measures and safeguard the identity of the originator of the information. In this case, the third party not listed in Article 2(1) shall protect the received information in accordance with provisions already in force at entity level, or where this is not possible, with the provisions and instructions provided by the relevant competent authority.

Article 46(9)

This Article does not apply to entities not listed in Article 2(1) that are provided with information pursuant to paragraph 6 of this Article. In this case paragraph 7 of this Article shall be applied, or the competent authority may provide that entity with written provisions to apply in cases where information is received pursuant to this Regulation.

Article 47

1. Any information provided, received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraphs 2 to 5 of this Article of this Regulation and requirements as laid down in Article 65 of Regulation (EU) 2019/943. Any information provided, received, exchanged or transmitted among entities listed in Article 2 of this Regulation, for the purposes of implementing this Regulation, shall be protected, considering the confidentiality level of the information applied by the originator.
2. The obligation of professional secrecy shall apply to the entities listed in Article 2.
3. The CS-NCAs, the NRAs, the RP-NCAs and the CSIRTs shall exchange all necessary information to carry out their tasks.
4. Any information received, exchanged or transmitted among entities listed in Article 2(1), for the purposes of implementing Article 23, shall be anonymised and aggregated.
5. Information received by any entity or authority subject to this Regulation in the course of their duties may not be disclosed to any other entity or authority, without prejudice to cases covered by national law, other provisions of this Regulation or other relevant Union legislation.
6. Without prejudice to national or Union legislation, an authority, entity or natural person who receives information pursuant to this Regulation may not use it for any other purpose than carrying out its duties under this Regulation.
7. ACER, after consulting ENISA, all competent authorities, ENTSO for Electricity and the EU-DSO Entity, shall by 13 June 2025 issue guidelines addressing mechanisms for all entities listed in Article 2(1) to exchange information, and in particular envisaged communication flows, and methods to anonymise and to aggregate information for the purpose of implementation of this Article.
8. Information that is confidential pursuant to Union and national rules shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Regulation. The information exchanged shall be limited to that which is necessary and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of critical-impact or high-impact entities.

Article 47(1)

Any information provided, received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraphs 2 to 5 of this Article of this Regulation and requirements as laid down in Article 65 of Regulation (EU) 2019/943. Any information provided, received, exchanged or transmitted among entities listed in Article 2 of this Regulation, for the purposes of implementing this Regulation, shall be protected, considering the confidentiality level of the information applied by the originator.

Article 47(2)

The obligation of professional secrecy shall apply to the entities listed in Article 2.

Article 47(3)

The CS-NCAs, the NRAs, the RP-NCAs and the CSIRTs shall exchange all necessary information to carry out their tasks.

Article 47(4)

Any information received, exchanged or transmitted among entities listed in Article 2(1), for the purposes of implementing Article 23, shall be anonymised and aggregated.

Article 47(5)

Information received by any entity or authority subject to this Regulation in the course of their duties may not be disclosed to any other entity or authority, without prejudice to cases covered by national law, other provisions of this Regulation or other relevant Union legislation.

Article 47(6)

Without prejudice to national or Union legislation, an authority, entity or natural person who receives information pursuant to this Regulation may not use it for any other purpose than carrying out its duties under this Regulation.

Article 47(7)

ACER, after consulting ENISA, all competent authorities, ENTSO for Electricity and the EU-DSO Entity, shall by 13 June 2025 issue guidelines addressing mechanisms for all entities listed in Article 2(1) to exchange information, and in particular envisaged communication flows, and methods to anonymise and to aggregate information for the purpose of implementation of this Article.

Article 47(8)

Information that is confidential pursuant to Union and national rules shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Regulation. The information exchanged shall be limited to that which is necessary and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of critical-impact or high-impact entities.

