NISTify ENERGY

E-LEARNING COURSE

Introduction to the Implementation of the NCCS Regulation - Full version

NIS2U GmbH

1.0.0 – 08/01/2025

Contents

Chapter 1

Introduction

The NCCS (Network Code on Cybersecurity), as established by the COMMISSION DELEGATED REGULATION (EU) 2024/1366 [1], aims to create a unified cybersecurity framework within the European electricity sector, ensuring the security of cross-border electricity flows. 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.

The Network Code on Cybersecurity NCCS was officially adopted on May 24, 2024.

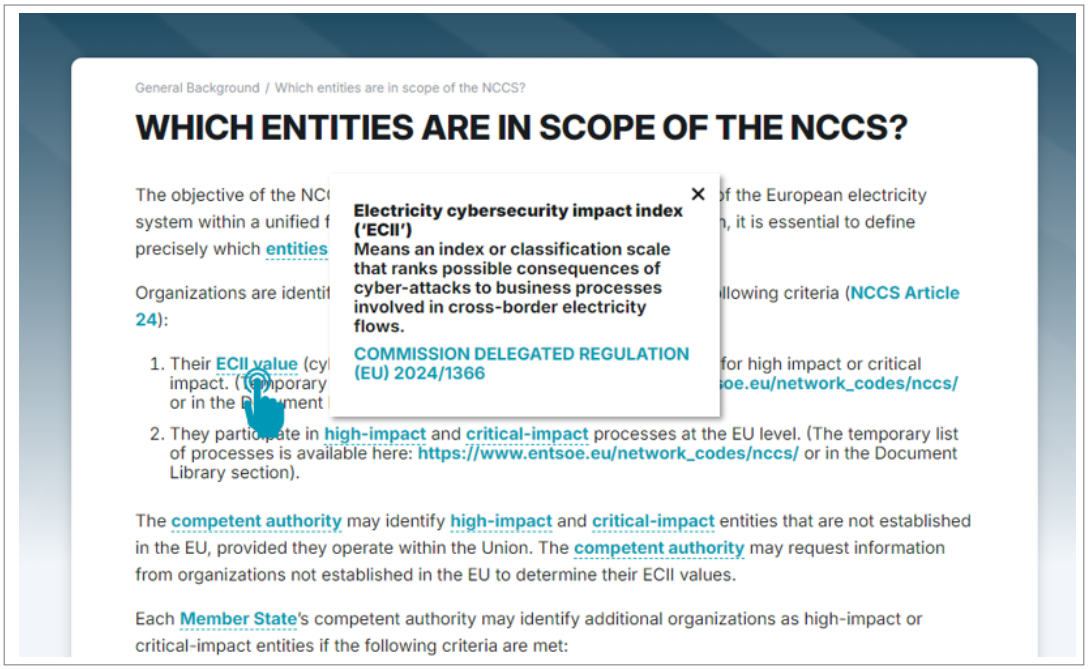
The regulation came into effect immediately upon its publication in the Official Journal of the European Union.

The objective of this material is to support electricity sector stakeholders in understanding and effectively applying the NCCS cybersecurity regulation.

1.1 NCCS basic definitions

Before starting the course material, it is advisable to familiarize yourself with the basic definitions. You can review these definitions in this section, and they will also be accessible within the relevant parts of the material by clicking on the respective term.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1738930273703



1.1.1 A

TERM

Accreditation

Shall mean an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.

REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0765

TERM

Asset

Means any information, software or hardware in the network and information systems ei-

ther tangible or intangible, that has value to an individual, an organisation or a government.

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

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

TERM

Assurance level

Means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

TERM

Authorities responsible for the management of cyber crises

Authorities designated or established pursuant to Article 9(1) of Directive (EU) 2022/2555 on the management of cyber crises. Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.

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

1.1.2 C

TERM

CER Directive

On December 14, 2022, the European Union adopted the European Parliament and Council Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC

CER Directive. [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557

TERM

Conformity assessment

Shall mean the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled.

Regulation (EC) 765/2008 of the European Parliament and of the Council [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02008R0765-20210716

TERM

Conformity assessment body

Shall mean a body that performs conformity assessment activities including calibration, testing, certification and inspection.

Regulation (EC) 765/2008 of the European Parliament and of the Council [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02008R0765-20210716

TERM

Conformity self-assessment

Means an action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

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

TERM

Critical-impact asset

Means an asset that is necessary to carry out a critical-impact process.

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

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

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-impact process

Means a business process carried out by an entity for which the electricity cybersecurity impact indices are above the critical-impact threshold.

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

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

TERM

Critical-impact perimeter

Means a perimeter defined by an entity referred to in Article 2(1) [a] 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.

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_2
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

TERM

Critical-impact threshold

Means the values of the electricity cybersecurity impact indices referred to in Article 19(3) b [a], above which a cyber-attack on a business process will cause critical disruption of cross-border electricity flows.

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

TERM

Cross-border flow

Means a physical flow of electricity on a transmission network of a Member State that results from the impact of the activity of producers, customers, or both, outside that Member State on its transmission network.

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:02019R0943-20240716

TERM

Cyber attack

Cyber-attack means a malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset.

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

Cybersecurity

Means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

TERM

Cybersecurity control

Means the actions or procedures carried out with the purpose of avoiding, detecting, counteracting, or minimising cybersecurity risks.

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

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

TERM

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.

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

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

TERM

Cybersecurity operation centre (CSOC)

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.

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

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

TERM

Cybersecurity vulnerability management

Means the practice of identifying and addressing vulnerabilities.

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

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

TERM

Cyber threat

Means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

1.1.3 E

TERM

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.

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

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

TERM

Electricity crisis

Means a present or imminent situation in which there is a significant electricity shortage, as determined by the Member States and described in their risk-preparedness plans, or in which it is impossible to supply electricity to customers.

REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

TERM

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.

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

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

TERM

Entity

Means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations.

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

European cybersecurity certification scheme

Means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

1.1.4 H

TERM

High-impact asset

Means an asset that is necessary to carry out a high-impact process.

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

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

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

TERM

High-impact perimeter

Means a perimeter defined by any entity listed in Article 2(1) [a] 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.

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_2
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

TERM

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.

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

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

TERM

High-impact threshold

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

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

1.1.5 I

TERM

ICT

Information and Communications Technology.

TERM

ICT process

Means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

TERM

ICT product

Means an element or a group of elements of a network or information system.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

TERM

ICT service

Means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

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

TERM

Incident

Means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

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

Incident handling

Means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident.

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

1.1.6 L

TERM

Large-scale cybersecurity incident

Means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States.

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

Legacy ICT system

Means an ICT system that has reached the end of its lifecycle (end-of-life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity.

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554

1.1.7 M

TERM

Mapping matrix

Developed in accordance with COMMISSION DELEGATED REGULATION (EU) 2024/1366 Art.34 [a], that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_34

TERM

Managed security service provider

Means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management.

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

Managed service provider

Means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely.

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

Member state

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

1.1.8 N

TERM

National accreditation body

Shall mean the sole body in a Member State that performs accreditation with authority derived from the State.

REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02008R0765-20210716

TERM

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 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a].

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

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

TERM

Near miss

Means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise.

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

Network and information system

Means:

Article 6 point (1): . an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972; . any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or . digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

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

1.1.9 O

TERM

Originator

Means an entity that initiates an information exchange, information sharing or information storage event.

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

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

TERM

OT (Operation Technology)

OT is the combination of production automation, machine-to-machine communication and data collection.

1.1.10 P

TERM

Procurement specifications

Means the specifications that entities define for the procurement of new or updated ICT products, ICT processes or ICT services.

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

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

1.1.11 R

TERM

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.

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

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

TERM

Risk

Means the potential for loss or disruption caused by an incident and is to be expressed as

a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident.

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

Risk impact matrix

Means a matrix used during risk assessment to determine the resulting risk impact level for each risk assessed.

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

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

1.1.12 S

TERM

Security of network and information systems

Means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems.

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

Significant cyber threat

Means a cyber threat which, based on its technical characteristics, can be assumed to

have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage.

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

Stakeholder

'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.

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

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

TERM

Standard

Means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory.

REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1025

TERM

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, established in accordance with Article 36 of

Regulation (EU) 2019/943.

TERM

Single point of contact at entity level (SPOC)

Means single point of contact at entity level as designated under Article 38(1) point (c); [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_38
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

1.1.13 T

TERM

Technical specification

Means a document that prescribes technical requirements to be fulfilled by a product, process, service or system and which lays down one or more of the following.

REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1025

1.1.14 U

TERM

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.

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

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

1.1.15 V

TERM

Vulnerability

Means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat.

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

1.2 Entities involved in NCCS

During the course, you will encounter various actors involved in the NCCS regulation. Before beginning your studies, it is advisable to become familiar with them.

1.2.1 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

1.2.2 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

1.2.3 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

1.2.4 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

1.2.5 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 cybersecurity 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.

1.2.6 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.

1.2.7 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

1.2.8 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

1.2.9 U

TERM

Union-wide Critical-Impact Process

Any electricity sector process, possibly involving multiple entities, where a cyber-attack

may be deemed critical during the Union-wide cybersecurity risk assessment.

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

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

TERM

Union-wide High-Impact Process

Any electricity sector process, possibly involving multiple entities, where a cyber-attack may be deemed high during the Union-wide cybersecurity risk assessment.

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

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

Chapter 2

General Background

The Network Code on Cybersecurity [1] is a crucial regulation aimed at ensuring the cybersecurity of cross-border electricity flows within the European Union. The aim of this chapter is to provide an overview of the cybersecurity regulation, its necessity, and its background. You will learn why this regulation has become critically important in the electricity sector, which entities fall under its scope, and which authorities are responsible for its implementation.

2.1 Why is the cybersecurity regulation necessary?

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

NOTE

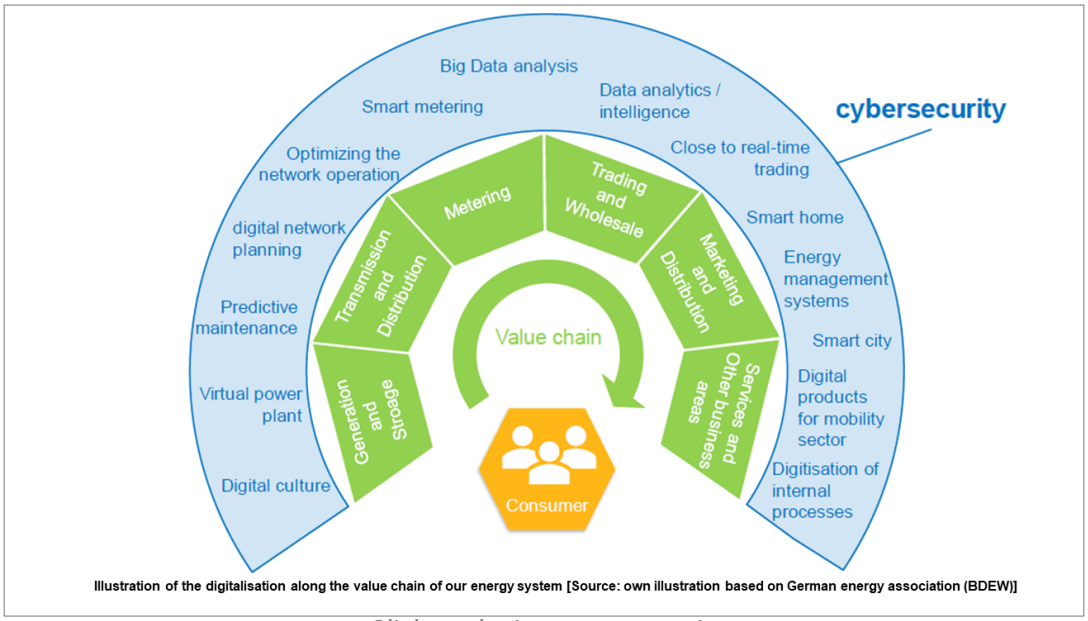
The subtitles of the video were generated using AI tools, so errors may be present.

NCCS is of fundamental importance to European citizens and businesses.