Article 48

1. Until the approval of the terms and conditions or methodologies referred to in Article 6(2) or plans referred to in Article 6(3), the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop non-binding guidance on the following issues: (a) a provisional electricity cybersecurity impact index (ECII) pursuant to paragraph 2 of this Article; (b) a provisional list of Union-wide high-impact and critical-impact processes pursuant to paragraph 4 of this Article; and (c) a provisional list of European and international standards and controls required by national legislatio
2. By 13 October 2024, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a recommendation for a provisional ECII. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall notify the recommended provisional ECII to the competent authorities.
3. Four months of receipt of the recommended provisional ECII, or the latest by 13 February 2025, the competent authorities shall identify candidates for high-impact and critical-impact entities in their Member State based on the recommended ECII and shall develop a provisional list of high-impact and critical-impact entities.
4. The high-impact and critical-impact entities identified in the provisional list may voluntarily fulfil their obligations as laid down in this Regulation based on a precautionary principle. By 13 March 2025, the competent authorities shall notify the entities identified in the provisional list that they have been identified as a high-impact or critical-impact entity.
5. By 13 December 2024, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a provisional list of Union-wide high-impact and critical-impact processes.
6. The entities notified pursuant to paragraph (3) that voluntarily decide to fulfil their obligations as laid down in this Regulation based on a precautionary principle shall use the provisional list of high-impact and critical-impact processes to determine the provisional high-impact and critical-impact perimeters and to determine which assets are to be included in the first cybersecurity risk assessment at entity level.
7. By 13 September 2024, each competent authority according to Article 4 (1) shall provide a list of its national legislation with relevance for cybersecurity aspects of cross-border electricity flows to the ENTSO for Electricity and the EU DSO entity.
8. By 13 June 2025, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall prepare a provisional list of European and international standards and controls required by national

legislation with relevance for cybersecurity aspects of cross-border electricity flows, taking into account the information provided by the competent authorities.

9. The provisional list of European and international standards and controls shall include: (a) European and international standards and national legislation which provide guidance on methodologies for cybersecurity risk management at entity level; and (b) cybersecurity controls equivalent to the controls that are expected to be part of the minimum and advanced cybersecurity controls.
10. The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by ENISA and ACER when finalising the provisional list of standards. The ENTSO for Electricity and the EU DSO entity shall publish the transitional list of European and international standards and controls on their websites.
11. The ENTSO for Electricity and the EU DSO entity shall consult ENISA and ACER on the proposals for non-binding guidance developed pursuant to paragraph 1.
12. Until the minimum and advanced cybersecurity controls are developed pursuant to Article 29 and adopted pursuant to Article 8, all entities listed in Article 2(1) shall strive to progressively apply the non-binding guidance developed pursuant to paragraph 1.

Article 48(1)

Until the approval of the terms and conditions or methodologies referred to in Article 6(2) or plans referred to in Article 6(3), the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop non-binding guidance on the following issues:

a. a provisional electricity cybersecurity impact index ('ECII') pursuant to paragraph 2 of this Article;
b. a provisional list of Union-wide high-impact and critical-impact processes pursuant to paragraph 4 of this Article; and
c. a provisional list of European and international standards and controls required by national legislatio

Article 48(10)

Until the minimum and advanced cybersecurity controls are developed pursuant to Article 29 and adopted pursuant to Article 8, all entities listed in Article 2(1) shall strive to progressively apply the non-binding guidance developed pursuant to paragraph 1.

Article 48(2)

By 13 October 2024, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a recommendation for a provisional ECII. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall notify the recommended provisional ECII to the competent authorities.

Article 48(3)

Four months of receipt of the recommended provisional ECII, or the latest by 13 February 2025, the competent authorities shall identify candidates for high-impact and critical-impact entities in their Member State based on the recommended ECII and shall develop a provisional list of high-impact and critical-impact entities.

The high-impact and critical-impact entities identified in the provisional list may voluntarily fulfil their obligations as laid down in this Regulation based on a precautionary principle. By 13 March 2025, the competent authorities shall notify the entities identified in the provisional list that they have been identified as a high-impact or critical-impact entity.

Article 48(4)

By 13 December 2024, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a provisional list of Union-wide high-impact and critical-impact processes.

The entities notified pursuant to paragraph (3) that voluntarily decide to fulfil their obligations as laid down in this Regulation based on a precautionary principle shall use the provisional list of high-impact and critical-impact processes to determine the provisional high-impact and critical-impact perimeters and to determine which assets are to be included in the first cybersecurity risk assessment at entity level.