Several factors contribute to this:

- Electricity is vital for European citizens and businesses.
- The electricity sector within the Union is **experiencing a significant transformation**, marked by increasingly decentralised markets with a greater number of participants, a higher share of energy sourced from renewables, and more digitalised and interconnected systems.
- The **interconnected European electricity grid** is unique because it enables the seamless transfer of electricity across multiple countries, enhancing energy security, efficiency, and the integration of renewable energy sources. Here you can find the grid map of the EU: Grid Map [2]
- Europe has set a clear goal of a **fully-integrated internal energy market**, which ensures non-discriminatory market access of existing and new actors and facilitates cross-border energy trading.
- **Digitalisation** and cybersecurity are decisive to provide essential services and therefore of strategic relevance for critical energy infrastructure.
- **Digitalisation creates significant risks** as an increased exposure to cyberattacks and cybersecurity incidents potentially jeopardises the security of energy supply and the privacy of consumer data. The digitalisation of the energy sector comes with a price: increased exposure to cyber incidents and attacks. Ubiquitous connectivity and data collection heighten the already clear need for vigilance with data security for customers, systems or assets. Many energy system assets have been operational since decades in times when communication interconnectivity layers were not considered, or purely monitoring based, or at least tailored for the specific application.

[2] https://www.entsoe.eu/data/map/



Click on the image to zoom in

GOOD TO KNOW

NCCS complementing and building upon NIS2 to include sector-specific cybersecurity requirements provides more precise instructions and procedures.

The goal of NCCS is to establish a **comprehensive and unified cybersecurity framework** for the European **electricity sector**, which is essential for ensuring the **security and reliability** of OT and IT systems in the digital age. This, in turn, guarantees the security of **cross-border electricity** supply.

This Regulation has been developed in close cooperation with ACER, ENISA, the ENTSO for Electricity, the EU DSO entity and other stakeholders, in order to adopt effective, balanced and proportionate rules in a transparent and participative manner.

2.2 Legislations

?**Network Code on Cybersecurity (NCCS)**

COMMISSION DELEGATED REGULATION (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity

flows [a]

On 13 June 2024, the Commission (EU) regulation establishing a European framework for the cyber security of cross-border electricity flows entered into force.

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

?**Legislation on cybersecurity**

- DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [3]

?**Legislation on the resilience of critical entities**

- DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [4]

?**Other relevant legislations**

- REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 June 2019 on the internal market for electricity [5]
- REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC [6]
- REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [7]
- REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision,87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council [8]

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0943
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0941
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1025

- Accreditation of conformity assessment bodies in the European Union [9]
- REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [10]

2.3 Which cybersecurity aspects does the NCCS cover?

The NCCS is a comprehensive regulation that covers multiple aspects of cybersecurity in the electricity sector. The key areas include:

1. Cybersecurity Risk Assessment

Risk assessment is one of the key pillars of the NCCS. Cybersecurity risk management under the scope of the NCCS regulation requires a structured process that includes, among other aspects, the identification of risks arising from cyberattacks affecting cross-border electricity flows, the related operational processes and scopes, as well as appropriate cybersecurity controls and authentication mechanisms. **Risk assessment is conducted cyclically at the EU, regional, national, and entity levels.** The risk-based approach outlined in various provisions aims to identify the processes, supporting assets, and the entities operating them that impact cross-border electricity flows. Depending on the extent to which potential cyberattacks affect these entities' operations related to cross-border electricity flows, the entities may be classified as having a high impact or a critical impact. Member States are responsible for identifying entities that meet the qualification criteria for high-impact and critical-impact entities through the competent authority designated under the NCCS regulation. The cybersecurity risk assessments at the EU, national, regional, and entity levels, as stipulated in the NCCS regulation, may be limited to risks arising from cyberattacks as defined in REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [11] of the European Parliament and the Council. Consequently, they may exclude risks associated with physical attacks, natural disasters, and operational disruptions caused by facility or human resource outages.

The provisions of the NCCS regulation shall not prejudice Union law establishing specific rules for the certification of information and communication technology (ICT) products, ICT services, and ICT processes, particularly concerning the framework for the establishment of European cybersecurity certification schemes, as set out in REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [12] of the European Parliament and the Council.

2. Common Electricity Cybersecurity Framework

With a view to mitigating cybersecurity risks, it is necessary to establish a detailed rulebook governing the actions of, and the cooperation amongst, relevant stakeholders, whose activities concern cybersecurity aspects of cross-border electricity flows, with the aim of ensuring system security. Those organisational and technical rules should ensure that most electricity incidents

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0765
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881

with cybersecurity root causes are effectively dealt with at operational level. It is necessary to set out what those relevant stakeholders should do to prevent such crises and what measures they can take should system operation rules alone no longer suffice. **Therefore, it is necessary to establish a common framework of rules on how to prevent, prepare for and manage simultaneous electricity crises with a cybersecurity root cause.** This brings more transparency in the preparation phase and during a simultaneous electricity crisis and ensures that measures are taken in a coordinated and effective manner together with the competent authorities for cybersecurity in the Member States.

3. Information Sharing

Since the exploitation of vulnerabilities in network and information systems can cause significant disruptions in energy supply and substantial damage to the economy and consumers, these vulnerabilities must be swiftly identified and addressed to mitigate risks. To facilitate the effective implementation of the NCCS regulation, relevant entities and competent authorities must cooperate in practicing and testing activities deemed appropriate for this purpose. This includes the exchange of information related to cyber threats, cyberattacks, vulnerabilities, assets and methods, tactics, techniques, and procedures, as well as cybersecurity crisis management preparedness and other exercises. **The regulation defines the scope of reportable cyberattacks, threats, and vulnerabilities, as well as the rules for information sharing and confidentiality obligations.**

4. Supply Chain Security

Recent cyber-attacks show that entities are increasingly becoming the target of supply chain attacks. Such supply chain attacks not only have an impact on individual entities in the scope but can also have a cascading effect on larger attacks on entities to which they are connected in the electricity grid.

Based on the regulation, minimum and advanced cybersecurity control requirements and procurement recommendations will be formulated for the actors in the supply chain.

2.4 What is the background of NCCS regulation?

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [13] 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 [14] of the European Parliament and of the Council complements DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [15] 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 [16] complements DIRECTIVE

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943

(EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [17] and REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [18] 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 [19] 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) [20] the DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [21] the Cybersecurity Package (JOIN/2017/450 final) [22] 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 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 [23]), whenever cross-border electricity flows are concerned.

GOOD TO KNOW

- The NCCS **is directly applicable and legally binding in all EU Member States.**
- The NCCS entered into force on June 13, 2024.

2.5 Identification method of the entities

The objective of the NCCS regulation is to strengthen the cybersecurity of the European electricity system within a unified framework. To ensure its effective implementation, it is essential to define precisely which **entities** are subject to its requirements.

Entities are identified by the competent authorities based on NCCS Article 24 [24], NCCS Article

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553779410177&uri=CELEX:52013JC0001
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[24] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_24

48 [25].

Identification criteria:

1. Their ECII value (cybersecurity impact index) exceeds the threshold for high impact or critical impact.

Temporary ECII values are available here:

Temporary ECII Values by ENTSO-E [26].

2. They participate in high-impact and critical-impact processes at the EU level.

The temporary list of processes is available here:

Temporary list of processes by ENTSO-E [27].

Identification of additional entities

1. Entities that are not registered in the Union but provide services to entities operating within the Union

The **competent authority** may identify **high-impact** and **critical-impact** entities that are not established in the EU, provided they operate within the Union. The **competent authority** may request information from entities not established in the EU to determine their ECII values. Entities that are not registered in the Union but provide services to entities operating within the Union and have been notified that they qualify as high or critical-impact entity must, within three months of receiving the notification, designate a Union representative in writing and inform the notifying competent authority accordingly, as stipulated in Article 15 of the NCCS.

2. Group of entities

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

a. The entities are part of a group of entities that face a significant risk of being simultaneously affected by a **cyber attack**.

b. The aggregated ECII value for the group exceeds the threshold for high impact or critical impact.

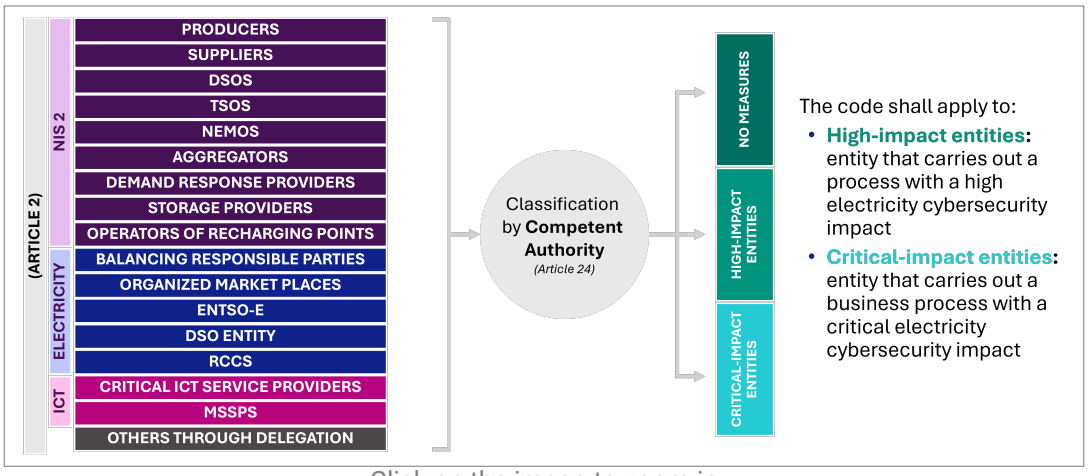
2.6 Which entities are in scope of the NCCS?

Entities are categorized as "**high-impact**" or "**critical-impact**" based on the **potential severity of a cyberattack on their processes and related assets**, as well as its **impact on cross-border**

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_48
[26] https://www.entsoe.eu/network_codes/nccs/
[27] https://www.entsoe.eu/network_codes/nccs/

electricity flows (NCCS Article 24 [28]).

The following entities fall under the scope of NCCS Article 2 Paragraph 1. [29]:



Click on the image to zoom in

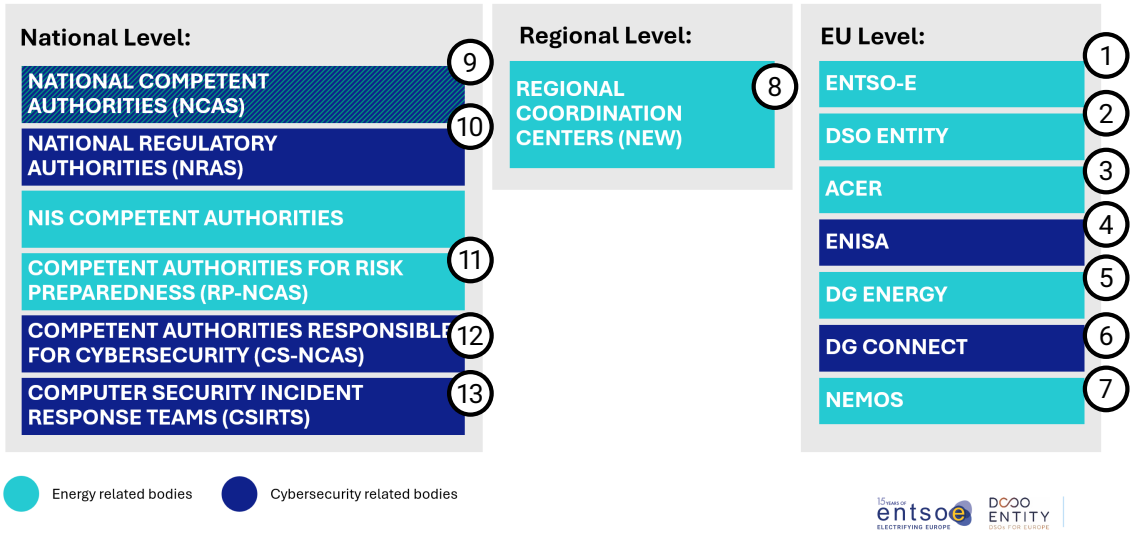
GOOD TO KNOW

- Entities are identified based on defined threshold values (ECII). The competent authority may also assess their participation in EU-wide high-impact and critical-impact processes.
- The competent authority classifies entities into high-impact and critical-impact categories.

2.7 Who is responsible for the governance of the NCCS?

The governance of NCCS involves multiple stakeholders.

[28] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_24
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_2



1

ENTSO-E (European Network of Transmission System Operators for Electricity) The ENTSO-E [30] is an entity that brings together European transmission system operators. Under the NCCS framework, ENTSO-E is responsible for conducting the Union-wide cybersecurity risk assessment (NCCS Article 19 [31]) and compiling regional cybersecurity risk assessment reports (NCCS Article 21 [32]). The regional cybersecurity risk assessment considers cybersecurity-related regional electricity supply crisis scenarios identified under (EU) 2019/941, Article 6 [33]. ENTSO-E, in collaboration with the EU DSO, organizes regional cybersecurity exercises in all system operation regions (NCCS Article 44 [34]).

2

EU DSO (European Distribution System Operators) The EU DSO [35] represents European distribution system operators. Under the NCCS framework, the EU DSO collaborates with ENTSO-E in conducting the Union-wide cybersecurity risk assessment (NCCS Article 19 [36]) and compiling regional cybersecurity risk assessment reports (NCCS Article 21 [37]). ENTSO-E and the EU DSO together organize regional cybersecurity exercises in all system operation regions (NCCS Article 44 [38]).

3

[30] https://www.entsoe.eu/
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_19
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_21
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941#d1e698-1-1
[34] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_44
[35] https://eudsoentity.eu/
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_19
[37] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_21
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_44

ACER (European Union Agency for the Cooperation of Energy Regulators) The ACER [39] is an EU agency that facilitates energy market regulation. Under the NCCS framework, ACER provides opinions on cybersecurity risk assessment methodologies (NCCS Article 8 [40]), monitors the implementation of NCCS (NCCS Article 12 [41]), and issues reporting obligations (NCCS Article 27 [42], NCCS Article 39 [43]) along with non-binding performance indicators (NCCS Article 13 [44]). It also oversees the adoption process and implementation of terms, methodologies, and plans (NCCS Article 6 [45]). Furthermore, ACER develops a Union-wide cybersecurity crisis management and response plan for the electricity sector (NCCS Article 41 [46]).

4

ENISA (European Union Agency for Cybersecurity) The ENISA [47] is an EU agency that provides expertise and support in cybersecurity. Under the NCCS framework, ENISA consults ACER and ENTSO-E on cybersecurity risk assessment methodologies (NCCS Article 6 [48]), evaluates cybersecurity exercises (NCCS Article 43 [49]), and operates the European Cybersecurity Information Exchange and Analysis Center (ECEAC) (NCCS Article 42 [50]).

5

DG ENER (Directorate-General for Energy) The European Commission's Directorate-General for Energy [51] is responsible for the EU's energy policy.

6

DG CONNECT (Directorate-General for Communications Networks, Content and Technology) The European Commission's Directorate-General for Communications Networks, Content and Technology [52] is responsible for the EU's digital policies.

7

NEMOs Nominated Electricity Market Operators.

8

Regional Coordination Centers (RCCs) These centers have a consultative role in developing

[39] https://www.acer.europa.eu/
[40] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_8
[41] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_12
[42] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_27
[43] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_39
[44] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_13
[45] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_6
[46] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_41
[47] https://www.enisa.europa.eu/
[48] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_6
[49] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_43
[50] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_42
[51] https://commission.europa.eu/about/departments-and-executive-agencies/energy_en
[52] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/communications-networks-content-and-technology_en

regional cybersecurity risk assessment and risk mitigation plans and coordinate cybersecurity cooperation between Member States.

9

National Competent Authorities (NCAs) NCAs are responsible for implementing the NCCS in Member States. Their tasks include identifying high-impact and critical-impact entities (NCCS Article 24 [53]), approving conditions and methodologies (NCCS Article 6 [54]), granting exemptions from minimum and advanced cybersecurity controls (NCCS Article 30 [55]), conducting national cybersecurity risk assessments (NCCS Article 20 [56]), ensuring compliance and conducting audits (NCCS Article 25 [57]), and facilitating information sharing on cyberattacks.

10

National Regulatory Authorities (NRAs) NRAs are responsible for energy market regulation within Member States. Under the NCCS framework, NRAs determine mechanisms for cybersecurity investment cost recovery (NCCS Article 11 [58]) and conduct performance evaluations (NCCS Article 13 [59]).

11

Risk Preparedness National Competent Authorities (RP NCAs) RP NCAs are responsible for developing and implementing risk preparedness plans. Under the NCCS framework, RP-NCAs play a role in cybersecurity risk assessments and cyberattack management.

12

Cybersecurity Competent Authorities (CS NCAs) CS NCAs are responsible for developing and implementing national cybersecurity strategies.

13

Computer Security Incident Response Teams (CSIRTs) CSIRTs handle cybersecurity incidents. Under the NCCS framework, CSIRTs support high-impact and critical-impact entities in managing cyberattacks, share information on cyber threats, and participate in cybersecurity exercises.

[53] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_24
[54] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_6
[55] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_30
[56] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_20
[57] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_25
[58] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_11
[59] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_13

2.7.1 Key regulatory stakeholders

Member States play a key role in the implementation of NCCS. To ensure that the NCCS requirements are effectively enforced, each **Member State** designates a competent authority responsible for the regulation's implementation (NCCS Article 4 [60]).

National Competent Authority

Performs the following tasks:

- A national governmental or regulatory authority is **responsible** for carrying out the tasks assigned to it in the Regulation (ps://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=173 Article 4]).
- Designated by each member state for **six months** after entry into force of the Regulation (NCCS Article 4 Paragraph 1 [61]).
- **Shall coordinate and cooperate** with cybersecurity competent authorities, NRAs, RP NCAs, CSIRTs, and other authorities determined by each Member State to ensure the fulfillment of NCCS and avoid duplication of tasks (NCCS Article 5 [62]).
- **May delegate tasks** to other national authorities (NCCS Article 4 Paragraph 3 [63]).
- **Identify high-impact and critical-impact entities** (NCCS Article 24 Paragraph 2 [64]).
- **Approve the developed conditions and methodologies** (NCCS Article 6 Paragraph 2 [65]).
- **Conduct cybersecurity risk assessments** (NCCS Article 20 Paragraph 1 [66]).
- **Grant exemptions from minimum and advanced cybersecurity controls** (NCCS Article 30 Paragraph 1 [67]). m
- **May perform inspections** of critical-impact entities according to national law to verify their compliance with the NCCS (NCCS Article 25 [68]).

[60] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_4
[61] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[62] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_5
[63] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[64] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[65] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_6
[66] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_20
[67] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_30
[68] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_25

National Regulatory Authority

Performs the following tasks:

- **Implementing the NCCS** regulation in accordance with DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Article 59 Paragraph 1 e) point [69]
- **Evaluating costs** borne by Transmission System Operators (TSOs) and Distribution System Operators (DSOs) as specified in DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Article 11 [70]
- **Performing evaluation analysis** within 12 months after the development of the performance evaluation guidelines, as required by DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Article 13 Paragraph 2 [71]

---

[69] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944#art_59
[70] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944#art_11
[71] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944#art_13

Chapter 3

Temporary Provisions of the NCCS

In this chapter, you will learn about the most important temporary provisions of the NCCS.

The NCCS regulation's Article 48 [1] outlines temporary provisions that ensure the enhanced application of cybersecurity guidelines in the electricity sector until the final conditions and methodologies are developed and adopted.

Under the precautionary principle, **high-impact and critical-impact entities** may voluntarily comply with the obligations defined in the NCCS regulation during the **temporary period** (lasting until June 13, 2028, depending on the EU-wide adoption of relevant methodologies) before their final identification under NCCS Article 24 [2]. Furthermore, NCCS Article 48 Paragraph 10 [3] mandates that until the minimum and advanced cybersecurity controls under NCCS Article 29 [4] are adopted, all identified entities must strive to progressively implement the guidelines developed under NCCS Article 48 Paragraph 1 [5].

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48

Topic	Developed by	Timeline
Development of provisional ECII values (NCCS Article 48 Paragraph 2 [6]) The provisional ECII assists competent authorities in identifying high-impact and critical-impact entities.	ENTSO-E, EU DSO	October 13, 2024
Compilation of the list of high-impact and critical-impact processes (NCCS Article 48 Paragraph 4 [7]) In addition to the provisional ECII, these processes provide further guidance to competent authorities for identifying entities.	ENTSO-E, EU DSO	December 13, 2024
Compilation of the provisional list of high-impact and critical-impact entities and notification of entities (NCCS Article 48 Paragraph 3 [8])	Competent authority	Identification of designated entities: February 13, 2025 Notification of designated entities: March 13, 2025
Development of a **provisional list of European and international standards and controls** required by national regulations relevant to the cybersecurity aspects of cross-border electricity flows (NCCS Article 48 [9])	ENTSO-E, EU DSO	June 13, 2025

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:

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48

FILE 1

Provisional list of Union-wide high-impact and critical-impact processes

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

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)

files/Provisional ECII.pdf

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

FILE 4

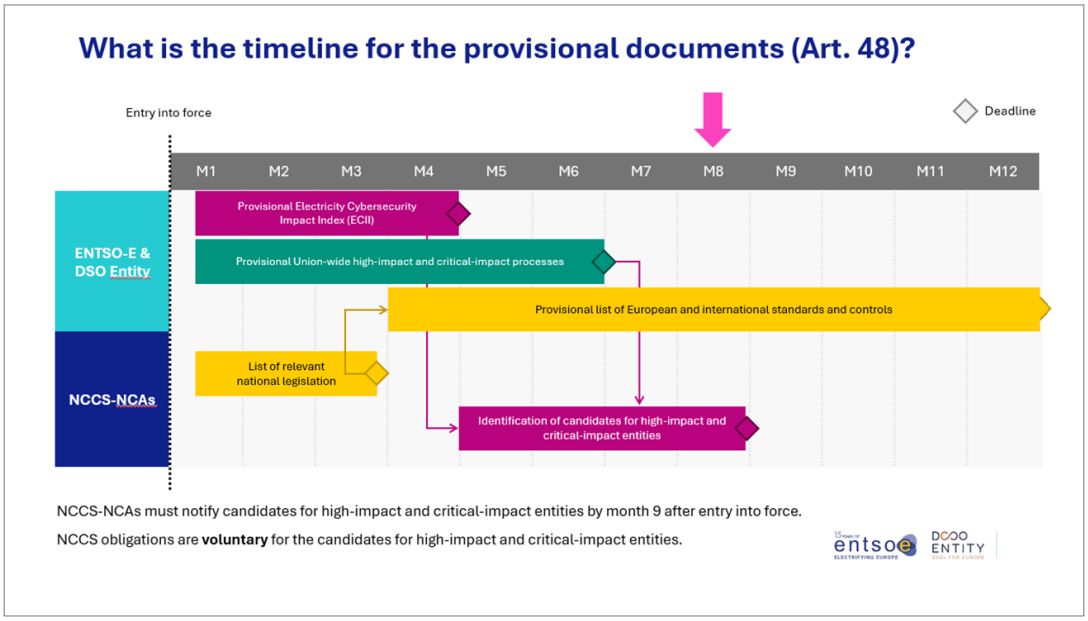
Supporting document for the provisional Electricity Cybersecurity Impact Index (ECII)

files/Supporting document provisional ECII.pdf

GOOD TO KNOW

- Competent authorities will notify the entities identified in the provisional list **no later than March 13, 2025**, informing them that they have been designated as high-impact or critical-impact entities.
- Entities identified in the provisional list as high-impact and critical-impact may voluntarily comply with the obligations outlined in this regulation under the precautionary principle.

Here you can see the provisional time line:



Unresolved directive in main_01.adoc - include::03_nccs_nis2_02.adoc[]

Chapter 4

Cybersecurity Framework

The purpose of this chapter is to present the fundamentals of the common cybersecurity framework for the electricity sector.

You will learn about the significance of minimum and advanced controls, the mapping matrix, critical impact perimeters, high impact perimeters and the cybersecurity management system of the framework.

4.1 Common electricity cybersecurity framework

NOTE

The subtitles of the video were generated using AI tools, so errors may be present.

The NCCS regulation (NCCS Article 28 [1]) establishes a common cybersecurity framework for the electricity sector, aiming to effectively manage cybersecurity risks across the entire European Union. The framework's objective is to harmonize the cybersecurity requirements and practices of mmember states within the electricity sector.

The cybersecurity framework consists of several components:

- Minimum and advanced cybersecurity controls developed according to NCCS Article 29 [2] and NCCS Article 33 [3]. m
- The Mapping matrix established in NCCS Article 34 [4].
- The cybersecurity management system defined in NCCS Article 32 [5].

The following chapters describe these topics and the concept of scope in more detail.

4.2 Minimum and advanced cybersecurity controls

Article NCCS 29 [6]

According to NCCS Article 29 Paragraph 1 [7], within 7 months of the submission of the first draft of the EU-wide cybersecurity risk assessment report, **transmission system operators**, assisted by the ENTSO for Electricity and in cooperation with the EU DSO, **shall develop** a proposal for **minimum and advanced cybersecurity controls**.