Article 48(5)

By 13 September 2024, each competent authority according to Article 4 (1) shall provide a list of its national legislation with relevance for cybersecurity aspects of cross-border electricity flows to the ENTSO for Electricity and the EU DSO entity.

Article 48(6)

By 13 June 2025, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall prepare a provisional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows, taking into account the information provided by the competent authorities.

Article 48(7)

The provisional list of European and international standards and controls shall include:

a. European and international standards and national legislation which provide guidance on methodologies for cybersecurity risk management at entity level; and
b. cybersecurity controls equivalent to the controls that are expected to be part of the minimum

and advanced cybersecurity controls.

Article 48(8)

The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by ENISA and ACER when finalising the provisional list of standards. The ENTSO for Electricity and the EU DSO entity shall publish the transitional list of European and international standards and controls on their websites.

Article 48(9)

The ENTSO for Electricity and the EU DSO entity shall consult ENISA and ACER on the proposals for non-binding guidance developed pursuant to paragraph 1.

Article 5

The competent authorities shall coordinate and ensure appropriate cooperation between the competent authorities responsible for cybersecurity, the cyber crisis management authorities, the NRAs, competent authorities for risk preparedness and CSIRTs for the purpose of the fulfilment of the relevant obligations laid down in this Regulation. The competent authorities shall also coordinate with any other bodies or authorities as determined by each Member State, to ensure efficient procedures and avoid duplications of tasks and obligations. The competent authorities shall be able to instruct the respective NRAs to request ACER for an opinion pursuant to Article 8(3).

Article 6

1. TSOs shall develop, in cooperation with the EU DSO entity, proposals for the terms and conditions or methodologies pursuant to paragraph 2, or for plans pursuant to paragraph 3.
2. The following terms and conditions or methodologies and any amendments thereof shall be subject to approval by all competent authorities:

a. the cybersecurity risk assessment methodologies pursuant to Article 18(1);

b. the comprehensive cross-border electricity cybersecurity risk assessment report pursuant to Article 23;

c. the minimum and advanced cybersecurity controls pursuant to Article 29, the mapping of electricity cybersecurity controls against standards pursuant to Article 34, including minimum and advanced cybersecurity controls in the supply chain in accordance with Article 33;

d. a cybersecurity procurement recommendation pursuant to Article 35;

e. the cyber-attacks classification scale methodology pursuant to Article 37(8).

1. The proposals for the regional cybersecurity risk mitigation plans pursuant to Article 22 shall be subject to approval by all competent authorities of the concerned system operation region.
2. The proposals for terms and conditions, methodologies listed in paragraph 2, or for plans listed in paragraph 3, shall include a proposed timescale for their implementation and a description of their expected impact on the objectives of this Regulation.
3. The EU DSO entity may provide a reasoned opinion to the concerned TSOs until 3 weeks before the deadline to submit the proposal for terms and conditions or methodologies or plans to the competent authorities.
4. TSOs responsible for the proposal for terms and conditions or methodologies or plans shall take into consideration the reasoned opinion of the EU DSO entity prior to its submission for competent authorities approval. TSOs shall provide reasoning where the EU DSO entity opinion is not taken into account.
5. When jointly developing terms, conditions and methodologies and plans, the participating TSOs shall closely cooperate. TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall regularly inform competent authorities and ACER about the progress of developing the terms and conditions or methodologies, or plans.

Article 6(1)

TSOs shall develop, in cooperation with the EU DSO entity, proposals for the terms and conditions or methodologies pursuant to paragraph 2, or for plans pursuant to paragraph 3.

Article 6(2)

The following terms and conditions or methodologies and any amendments thereof shall be subject to approval by all competent authorities:

a. the cybersecurity risk assessment methodologies pursuant to Article 18(1);

b. the comprehensive cross-border electricity cybersecurity risk assessment report pursuant to Article 23;

c. the minimum and advanced cybersecurity controls pursuant to Article 29, the mapping of electricity cybersecurity controls against standards pursuant to Article 34, including minimum and advanced cybersecurity controls in the supply chain in accordance with Article 33;

d. a cybersecurity procurement recommendation pursuant to Article 35;

e. the cyber-attacks classification scale methodology pursuant to Article 37(8).