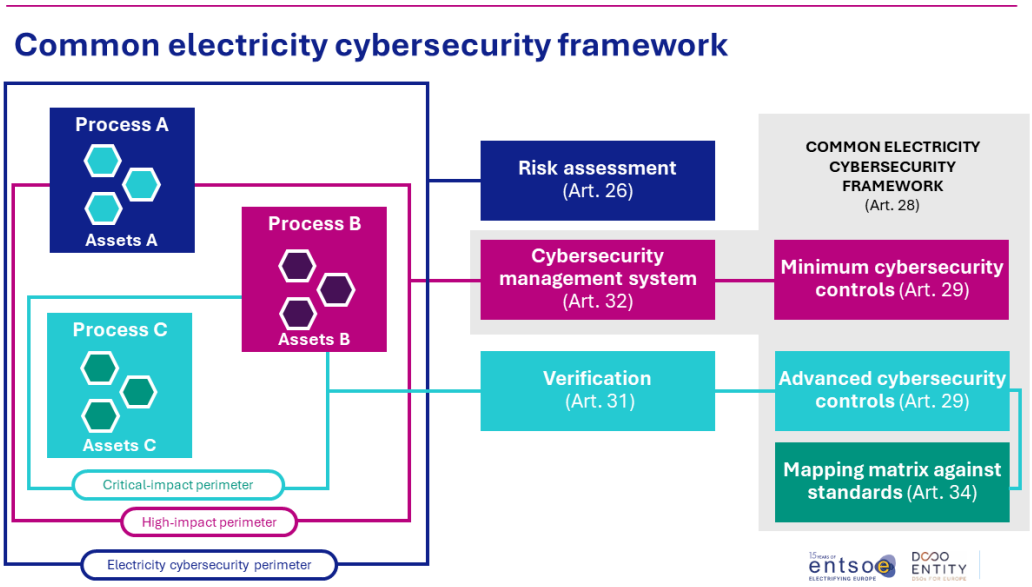
The minimum and advanced cybersecurity controls may be audited in accordance with the procedure set out in NCCS Article 31 [8] on the basis of participation in the national compliance audit scheme or by conducting security audits by an independent third party in accordance with the requirements listed in NCCS Article 25 Paragraph 2 [9].

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_34
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_31
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_25

The baseline minimum and advanced cybersecurity controls developed pursuant to NCCS Article 29 Paragraph 1 [10] shall be based on the risks identified in the EU-wide cybersecurity risk assessment report referred to in NCCS Article 19 Paragraph 5 [11] Modified minimum and advanced cybersecurity controls developed pursuant to NCCS Article 29 Paragraph 2 [12] shall be based on the regional cybersecurity risk assessment report referred to NCCS Article 21 Paragraph 2 [13].

Minimum cybersecurity controls include controls to protect information shared under NCCS Article 46 [14].

Transmission System Operators (TSOs), together with ENTSO-E and the EU DSO, shall develop **minimum and advanced cyber security control proposals** for the supply chain (NCCS Article 33 [15]) in accordance with the minimum and advanced controls (NCCS Article 29 [16]).



4

3

1

Minimum and advanced cybersecurity controls

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_19
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_21
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_46
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_33
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_29

Critical and high-impact entities will apply the minimum cybersecurity controls within the high-impact scope, while critical-impact entities will apply the advanced cybersecurity controls within the critical-impact scope.

2

Mapping matrix The controls defined in points (a) and (b) of (NCCS Article 28 Paragraph 1 [17]) serve as a matrix for ensuring compliance with selected European and international standards, as well as relevant technical specifications, including the applicable national standards under (European Parliament and Council Directive (EU) 2022/2555 Article 5 [18]).

3

Cybersecurity Management System This system prescribes a comprehensive approach to managing cybersecurity at the entity level. The system includes, for example, the development of cybersecurity policies, the assignment of responsibilities, the conduct of risk assessments, and the provision of necessary resources. Its core components are designed to ensure that the entity can proactively manage cybersecurity risks, establish clear roles and responsibilities, and allocate the resources needed to protect against potential threats and vulnerabilities. This system serves as a foundational framework for the ongoing protection and resilience of organizational assets in the face of evolving cyber threats.

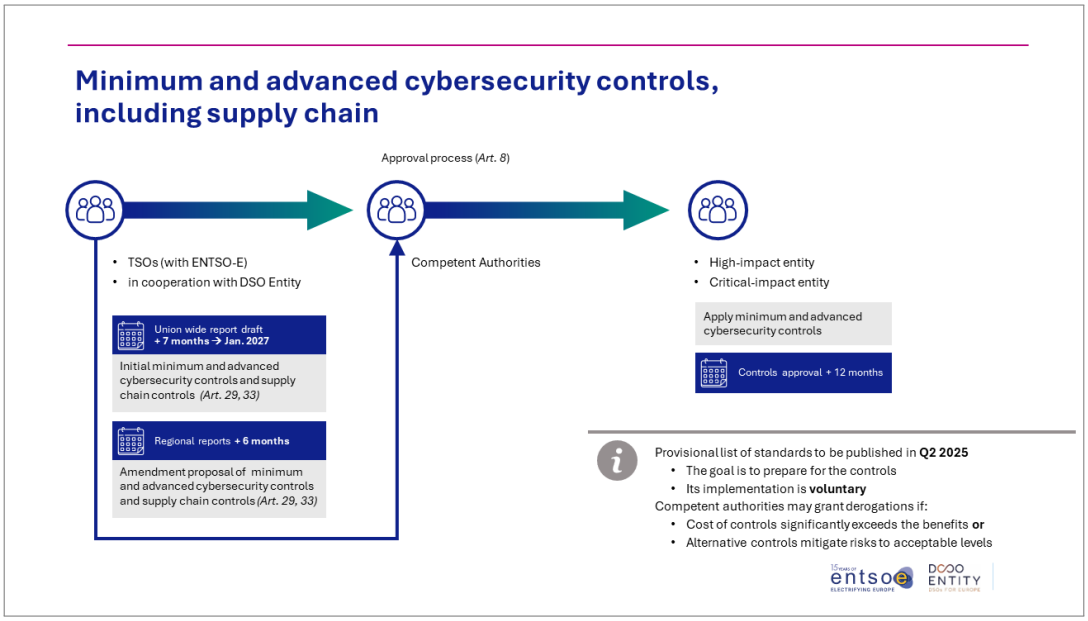
4

Risk Assessment According to Article 26 of the NCCS (NCCS Article 26 [19]), risk assessment is a structured process aimed at protecting the organization's network and information systems. Every high-impact and critical-impact entities is required to conduct a risk assessment every three years. This process ensures that entities continuously evaluate the security posture of their systems, identify potential threats and vulnerabilities, and implement appropriate risk mitigation measures. It is an essential practice for maintaining the integrity and resilience of critical infrastructure in the face of evolving cybersecurity challenges.

GOOD TO KNOW

A provisional list of European and international standards and controls will be published **until 13 June 2025**. Implementation will be on a **voluntary basis** and may prepare entities to implement minimum and advanced controls. **Critical and high-impact entities will apply minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical perimeter.**

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555#art_25
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26



GOOD TO KNOW

Entities may request the competent authority to allow an exemption from the obligation to apply minimum and advanced cybersecurity controls.

The competent authority may grant such an exemption if the entity:

- Can prove that the costs of implementing the appropriate cybersecurity controls significantly outweigh the benefits; or
- Submits an enterprise-level risk assessment plan that reduces cybersecurity risks to an acceptable level using alternative control measures, in accordance with the risk acceptance criteria. The competent authority then has three months to decide whether the exemption from the minimum and advanced cybersecurity controls can be granted.

Exemptions will be granted for a period of up to three years, with the possibility of extension.

4.3 Mapping matrix

NCCS Article 34 [20]

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_34

Mapping matrix for electricity cybersecurity controls and standards

Within 7 months of the submission of the first draft of the EU-wide cybersecurity risk assessment report under NCCS Article 19 paragraph 4 [21], **TSOs**, with the assistance of the ENTSO for Electricity and in cooperation with the EU DSO and in consultation with ENISA, **shall develop a proposal** for the development of a cybersecurity risk assessment report for the EU-wide cybersecurity risk assessment report under NCCS Article 28 Paragraph 4 [22] The ENTSO for Electricity and the EU DSO shall document the equivalence of the different controls and the controls defined in NCCS Article 28 Article 1 [23] (a) and (b) with the selected European and international standards and relevant technical specifications (mapping matrix).

If such a mapping is provided by a competent authority of a Member State, the ENTSO for Electricity and the EU DSO shall integrate this national mapping into the mapping matrix.

4.4 Cyber Security Management System

NCCS Article 32 [24]

Within 24 months of being notified by the competent authority that they have been identified as a high impact or critical impact entity in accordance with NCCS Article 24 Paragraph 6 [25], each entity shall, in accordance with NCCS Article 32 Paragraph 1 [26]

(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 NCCS Article 26 [27];

(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;

[21] https://eur-lex.europa.eu/legal-content/ENTXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_19
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[24] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

(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.

GOOD TO KNOW

Within 24 months of **identification**, all high impact and critical impact entities **shall establish a cyber security management system** and **shall review this system every three years** thereafter. According to NCCS Article 32 Paragraph 2 [a], the scope of the cybersecurity management system shall include all assets within the high impact and critical impact scope of the high impact and critical impact entity.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32

4.5 Perimeters

12 months after the approval of the minimum and advanced cybersecurity controls under NCCS Article 8 Paragraph 5 [28] or their update under NCCS Article 8 Paragraph 10 [29], the organizations listed in NCCS Article 2 Paragraph 1 [30] of the NCCS and identified as critical impact or high impact entities under NCCS Article 24 [31] of the NCCS shall, in accordance with NCCS Article 26 Paragraph 5 [32] of the NCCS, apply minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter when developing their entity-level risk mitigation plan.

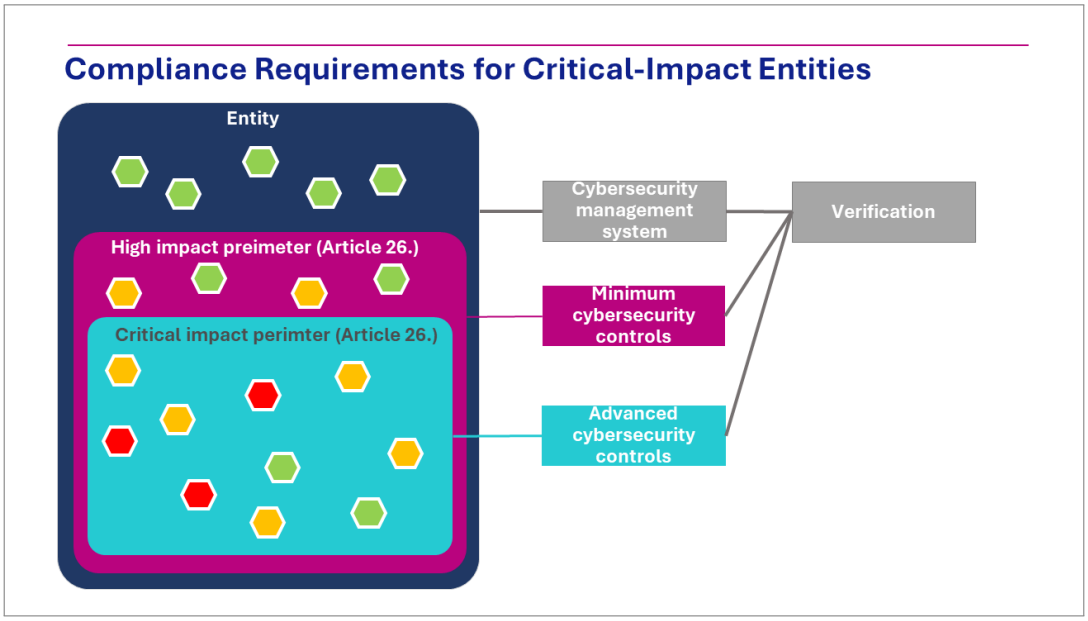
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[30] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art26

Compliance Requirements for Critical-Impact Entities

GOOD TO KNOW

Critical impact perimeter

The physical and/or logical segregation defined by the entity (e.g., fencing, server rooms, firewalls, proxy servers, etc.), which includes all **high-impact and critical-impact devices**, as well as any other devices that are within this segregation.