Article 6(3)

The proposals for the regional cybersecurity risk mitigation plans pursuant to Article 22 shall be subject to approval by all competent authorities of the concerned system operation region.

Article 6(4)

The proposals for terms and conditions, methodologies listed in paragraph 2, or for plans listed in paragraph 3, shall include a proposed timescale for their implementation and a description of their expected impact on the objectives of this Regulation.

Article 6(5)

The EU DSO entity may provide a reasoned opinion to the concerned TSOs until 3 weeks before the deadline to submit the proposal for terms and conditions or methodologies or plans to the competent authorities.

TSOs responsible for the proposal for terms and conditions or methodologies or plans shall take into consideration the reasoned opinion of the EU DSO entity prior to its submission for competent authorities' approval. TSOs shall provide reasoning where the EU DSO entity opinion is not taken into account.

Article 6(6)

When jointly developing terms, conditions and methodologies and plans, the participating TSOs shall closely cooperate. TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall regularly inform competent authorities and ACER about the progress of developing the terms and conditions or methodologies, or plans.

Article 7

1. Where TSOs deciding on proposals for terms and conditions or methodologies are not able to reach an agreement, they shall decide by qualified majority voting. A qualified majority for such proposals shall be calculated as follows:

a. TSOs representing at least 55 % of the Member States; and

b. TSOs representing Member States comprising at least 65 % of the population of the Union.

    1. A blocking minority for decisions on proposals for terms and conditions or methodologies listed in Article 6(2) shall include TSOs representing at least four Member States, failing of which the qualified majority shall be deemed attained.

2. Where TSOs of a system operation region deciding on proposals for plans listed in Article 6(2) are not able to reach an agreement, and where the system operation region concerned is composed of more than five Member States, TSOs shall decide by qualified majority voting. A qualified majority for proposals listed in Article 6(2) shall require the following majority:

a. TSOs representing at least 72 % of the Member States concerned; and

b. TSOs representing Member States comprising at least 65 % of the population of the concerned area.

1. A blocking minority for decisions on proposals for the plans shall include at least a minimum number of TSOs representing more than 35 % of the population of the participating Member States, plus TSOs representing at least one additional Member State concerned, failing of which the qualified majority shall be deemed attained.
2. For TSO decisions on proposals for terms and conditions or methodologies pursuant to Article 6(2), one vote shall be attributed per Member State. If there is more than one TSO in the territory of a Member State, the Member State shall allocate the voting powers among the TSOs.
3. If TSOs, in cooperation with the EU DSO entity, fail to submit an initial or amended proposal for terms and conditions or methodologies, or for plans, to the relevant competent authorities within the deadlines set out in this Regulation, they shall provide the relevant competent authorities and ACER with the relevant drafts of the terms and conditions or methodologies, or of the plans. They shall explain what has prevented an agreement. The competent authorities shall jointly take the appropriate steps for the adoption of the required terms and conditions or methodologies, or of the required plans. This may be done for instance by requesting amendments to the drafts pursuant to this paragraph, by revising and completing those drafts, or, where no drafts have been provided, by defining and approving the required terms and conditions or methodologies or plans. 6.

Article 7(1)

Where TSOs deciding on proposals for terms and conditions or methodologies are not able to reach an agreement, they shall decide by qualified majority voting. A qualified majority for such proposals shall be calculated as follows:

a. TSOs representing at least 55 % of the Member States; and

b. TSOs representing Member States comprising at least 65 % of the population of the Union.

Article 7(2)

A blocking minority for decisions on proposals for terms and conditions or methodologies listed in Article 6(2) shall include TSOs representing at least four Member States, failing of which the qualified majority shall be deemed attained.

Article 7(3)

Where TSOs of a system operation region deciding on proposals for plans listed in Article 6(2) are not able to reach an agreement, and where the system operation region concerned is composed of more than five Member States, TSOs shall decide by qualified majority voting. A qualified majority for proposals listed in Article 6(2) shall require the following majority:

a. TSOs representing at least 72 % of the Member States concerned; and

b. TSOs representing Member States comprising at least 65 % of the population of the concerned area.

Article 7(4)

A blocking minority for decisions on proposals for the plans shall include at least a minimum number of TSOs representing more than 35 % of the population of the participating Member States, plus TSOs representing at least one additional Member State concerned, failing of which the qualified majority shall be deemed attained.

Article 7(5)

For TSO decisions on proposals for terms and conditions or methodologies pursuant to Article 6(2), one vote shall be attributed per Member State. If there is more than one TSO in the territory of a Member State, the Member State shall allocate the voting powers among the TSOs.

Article 7(6)

If TSOs, in cooperation with the EU DSO entity, fail to submit an initial or amended proposal for terms and conditions or methodologies, or for plans, to the relevant competent authorities within the deadlines set out in this Regulation, they shall provide the relevant competent authorities and ACER with the relevant drafts of the terms and conditions or methodologies, or of the plans. They shall explain what has prevented an agreement. The competent authorities shall jointly take the appropriate steps for the adoption of the required terms and conditions or methodologies, or of the required plans. This may be done for instance by requesting amendments to the drafts pursuant to this paragraph, by revising and completing those drafts, or, where no drafts have been provided, by defining and approving the required terms and conditions or methodologies or plans.

Article 8

1. TSOs shall submit the proposals for terms and conditions or methodologies, or for plans for approval to the relevant competent authorities within the respective deadlines set out in

Articles 18, 23, 29, 33, 34, 35 and 37.

2. The competent authorities may jointly prolong these deadlines in exceptional circumstances, notably in cases where a deadline cannot be met due to circumstances external to the sphere of TSOs or of the EU DSO entity.

3. Proposals for terms and conditions, methodologies or for plans pursuant to paragraph 1, shall be submitted for information to ACER at the same time that they are submitted to the competent authorities.

4. Upon a joint request of the NRAs, ACER shall issue an opinion on the proposal for terms and conditions or methodologies, or for the plans, within six months of the receipt of the proposals for terms and conditions or methodologies, or for plans and notify NRAs and competent authorities of the opinion.

5. NRAs, CS-NCAs and any other authorities designated as competent authorities shall coordinate with each other before the NRAs requests an opinion to ACER.

6. ACER may include recommendations in such opinion. ACER shall consult ENISA before issuing an opinion on the proposals listed in Article 6(2).

7. The competent authorities shall consult and closely cooperate and coordinate with each other in order to reach an agreement on the proposed terms and conditions, methodologies, or plans. Before approving the terms and conditions or methodologies, or the plans, they shall revise and complete the proposals where necessary, after consulting the ENTSO for Electricity and the EU DSO entity, in order to ensure that the proposals are in line with this Regulation and contribute to a high common level of cybersecurity across the Union.

8. The competent authorities shall decide on the terms and conditions or methodologies or on the plans within six months following the receipt of the terms and conditions or methodologies or of the plans by the relevant competent authority or, where applicable, by the last relevant competent authority concerned.

9. Where ACER issues an opinion, the relevant competent authorities shall take that opinion into account and shall take their decisions within six months from the receipt of ACER s opinion.

10. Where the competent authorities jointly require an amendment to the proposed terms and conditions or methodologies, or the plans, in order to approve them, the TSOs shall develop, in cooperation with the EU DSO entity, a proposal for such amendment to the terms and conditions or methodologies, or the plans. The TSOs shall submit the amended proposal for approval within two months following the request of the competent authorities.

11. The competent authorities shall decide on the amended terms and conditions or methodologies, or plans, within two months following their submission.

12. Where the competent authorities have not been able to reach an agreement within the period referred to in paragraph 5 or 7, they shall inform the Commission. The Commission may take appropriate steps to make possible the adoption of the required terms and conditions or methodologies, or plans. 8.

13. TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO entity shall publish the terms and conditions or methodologies, or the plans, on their websites following approval by the relevant competent authorities, except where such information is considered as confidential in accordance with Article 47.