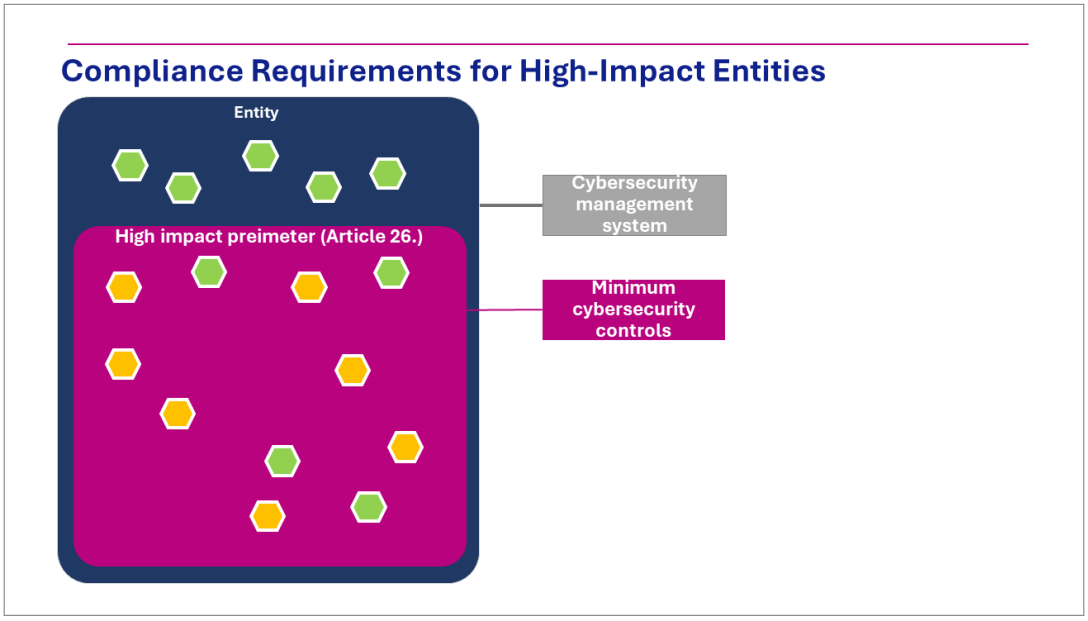
Compliance Requirements for High-Impact Entities

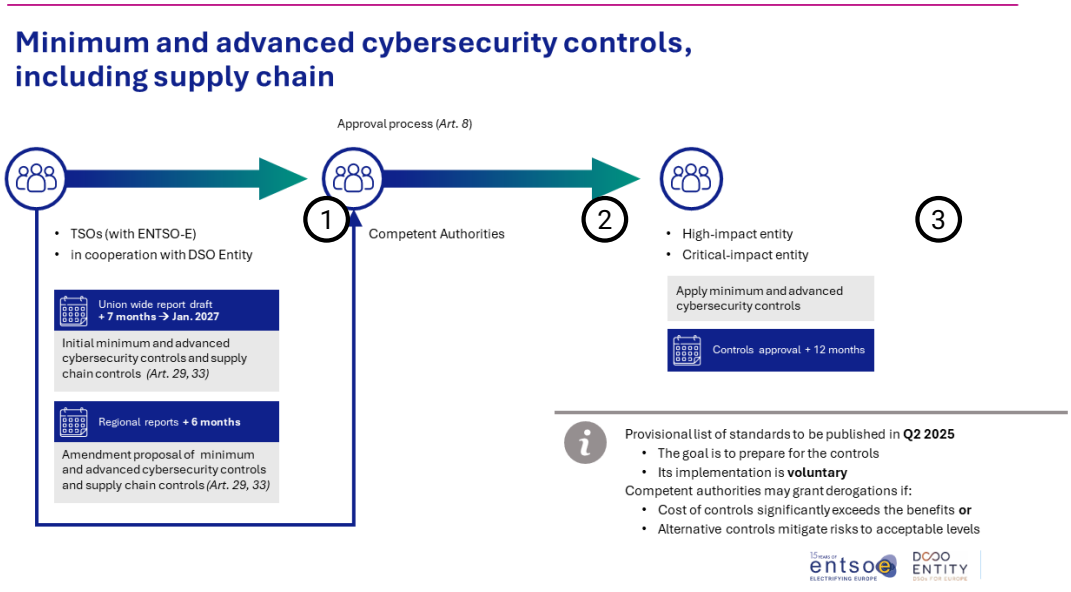
GOOD TO KNOW

High impact perimeter

The physical and/or logical segregation defined by the entities (e.g., fencing, server rooms, firewalls, proxy servers, etc.), which includes all **high-impact devices** and any other devices

that are within this segregation.





1

The transmission system operators (TSOs), with the assistance of ENTSO-E and the DSO Entity, will develop a proposal for the minimum and advanced cybersecurity controls.

2

The competent authorities will then have six months to make a decision on the minimum and advanced cybersecurity controls based on the proposal.

3

Subsequently, in January 2028, critical-impact and high-impact entities will apply the minimum cybersecurity controls within the high-impact perimeter, and the advanced cybersecurity controls within the critical-impact perimeter.

Chapter 5

National verification schemes

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.

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;tion 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.

Chapter 6

Risk assessment according to the NCCS regulation

The aim of this chapter is to present the risk assessment process according to the NCCS regulation.

Risk assessment is a cornerstone of the NCCS; the **risk assessment is conducted cyclically at the EU, regional, member state, and entity levels**. The regulation mandates the development and application of risk assessment methodologies at the EU and regional levels. Risk assessments must take into account potential cyber threats, vulnerabilities, and the possible impacts of cyberattacks.

6.1 Cybersecurity Risk Assessment Cycle

NOTE

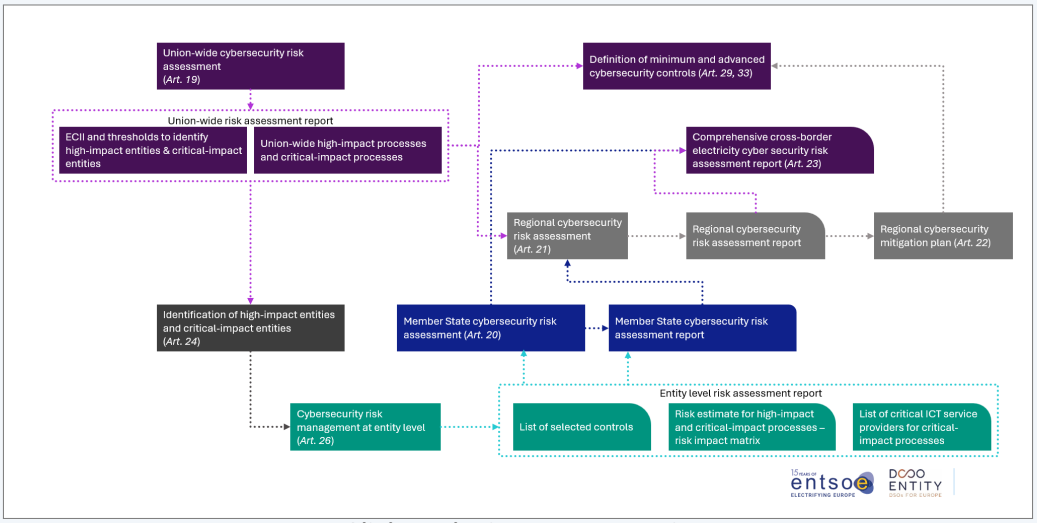
The subtitles of the video were generated using AI tools, so errors may be present.

The NCCS regulation prescribes a **structured process** for the identification and evaluation of cybersecurity risks in the European electricity sector. **Risk assessment** is the central element of this process and **occurs cyclically at multiple levels** (EU level, regional level, member state level, entity level).

GOOD TO KNOW

The goal of the **risk assessment is to identify cybersecurity risks threatening cross-border electricity flows at multiple levels (EU level, regional level, member state level, entity level)**.

The cycle includes the following levels and steps:



Click on the image to zoom in

6.2 Cybersecurity Risk Assessment Methods

The NCCS Article 18 [1] addresses the methodology for cybersecurity risk assessment.

Timeline	Levels
The cybersecurity risk assessment process will begin in March 2025, when ENTSO-E and the EU DSO entities, in consultation with the NIS Cooperation Group, will develop the assessment methodologies.	* Union * Regional * Member state

Risk assessment methodology

The cybersecurity risk assessment methodologies at the EU, regional, and member state levels include the following:

a) The list of cyber threats to be examined, including at least the following threats affecting the supply chain:

- severe and unexpected disruption of the supply chain
- absence of ICT products, ICT services or ICT processes in the supply chain.
- Cyberattacks initiated through supply chain participants;
- leaking sensitive information through the supply chain, including tracking of the supply chain;
- the introduction of vulnerabilities or backdoors into ICT products, ICT services, or ICT processes through supply chain actors.

b) Criteria for assessing the high or critical impact of cybersecurity risks, using the defined thresholds for consequences and probability;

c) An approach for analyzing cybersecurity risks arising from legacy, the cascading effects of cyberattacks, and the real-time nature of the systems operating the network.

d) an approach for analyzing cybersecurity risks arising from dependency on a single supplier of ICT products, ICT services, or ICT processes.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18

Risk impact matrix

NCCS Article 18 Paragraph 2 [2]

(a) measure the **consequences of cyber-attacks** based on the following criteria:

(i) loss of load;

(ii) reduction of power generation;

(iii) loss of capacity in the primary frequency reserve;

(iv) 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');

(v) the expected duration of an electricity outage affecting customers in combination with the scale of the outage in customer numbers; and

(vi) 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.

GOOD TO KNOW

The EU, regional, and member state cybersecurity risk assessment methodologies evaluate cybersecurity risks using the same risk impact matrix.

6.3 Entity-level cybersecurity risk assessment

NCCS Article 26 [3] and NCCS Article 27 [4] outline the details of entity-level cybersecurity risk assessment and management.

According to NCCS Article 26 Paragraph [5], during the cybersecurity risk management phase, each high-impact and critical-impact entity must develop an entity-level risk reduction plan for all

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_27
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

assets within the high-impact and critical-impact perimeter and must conduct a risk assessment every three years.

The entity analyzes the likelihood and consequences of identified cybersecurity risks and determines the cybersecurity risk level using the risk impact matrix, which is developed by transmission system operators (TSOs) in collaboration with ENTSO-E for the electricity market and the EU DSO, in accordance with NCCS Article 19 Paragraph 2 [6], integrating EU, regional, and member state cybersecurity risk assessment methodologies.

According to NCCS Article 26 Paragraph 2 [7], each high-impact and critical-impact entity must base its cybersecurity risk management on an approach aimed at protecting its network and information systems, consisting of the following phases:

a) Establishing the context;

b) Conducting cybersecurity risk assessment at the entity level;

c) Managing cybersecurity risks;

d) Accepting cybersecurity risks.

Timeline	Levels
* **Identification of high and critical-impact entities + 12 months.** * **Every 3 years**	* Critical impact entity * High impact entity

The steps of the procedure are as follows:

1. Defining the scope, taking into account high-impact processes, critical-impact processes, or other processes.
2. Defining the risk assessment and acceptance criteria (risk impact matrix).
3. Identification of cybersecurity risks,cyber threats, vulnerabilities, cyberattack scenarios, considering EU-level risk assessments.
4. Analysis of the probability and consequences of cybersecurity risks using the risk impact matrix.
5. Classification of assets based on the consequences of potential compromise, as well as the determination of high and critical impact scopes using ECII.
6. Evaluation of cybersecurity risks by ranking them.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_19
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

7. Development of an entity-level risk mitigation plan.
8. Deciding whether the residual risk is acceptable based on the risk acceptance criteria.
9. Maintaining an inventory of assets for all assets within the high-impact and critical-impact perimeter. This asset inventory is not part of the risk assessment report.

Results

Entity-level cybersecurity risk assessment reports:

Entity-Level Cybersecurity Risk Assessment Report According to NCCS Article 27 [8]m. Every high-impact and critical-impact entities must submit a report to the competent authority within 12 months of identification as a high-impact or critical-impact entity, and subsequently every three years.

The report must include the following information:

- A **list of selected controls** from the entity-level risk mitigation plan, as required by NCCS Article 26 Paragraph 5 [9], along with the current implementation status of each control.
- **Risk estimation** related to the compromise of the confidentiality, integrity, and availability of information and relevant assets for each EU-level, high-impact, or critical-impact process. This risk estimation must follow the risk impact matrix specified in NCCS Article 19 Paragraph 2 [10] .
- A list of critical ICT service providers that are essential for their critical-impact processes.

GOOD TO KNOW

- After identifying high and critical-impact entities, an entity-level risk assessment must be conducted within 12 months, and it should be repeated every 3 years.

[8]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_27
[9]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[10]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_19

6.4 Member state-level cybersecurity risk assessment

NCCS Article 20 [11]

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 NCCS Article 18 [12] and approved pursuant to NCCS Article 8 [13]. **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.

Within 21 months after the notification of the high-and critical-impact entities pursuant to NCCS Article 24 Paragraph 6 [14] 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 NCCS Article 29 [15];

(b) a list of all cyber-attacks reported in the previous three years pursuant to NCCS Article 38 Paragraph 3 [16];

(c) a summary of the cyber threat information reported in the previous three years pursuant to NCCS Article 38 Paragraph 6 [17];

(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 NCCS Article 24 Paragraph 2,3,5 [18].

The Member State cybersecurity risk assessment report shall take into account the Member State's risk preparedness plan established pursuant to REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Article 10 [19].

The information contained in the Member State cybersecurity risk assessment report 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

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_20
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941#art_10

authorities in the Member States pursuant to NCCS Article 30 [20].

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_30

Chapter 7

Supply chain

Recent cyberattacks show that entities are increasingly becoming targets of attacks against supply chains. Such attacks not only affect individual entities covered by this regulation but can also have a ripple effect, leading to larger-scale attacks on entities connected through the electricity grid.

The purpose of this chapter is to present the sections of the NCCS regulation that address the **minimum and advanced cybersecurity controls related to supply chains**, as well as non-binding **cybersecurity procurement recommendations**.

7.1 Overview of Supply Chain Cybersecurity

NOTE

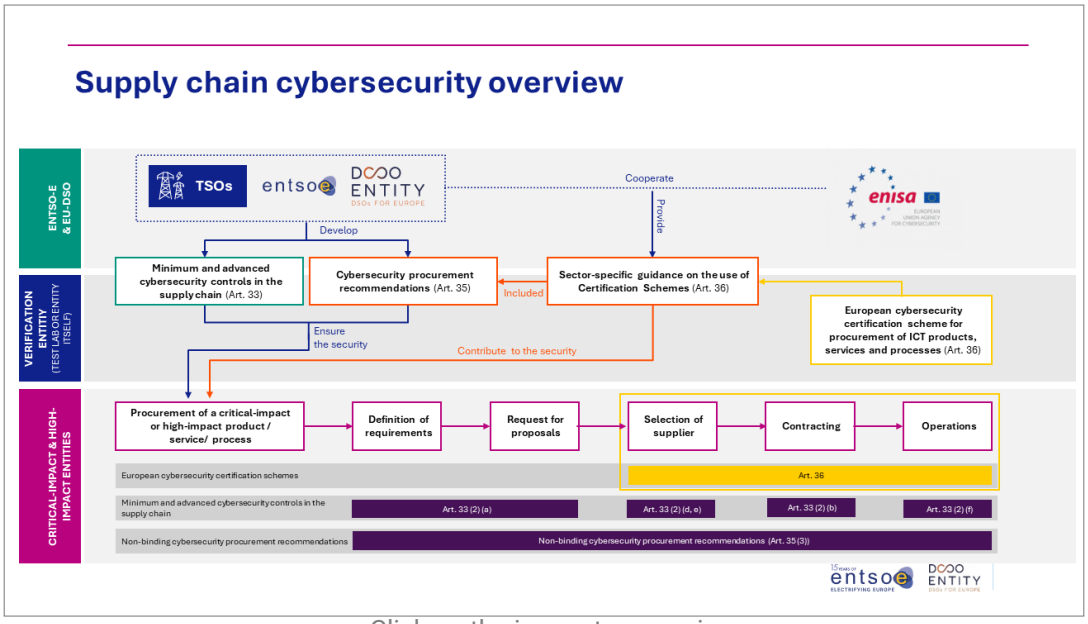
The subtitles of the video were generated using AI tools, so errors may be present.

7.2 Minimum and Advanced Cybersecurity Controls and Recommendations in the Supply Chain

Transmission system operators (TSOs), in collaboration with ENTSO-E and the EU DSO, are developing minimum and advanced cybersecurity control recommendations for the supply chain (NCCS Article 33 [1]) in accordance with the minimum and advanced controls (NCCS Article 29 [2]), as well as non-mandatory cybersecurity procurement recommendations (NCCS Article 35 [3]). These recommendations can be utilized by high and critical impact entities when procuring ICT products, ICT services, and ICT processes identified within the high and critical perimeters.

Non-binding cybersecurity procurement recommendations may include sector-specific guidance on the use of European cybersecurity certification schemes, provided that an appropriate scheme is available for the ICT products, ICT services, or ICT processes used by critical-impact entities. Transmission system operators (TSOs), ENTSO-E, the EU DSO, and ENISA collaborate in the development of such guidelines (NCCS Article 36 [4]).

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_33
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_29
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_35
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_36



Click on the image to zoom in

GOOD TO KNOW

Suppliers within the supply chain that entities identify as high-impact or critical-impact ICT service providers are classified as critical ICT service providers (NCCS Article 3 Paragraph [a]).

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_3

7.3 Minimum and Advanced Cybersecurity Controls in the Supply Chain

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 and high-impact entities pursuant to NCCS Article 24 [5] that starts six months after the adoption or update of the minimum and advanced cybersecurity controls referred to in NCCS Article 29 [6] (NCCS Article 33 Paragraph 5 [7]).

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33

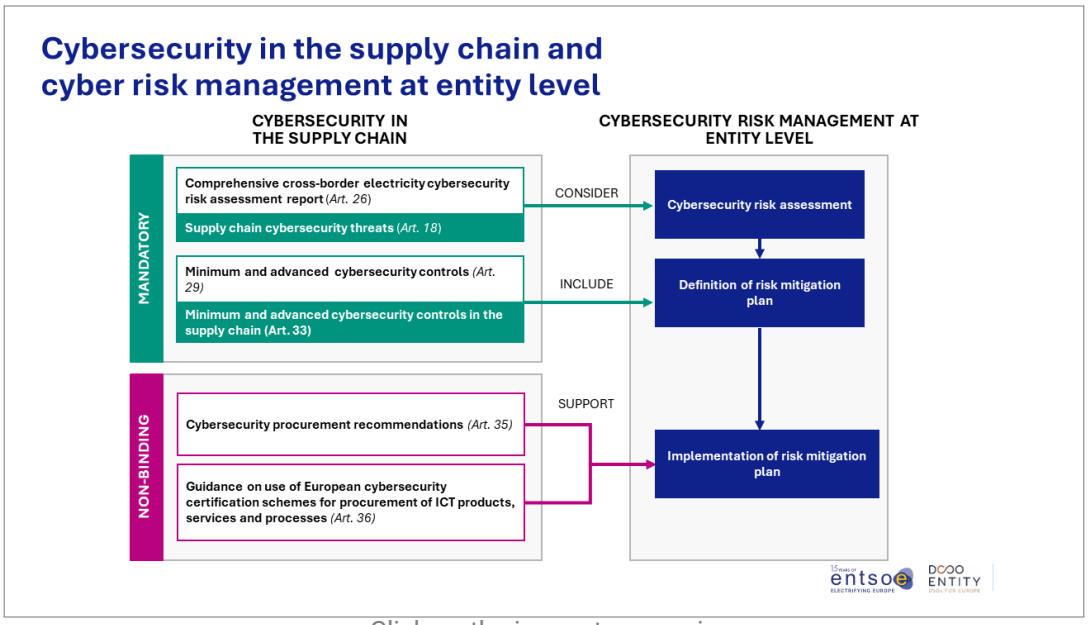
Within six months of the completion of the regional cybersecurity risk assessment reports, as required by (NCCS Article 21 Paragraph 2 [8]), transmission system operators (TSOs), in collaboration with ENTSO-E for the electricity market and the EU DSO, will propose modifications to the supply chain's minimum and advanced cybersecurity controls to the competent authority.

This proposal will be prepared in accordance with NCCS Article 8 Paragraph 10 [9] and will consider the risks identified in the regional risk assessment that affect the procurement processes of entities identified as critical-impact and high-impact under NCCS Article 24 [10] (NCCS Article 33 Paragraph 6 [11]).

During the cybersecurity **risk management phase**, each high and critical entity must establish an entity-wide risk mitigation plan for all assets within their high-impact and critical-impact perimeters and conduct a risk assessment every three years (NCCS Article 26 [12]).

During the cybersecurity **risk assessment phase**, each high-impact and critical-impact entity must **identify potential cybersecurity risks**:

- the **cyber threats** identified in the latest comprehensive cybersecurity risk assessment report on the cross-border electricity sector (NCCS Article 23 [13]);
- **potential supply chain threats** (NCCS Article 18 [14])



Click on the image to zoom in

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_21
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_23
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18

7.4 Minimum and Advanced Controls in the Supply Chain

The minimum controls in the supply chain should include the following according to

NCCS Article 33 Paragraph 1 [15]:

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 [16] and Directive (EU) 2016/680 of the European Parliament and of the Council Article 18 [17]. 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

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[17] https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

(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 supply chains carried out in accordance with Article 22(1) of DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [18];

d) include criteria to select and contract suppliers that can meet the cybersecurity specifications as stated in paragraph (a) and that possess a level of cybersecurity appropriate to the cybersecurity risks of the ICT product, ICT service, or ICT processes that the supplier delivers;

e) include criteria to diversify sources of supply for ICT products, ICT services and ICT processes and reduce the risk of a vendor lock-in;

f) include criteria to monitor, review or audit the cybersecurity specifications for supplier internal operational processes throughout the entire lifecycle of each ICT product, ICT service and ICT process on a regular basis.

The advanced controls of the supply chain

The advanced supply chain controls include the following, as outlined in NCCS Article 33 Paragraph 4 [19]:

During procurement, advanced cybersecurity controls in the supply chain encompass those controls applicable to critical impact organizations, ensuring that ICT products, ICT services, and ICT processes used as critical assets comply with cybersecurity requirements. The ICT product, ICT service, or ICT process must be certified through the European cybersecurity certification scheme mentioned in NCCS Article 36 [20] or verified through an audit procedure selected and conducted by the entity.

The level of detail and scope of verification activities ensure that the ICT product, ICT service, or ICT process can be used to mitigate risks identified in the entity's risk assessment. The critical impact entity documents include the steps taken to reduce the identified risks.

7.5 Procurement recommendations in the supply chain

Procurement recommendations

Content of procurement recommendations for high-impact and critical-impact entities according to

[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=OJ:L_202401366&qid=1730714105315#art_33
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_36

NCCS Article 35 Article 1 [21]

a) The description and classification of the types of ICT products, ICT services, and ICT processes used by high impact and critical impact entities within the high and critical perimeters.

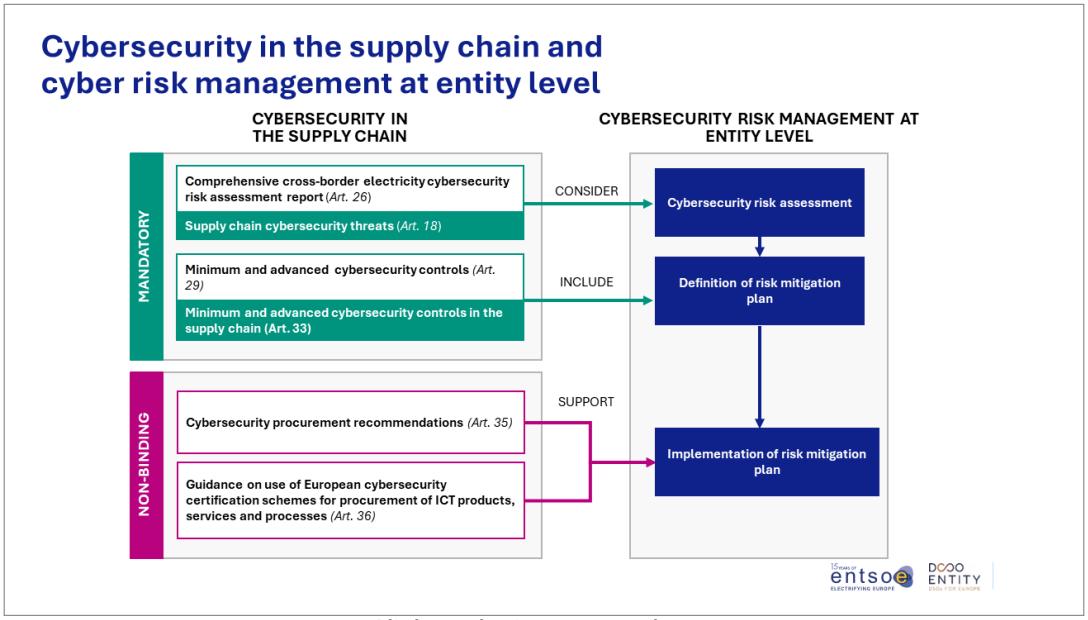
b) A list of types of ICT products, ICT services, and ICT processes for which non-binding cybersecurity-related recommendations are developed, based on the respective regional cybersecurity risk assessment reports and the priorities of high-impact and critical-impact entities.