14. The competent authorities may jointly request proposals for amendments of the approved terms and conditions or methodologies, or of the approved plans, from TSOs and the EU DSO entity and determine a deadline for the submission of those proposals.

15. TSOs, in cooperation with the EU DSO entity, may propose amendments to the competent authorities also on its own initiative. The proposals for amendment to the terms and conditions or methodologies, or for the amendments to the plans, shall be developed and approved in accordance with the procedure set out in this Article.

16. At least every three years after the first adoption of the respective terms and conditions or methodologies, or the respective adopted plans, TSOs in cooperation with the EU DSO entity, shall review the effectiveness of the adopted terms and conditions or methodologies, or the adopted plans, and shall report the findings of the review to the competent authorities and ACER without undue delay.

Article 8(1)

TSOs shall submit the proposals for terms and conditions or methodologies, or for plans for approval to the relevant competent authorities within the respective deadlines set out in Articles 18, 23, 29, 33, 34, 35 and 37.

The competent authorities may jointly prolong these deadlines in exceptional circumstances, notably in cases where a deadline cannot be met due to circumstances external to the sphere of TSOs or of the EU DSO entity.

Article 8(10)

The competent authorities may jointly request proposals for amendments of the approved terms and conditions or methodologies, or of the approved plans, from TSOs and the EU DSO entity and determine a deadline for the submission of those proposals.

TSOs, in cooperation with the EU DSO entity, may propose amendments to the competent authorities also on its own initiative. The proposals for amendment to the terms and conditions or methodologies, or for the amendments to the plans, shall be developed and approved in accordance with the procedure set out in this Article.

Article 8(11)

At least every three years after the first adoption of the respective terms and conditions or methodologies, or the respective adopted plans, TSOs in cooperation with the EU DSO entity, shall review the effectiveness of the adopted terms and conditions or methodologies, or the adopted plans, and shall report the findings of the review to the competent authorities and ACER without undue delay.

Article 8(2)

Proposals for terms and conditions, methodologies or for plans pursuant to paragraph 1, shall be submitted for information to ACER at the same time that they are submitted to the competent authorities.

Article 8(3)

Upon a joint request of the NRAs, ACER shall issue an opinion on the proposal for terms and conditions or methodologies, or for the plans, within six months of the receipt of the proposals for terms and conditions or methodologies, or for plans and notify NRAs and competent authorities of the opinion.

NRAs, CS-NCAs and any other authorities designated as competent authorities shall coordinate with each other before the NRAs requests an opinion to ACER.

ACER may include recommendations in such opinion. ACER shall consult ENISA before issuing an opinion on the proposals listed in Article 6(2).

Article 8(4)

The competent authorities shall consult and closely cooperate and coordinate with each other in order to reach an agreement on the proposed terms and conditions, methodologies, or plans. Before approving the terms and conditions or methodologies, or the plans, they shall revise and complete the proposals where necessary, after consulting the ENTSO for Electricity and the EU DSO entity, in order to ensure that the proposals are in line with this Regulation and contribute to a high common level of cybersecurity across the Union.

Article 8(5)

The competent authorities shall decide on the terms and conditions or methodologies or on the plans within six months following the receipt of the terms and conditions or methodologies or of the plans by the relevant competent authority or, where applicable, by the last relevant competent authority concerned.

Article 8(6)

Where ACER issues an opinion, the relevant competent authorities shall take that opinion into account and shall take their decisions within six months from the receipt of ACER's opinion.

Article 8(7)

Where the competent authorities jointly require an amendment to the proposed terms and conditions or methodologies, or the plans, in order to approve them, the TSOs shall develop, in cooperation with the EU DSO entity, a proposal for such amendment to the terms and conditions or

methodologies, or the plans. The TSOs shall submit the amended proposal for approval within two months following the request of the competent authorities.

The competent authorities shall decide on the amended terms and conditions or methodologies, or plans, within two months following their submission.

Article 8(8)

Where the competent authorities have not been able to reach an agreement within the period referred to in paragraph 5 or 7, they shall inform the Commission. The Commission may take appropriate steps to make possible the adoption of the required terms and conditions or methodologies, or plans.