7.6 Risk Management in the Supply Chain

During the cybersecurity risk management phase, every high-impact and critical-impact entity must establish an entity-wide risk mitigation plan for all assets within their high-impact and critical-impact perimeter and conduct a risk assessment every three years (NCCS Article 26 [22]).

During the cybersecurity risk assessment phase, all high-impact and critical-impact entities must identify potential cybersecurity risks, including:

- Cyber threats identified in the most recent comprehensive cybersecurity risk assessment report for the cross-border electricity sector (NCCS Article 23 [23]).
- Potential supply chain threats (NCCS Article 18 [24]).



Click on the image to enlarge.

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_35
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_23
[24] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18

Chapter 8

Cybersecurity information management

This chapter presents how the NCCS regulation governs the management of cyber attack, vulnerabilities, and threats.

Simultaneous cyberattacks may potentially cause a electricity supply crisis, thereby affecting cross-border electricity flows. Such a security event could also impact other sectors dependent on the security of electricity supply.

8.1 The cybersecurity defense capabilities of high-impact and critical-impact entities

NOTE

The subtitles of the video were generated using AI tools, so errors may be present.

The NCCS regulation provides detailed regulations on responding to cyberattacks in the electricity sector.

- Establish **CSOC** capabilities and designate a **Single point of contact** (NCCS Article 28 Paragraph 1 [1]).
- Develop capabilities to **handle detected cyber-attacks** with support from CSIRTs (NCCS Article 39 Paragraph 1 [2]).
- Implement effective processes to **identify, classify and respond to cyber-attacks that may affect cross-border electricity flows** (NCCS Article 39 Paragraph 1 [3]).
- **Cooperate among affected high-impact and critical-impact entities** to share information about cyber-attacks with effect on cross-border electricity flows (NCCS Article 39 Paragraph 2 [4]).
- Designate a **Single Point of Contact (SPOC)** and ensure they have access on a need-to-know basis to the information about cyber-attacks they received from the NCCS-NCA (NCCS Article 39 Paragraph 3 [5]).
- Establish **cyber-attack management procedures** (NCCS Article 39 Paragraph 3 [6]).
- **Test the overall cyber-attack management procedures** at least every year (NCCS Article 39 Paragraph 3 [7]).
- Have capabilities to take part in the detection and mitigation of cross-border risk (NCCS Article 40 Paragraph 4 [8]).
- **Investigate the root cause** of cross-border electricity crisis - when impacted (NCCS Article 40 Paragraph 4 [9]).

[1] https://eur-lex.europa.meu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_40
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_40

- Develop and test crisis management plans and **business continuity plans** (NCCS Article 41 [10]).
- By December 31 of the year following the designation of critical impact entities, and every three years thereafter, each **critical impact entity conducts a cybersecurity exercise** (NCCS Article 43 [11]).

GOOD TO KNOW

Entities must establish CSOC capability (even in an Managed service provider way), designate a Single point of contact, develop cyberattack management procedures that must be tested at least annually, and ensure that critical impact entity participate in cybersecurity exercises at least every three years.

8.2 Reporting of Cyberattacks

The following section presents the process of reporting a cyberattack.

TERM

Cyberattack

A security incident as defined in Article 3, Paragraph 14 of REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

A malicious ICT-related incident in which a threat actor attempts to destroy, disclose, modify, disable, steal, gain unauthorized access to, or make unauthorized use of an asset.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554

TERM

The Reportable Cyberattack

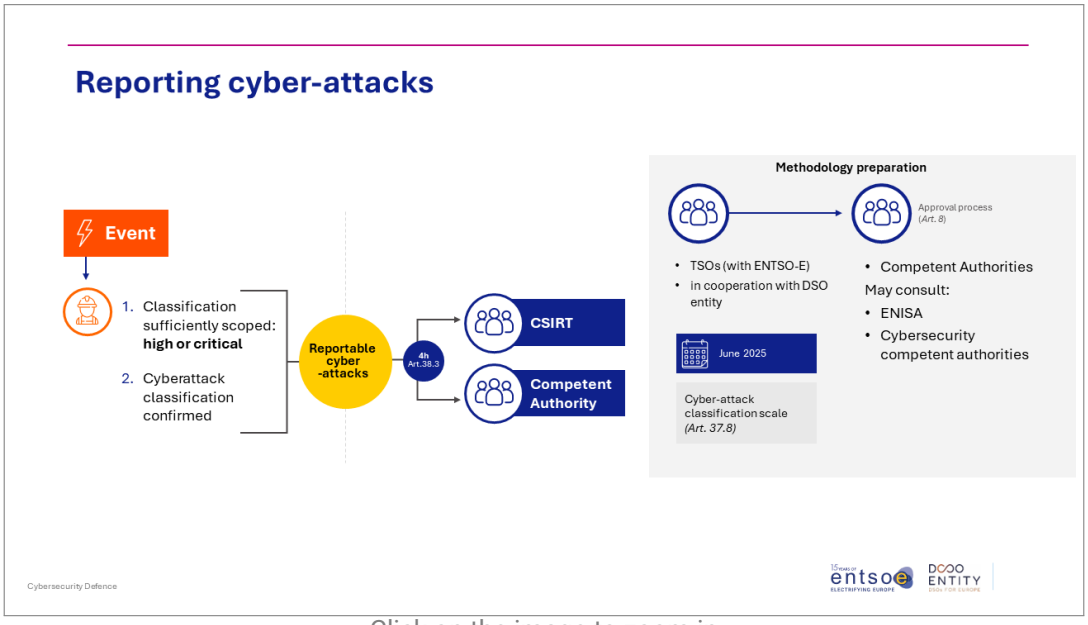
Every critical-impact and high-impact organization must, without undue delay but **no later**

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_41
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_43

than four hours after becoming aware that a cyber attack is reportable, share relevant information regarding the reportable cyber attack with its CSIRTs and competent authority, as per (NCCS Article 38 Paragraph 2 [a]).

According to (NCCS Article 38 Paragraph 3 [b]), information related to a cyber attack is considered reportable if the affected organization's assessment determines that, based on the classification scale outlined in (NCCS Article 37 Paragraph 8 [c]), the attack's **severity ranges from "high" to "critical."** The classification of security incidents is communicated by the single organizational point of contact designated under paragraph 1(c).

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[b] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[c] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37



Click on the image to zoom in

GOOD TO KNOW

Classification of Events

Transmission system operators, with the assistance of the electricity market ENTSO-E and in cooperation with EU DSO, shall develop a methodology for the classification scale of cyberattacks by June 13, 2025 (NCCS Article 37 [a]).

The methodology categorizes the severity of cyberattacks into five levels, with the two highest levels being "high" and "critical". The classification is based on the evaluation of the following parameters:

- the potential impact, considering the exposed assets and scopes identified in accordance with point (c) NCCS Article 26 Paragraph 4 [b]; and
- the severity of a cyberattack

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37
[b] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

GOOD TO KNOW

Cyberattacks that an organization classifies as malicious, which may have a significant impact on cross-border electricity flows, and are already in an advanced stage within the attack chain ("high" or "critical" classification), must be reported to the CSIRT and the competent authority within 4 hours.

8.2.1 Reporting cyber-attack

If a competent authority receives information related to a reportable cyber-attack, that competent authority (NCCS Article 37 Paragraph 1 [12]):

(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;

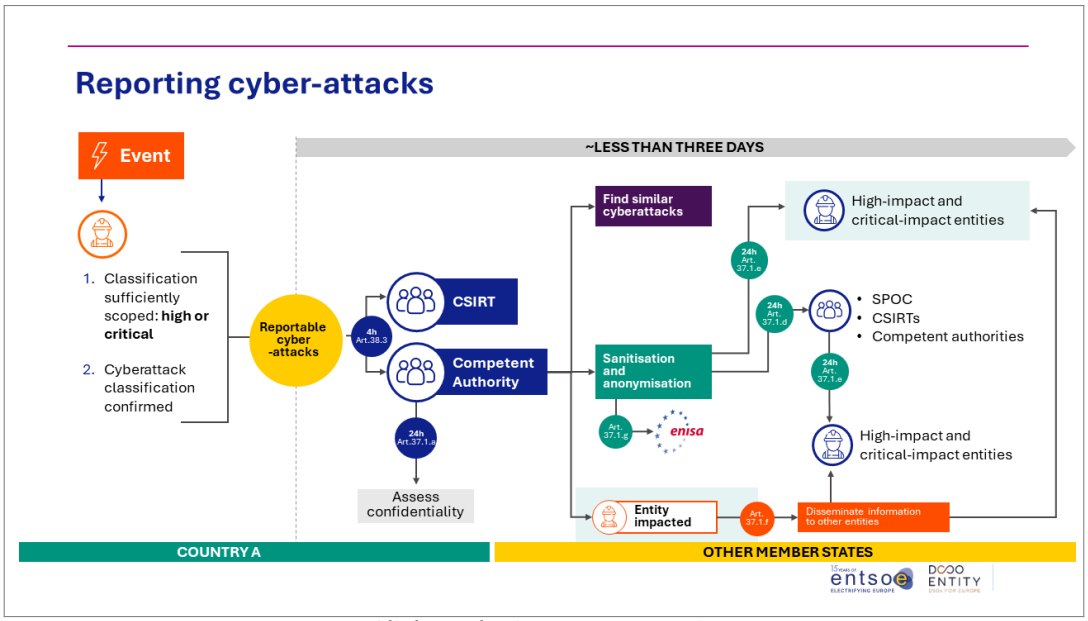
(d) shall share the information with the national single points of contact, CSIRTs and all competent authorities designated pursuant to Article 4 in other Member States without undue delay and no later than 24 hours after the reception of a reportable cyber-attack and provide updated information on a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

[12] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37

(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.



Click on the image to zoom in

8.3 Reporting unpatched actively exploited vulnerabilities

TERM

Unpatched, actively exploited vulnerability

A vulnerability as defined in Article 6, point 15 of Directive DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a] 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.

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

Unpatched, actively exploited vulnerabilities must be reported to the CSIRT, which provides sup-

port. According to NCCS Article 38 Paragraph 4 [13], if critical and high impact organisations report relevant information on uncorrected vulnerabilities that have been actively exploited to CSIRT, the latter may forward this information to the competent authority. In view of the sensitivity of the information reported, the CSIRT may withhold or delay the transmission of the information for legitimate cyber security reasons. Unpatched, actively exploited vulnerabilities that are actively exploited should be reported to the CSIRT, which will provide support.

If an unpatched, actively exploited vulnerability is reported to **CSIRT** according to NCCS Article 37 Paragraph 2 [14] then:

(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.

If the competent authority becomes aware of an unpatched, actively exploited vulnerability according to NCCS Article 37 Paragraph 3 [15], then:

(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.

GOOD TO KNOW

Click on the image to zoom in

Unpatched, actively exploited vulnerabilities must be reported to the CSIRT, which provides support.