Article 8(9)

TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO entity shall publish the terms and conditions or methodologies, or the plans, on their websites following approval by the relevant competent authorities, except where such information is considered as confidential in accordance with Article 47.

Article 9

1. TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall consult stakeholders, including ACER, ENISA and the competent authority of each Member State, on the draft proposals for terms and conditions or methodologies listed in Article 6(2) and for plans referred to in Article 6(3). The consultation shall last for a period of not less than one month.
2. The proposals for terms and conditions or methodologies listed in Article 6(2) submitted by the TSOs, in cooperation with the EU DSO entity, shall be published and submitted to consultation at Union level. The proposals for plans listed in Article 6(3) submitted by the relevant TSOs, in cooperation with the EU DSO entity, at regional level shall be submitted to consultation at least at regional level.
3. TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO Entity responsible for the proposal for terms and conditions or methodologies or plans shall duly take into account the views of stakeholders resulting from the consultations undertaken in accordance with paragraph 1, prior to its submission for regulatory approval. In all cases, a sound justification for including or not including the views resulting from the consultation shall be provided together with the submission and published in a timely manner before or simultaneously with the proposal for terms and conditions or methodologies.

Article 9(1)

TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall consult stakeholders, including ACER, ENISA and the competent authority of each Member State, on the draft proposals for terms and conditions or methodologies listed in Article 6(2) and for plans referred to in Article 6(3). The consultation shall last for a period of not less than one month.

Article 9(2)

The proposals for terms and conditions or methodologies listed in Article 6(2) submitted by the TSOs, in cooperation with the EU DSO entity, shall be published and submitted to consultation at Union level. The proposals for plans listed in Article 6(3) submitted by the relevant TSOs, in cooperation with the EU DSO entity, at regional level shall be submitted to consultation at least at regional level.

Article 9(3)

TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO Entity responsible for the proposal for terms and conditions or methodologies or plans shall duly take into account the views of stakeholders resulting from the consultations undertaken in accordance with paragraph 1, prior to its submission for regulatory approval. In all cases, a sound justification for including or not including the views resulting from the consultation shall be provided together with the submission and published in a timely manner before or simultaneously with the proposal for terms and conditions or methodologies.

Computer Security Incident Response Teams (CSIRT)

A dedicated center where a technical team consisting of one or more experts, supported by cybersecurity IT systems, performs security-related tasks (Cybersecurity Operation Center [CSOC] services) such as handling cyber-attacks and security configuration errors, security monitoring, log analysis, and cyber-attack detection.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [56]

Computer Security Incident Response Teams (CSIRT)

A dedicated center where a technical team consisting of one or more experts, supported by cybersecurity IT systems, performs security-related tasks (Cybersecurity Operation Center [CSOC] services) such as handling cyber-attacks and security configuration errors, security monitoring, log analysis, and cyber-attack detection.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [57]

[56] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[57] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

Critical ICT service provider

Means an entity which provides an ICT service, or ICT process that is necessary for a critical-impact or high-impact process affecting cybersecurity aspects of cross-border electricity flows and that, if compromised, may cause a cyber-attack with impact above the critical-impact or high-impact threshold.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [58]

Critical-impact entity

Means an entity that carries out a critical-impact process and that is identified by the competent authorities in accordance with Article 24. [59]

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [60]

DG CONNECT (Directorate-General for Communications Networks, Content and Technology)

The Directorate-General for Communications Networks, Content and Technology (DG CONNECT) develops and implements the European Commission's policies.

DG ENER (Directorate-General for Energy)

The Directorate-General for Energy of the European Commission is responsible for the EU's energy policy.

Distribution System Operator (DSO)

A natural or legal person responsible for operating, maintaining, and, if necessary, developing a distribution system in a given area, as well as for ensuring long-term capacity to meet justified demands for electricity distribution.

DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [61]

DSO Entity (EU DSO)

European Distribution System Operators Organization

[58] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[59] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[60] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[61] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944

The European Distribution System Operators Organization was established by the European Union to coordinate and develop electricity distribution system operations. The role of the EU DSO is particularly crucial in the integration of energy markets, the incorporation of renewable energy sources, and supporting the energy transition.

The EU DSO's activities are regulated by the EU Clean Energy Package and the Electricity Market Regulation (Regulation (EU) 2019/943).

https://eudsoentity.eu/ [62]

REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [63]

Electricity Coordination Group (ECG)

Electricity Coordination Group

The goal of the Electricity Coordination Group is to share and coordinate information on electricity policy measures with cross-border impacts, facilitating cooperation through knowledge and experience exchange.

COMMISSION DECISION 2012/C 353/02 [64]

European Commission (EC)

The European Commission is the executive branch of the European Union, responsible for implementing EU legislation, developing policies, and managing the budget.

European Network of Transmission System Operators for Electricity (ENTSO-E)

European Network of Transmission System Operators for Electricity

ENTSO-E is the common organization of European transmission system operators (TSOs). It plays a central role in the integration of the European electricity market and ensuring the stability of the electricity system. ENTSO-E's activities are regulated by the EU Clean Energy Package and the Electricity Market Regulation (Regulation (EU) 2019/943).

https://www.entsoe.eu/ [65]

REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [66]

European Union Agency for Cybersecurity (ENISA)

[62] https://eudsoentity.eu/
[63] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[64] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D1117(01)
[65] https://www.entsoe.eu/
[66] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943

ENISA is the EU's cybersecurity agency, supporting Member States in defending against cyber threats.

High-impact entity

Means an entity that carries out a high-impact process and that is identified by the competent authorities in accordance with Article 24. [67]

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [68]

Member state

Means a country that is a member of the European Union and complies with EU legislation.

National Competent Authority (NCA)

A national competent authority is an official body or organization authorized by legislation to regulate, supervise, and oversee a specific sector or area. These authorities ensure compliance with national and, where relevant, international laws and standards.

National Cybersecurity Competent Authorities (CS NCA)

The national competent authority responsible for cybersecurity within a given Member State.

National Regulatory Authority (NRA)

An official state or independent organization responsible for regulating, supervising, and overseeing designated areas within a country or region.

Network and Information Systems Cooperation Group (NIS CG)

Cybersecurity Cooperation Group

The Network and Information Security Cooperation Group (NIS CG) coordinates EU cybersecurity cooperation. The tasks of the NIS Cooperation Group are outlined in Article 11 of the NIS Directive.

COMMISSION IMPLEMENTING DECISION (EU) 2017/179 [69]

[67] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_19
[68] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[69] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017D0179

Nominated Electricity Market Operator (NEMO)

A Nominated Electricity Market Operator (NEMO) is a market operator designated by the competent authority of an EU Member State to participate in the operation of the Single Day-Ahead Market Coupling or the Single Intraday Market Coupling.

Regional Coordination Center (RCC)

Regional Coordination Centers (RCC)

These centers have a consultative role in the development of regional cybersecurity risk assessment and risk mitigation plans, coordinating Member States' cooperation in cybersecurity.

Established under Article 35 of Regulation (EU) 2019/943.

REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [70]

Risk Preparedness National Competent Authority (RP-NCA)

The RP-NCAs are responsible for developing and implementing risk preparedness plans.

System Operators

As defined in Article 2(29) and Article 2(35) of Directive (EU) 2019/944.

DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [71]

Transmission System Operator (TSO)

A natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity.

DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [72]

[70] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[71] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[72] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944

Resources

FILE 1

Provisional list of Union-wide high-impact and critical-impact processes (English)

files/Provisional list of Union-wide high-impact and critical-impact processes.pdf

FILE 2

Supporting document for the provisional list of Union-wide high-impact and critical-impact processes (English)

files/Supporting document Provisional list of Union-wide high-impact and critical-impact processes.pdf

FILE 3

Provisional Electricity Cybersecurity Impact Index (ECII) (English)

files/Provisional ECII.pdf

FILE 4

Supporting document for the provisional Electricity Cybersecurity Impact Index (ECII) (English)

files/Supporting document provisional ECII.pdf