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[14] https://eur-lex.europa.eu/legal-content/English/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37
[15] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37

8.4 Reporting of Cyber Threats

TERM

Cyber threat

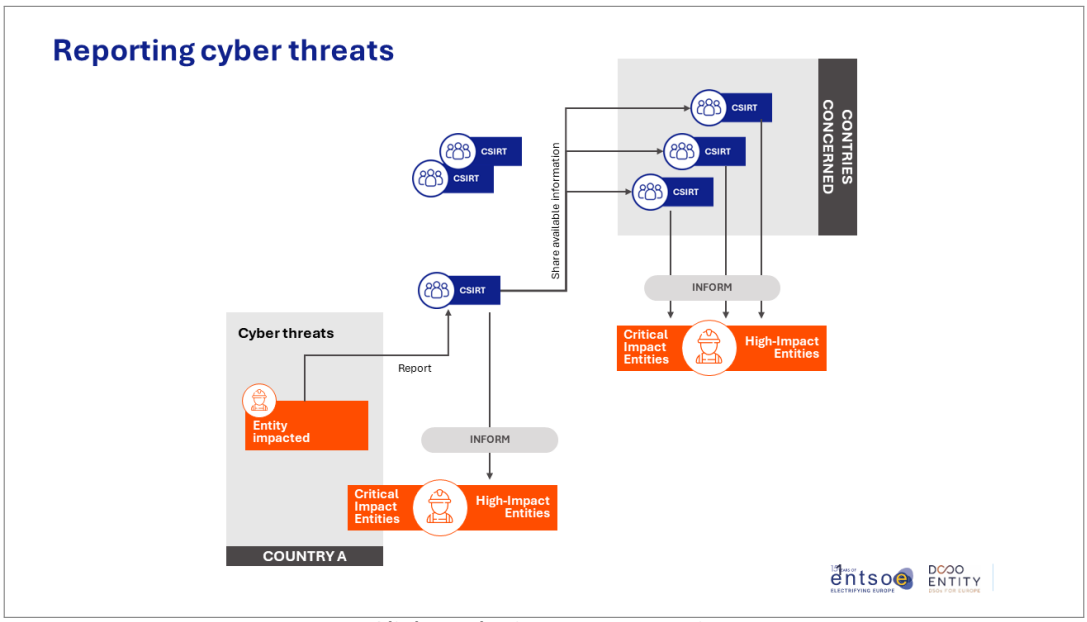
"Cyber threat" as defined in Article 2, point 8 of Regulation REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [a]

Threat means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

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

When reporting cross-border cyber threats, stricter time constraints apply:

the information must be reported immediately. The national CSIRT is responsible for receiving and sharing this information.



Click on the image to zoom in

GOOD TO KNOW

> Entities must promptly report cyber threats to the CSIRT based on NCCS Article 37 Paragraph 5 [a].
>
> [a] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37

m[image=1.chapter/Kep4.png, background=bg.png] == Main tasks of entities

Below, we outline the primary responsibilities of the most important stakeholders:

8.5 High impact and critical impact entities

High impact and critical impact entities

In the final chapter, we summarize the most important tasks of high-impact and critical impact entities:

- Appoints a Single Point of Contact (SPOC) (NCCS Article 38 Paragraph 1 [16]);
- Every three years, **entity level cybersecurity risk management** is conducted for all assets within the high-impact and critical impact perimeters (NCCS Article 26 [17], NCCS Article 27 [18]);
- Keeps an inventory of assets in the **Asset Inventory**. The asset inventory is not part of the risk assessment report (NCCS Article 26 [19]);
- Every three years, submits a **report** to the competent authority, which includes the following information (NCCS Article 27 [20]):
  1. List of controls, along with the current implementation status of each control;
  2. Estimation of the risks related to the confidentiality, integrity, and availability of information and relevant assets for all union-level, high-impact, or critical impact processes;
  3. List of critical ICT service providers based on their critical impact processes.
- Establishes a **cybersecurity management system** (NCCS Article 32 [21]);
- **Demonstrates** compliance with the cybersecurity management system and the **minimum or advanced cybersecurity controls (only critical impact entity)** (NCCS Article 25 [22]);
- **Applies minimum and advanced controls in the supply chain** (Article 33 [23]);

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[18] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_27
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_27
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_25
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33

- Establishes **CSOC capabilities** (NCCS Article 38 [24]);
- **Reports information** related to cyberattacks / cyber threats / unpatched, actively exploited vulnerabilities (NCCS Article 38 [25]);

Topic	Deadline	Organizations Required to Report
Cyberattack	Within 4 hours	CSIRT, Competent Authorithy
Unpatched, actively exploited vulnerability	NIS 2	CSIRT
Cyberthreat	Immediately	CSIRT

- Develops and tests **Cyber Attack Management Procedures** (NCCS Article 39 [26]) and **Crisis Management Plans** at least every three years (NCCS Article 41 [27]);
- Every three years, the -only - critical-impact entity **conducts a cybersecurity exercise** (NCCS Article 43 [28]).

8.6 National Competent Authority

- A national governmental or regulatory authority is **responsible** for carrying out the tasks assigned to it in the (NCCS Article 4 [29]).
- Designated by each member state **six months** after entry into force (NCCS Article 4 Paragraph 1 [30]).
- **Shall coordinate and cooperate** with cybersecurity competent authorities, NRAs, RP NCAs, CSIRTs, and other authorities determined by each Member State to ensure the fulfillment of NCCS and avoid duplication of tasks (NCCS Article 5 [31]).
- **May delegate tasks** to other national authorities (NCCS Article 4 Paragraph 3 [32]).
- **Identify high-impact and critical-impact entities** (NCCS Article 24 Paragrpah 2 [33]).
- **Approve the developed conditions and methodologies** (NCCS Article 6 Paragraph 2 [34]).

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_41
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_43
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[30] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_5
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[34] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_6

- **Conduct cybersecurity risk assessments** (NCCS Article 20 Paragraph 1 [35]).
- **Grant exemptions from minimum and advanced cybersecurity controls** (NCCS Article 30 Paragraph 1 [36]).
- **May perform inspections** of critical-impact entities according to national law to verify their compliance with the NCCS (NCCS Article 25 [37]).

8.7 National Regulatory Authority

1. National Regulatory Authority shall:
   - **Implement the NCCS** regulation in accordance with DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Article 59 Paragraph 1 e) point [38];
   - **Evaluate costs** borne by Transmission System Operators (TSOs) and Distribution System Operators (DSOs) as specified in DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Article 11 [39];
   - **Perform evaluation analysis** within 12 months after the development of the performance evaluation guidelines, as required by DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Article 13 Paragraph 2 [40].

[35] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_20
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_30
[37] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_25
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944#art_59
[39] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944#art_11
[40] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944#art_13

Chapter 9

Quiz

QUESTION 1

Which organization is responsible for preparing the Union-wide risk assessment report under the NCCS framework?

Mark the correct answer.

level: normal

A ENISA

B ACER

C ENTSO-E

D EU DSO

QUESTION 2

Which of the following statements is characteristic of the NCCS regulation?

Mark the correct answer.

level: easy

A It only applies to IT systems

B It covers the security of both OT and IT systems

C It is not legally binding for the member states

D It only applies to electricity-generating companies

QUESTION 3

Match the following concepts or organizations with their corresponding definitions

Match the letters with the numbers.

level: easy

1

ENTSO-E

2

ACER

3

NIS-2

A

Agency for the Cooperation of Energy Regulators

B

European Cybersecurity Directive for the protection of information systems

C

European Network of Transmission System Operators for Electricity

QUESTION 4

Match the organizations with their roles

Match the letters with the numbers.

level: normal

1

ENTSO-E

2

ENISA

3

EU DSO

4

ACER

A

Preparation of Union-wide cybersecurity risk assessment report

B

Regular Union-wide cybersecurity exercise

C

Supporting distribution system operators

D

Providing opinions on methodologies

QUESTION 5

Arrange the following transitional provisions related to the NCCS in chronological order

Write the numbers in the blanks.

level: normal

- Compilation of a provisional list of high-impact and critical impact entities
- Elaboration of provisional ECII
- Development of controls prescribed by relevant European and international standards and national regulations

QUESTION 6

Group the elements of the cybersecurity framework into the appropriate categories

Write the numbers to the correct category on the dotted line.

level: normal

1. Processes for the secure and controlled design, development, and manufacturing of ICT products, ICT services, and ICT processes
2. Background checks of personnel dealing with sensitive information or having access to the organization's high-impact or critical impact assets
3. Traceability of the application of cybersecurity requirements from the development through manufacturing to delivery of ICT products, ICT services, or ICT processes
4. Union-level high-impact processes and Union-level critical impact processes
5. ECII, as well as high-impact and critical impact thresholds
6. Development of cybersecurity risk methodologies
7. Regional risk assessment reports
8. Assessment of the risk profile of suppliers

Risk Assessment

Supply Chain Security

QUESTION 7

What is the main objective of the NCCS risk assessment process?

Mark the correct answer.

level: normal

A Risk assessment related to the implementation of new IT systems

B Development of a risk impact matrix

C Identification and management of risks affecting cross-border electricity flows

D Ensuring regulatory compliance

QUESTION 8

Which element is not included in the Risk Impact Matrix?

Mark the correct answer.

level: easy

A Consequences

B Probability

C Thresholds

D List of suppliers

QUESTION 9

What does the abbreviation ECII stand for?

Mark the correct answer.

level: normal

A Electronic Component Integration Index

B Electricity Cybersecurity Impact Index

C European Cyber Defence Index

D Risk Tool Selection Index

QUESTION 10

Match the risk assessment levels with their tasks

Match the letters with the numbers.

level: normal

1

Union Level

2

Member State Level

3

Regional Level

A

Preparation of regional risk assessment reports

B

Identification of high-impact and critical impact organizations

C

Risk Impact Matrix

QUESTION 11

Match the cybersecurity threats with the related processes

Match the letters with the numbers.

level: hard

1

Risks of Outdated Systems

2

Cascading Effects of Cyber Attacks

3

Supply Chain Threats

A

Analysis of real-time systems

B

Assessment of the risk profile of suppliers

C

Updating cybersecurity strategies

QUESTION 12

Match the following terms with their definitions

Match the letters with the numbers.

level: hard

1

Cyber Attack Scenario

2

Risk Mitigation Plan

3

Risk Impact Matrix

A

A tool for analyzing consequences and probability

B

An entity level action plan for managing risks

C

Modeling of possible attacks

QUESTION 13

Order the levels of the NCCS risk assessment processes

Write the numbers in the blanks.

level: easy

- National Level
- Entity Level
- Union Level
- Regional Level

QUESTION 14

Arrange the following steps based on the cybersecurity impact matrix

Write the numbers in the blanks.

level: hard

- Categorization of risks
- Application of thresholds
- Analysis of probabilities
- Determination of consequences

QUESTION 15

Group the following cybersecurity levels with their related tasks

Write the numbers to the correct category on the dotted line.

level: normal

1. National risk assessment reports
2. Development of risk impact matrix
3. Regional cybersecurity risk mitigation plans
4. Preparation of regional risk assessment reports
5. Union-level high-impact processes and union-level critical impact processes

6. Identification of high-impact entities

Union Level

. . . . . .

Regional Level

. . . . . .

National Level

. . . . . .

QUESTION 16

Which cyberattacks need to be reported?

Mark the correct answer.

level: normal

A All cyberattacks

B All malicious cyberattacks

C All malicious cyberattacks classified as "high" or "critical"

QUESTION 17

Within what time frame should malicious cyberattacks classified as "high" or "critical" be reported?

Mark the correct answer.

level: normal

A They must be reported to the competent authority immediately

B They must be reported to the CSIRT within 2 hours

C They must be reported to both the CSIRT and the competent authority within 4 hours

QUESTION 18

Which statement is true?

Mark the correct answer.

level: normal

A High-impact and critical impact emtities must establish CSOC capability (even if outsourced)

B Only critical impact entities must establish CSOC capability (even if outsourced)

C High-impact and critical impact entities must establish CSOC capability (cannot be outsourced)

QUESTION 19

What does high-impact scope mean?

Mark the correct answer.

level: normal

A Physical and/or logical demarcation determined by the organization (e.g., fence, server room, firewall, proxy server, etc.) that encompasses all high-impact assets and any other assets within this demarcation.

B Physical and/or logical demarcation determined by the organization (e.g., fence, server room, firewall, proxy server, etc.) that encompasses all critical, high-impact assets and any other assets within this demarcation.

C Physical demarcation determined by the organization (e.g., fence, server room, firewall, proxy server, etc.) that encompasses all high-impact assets and any other assets within this demarcation.

Chapter 10

Discover the next level of up-to-date cybersecurity Readiness

You've reached the end of the NCCS Full content.

We hope you gained valuable and insightful information to support your organisation's cybersecurity efforts.

Unlock AI-Driven Readiness Tiers

As a next level in your journey, get a concise overview of how the Readiness Tiers can support your organisation through a unique, AI-driven, near-real-time knowledge transfer. Explore our Readiness Tiers and subscribe to get instant access to up-to-date information on how to mitigate, prevent, and defend against risks arising from vulnerabilities.

Glossary

Accreditation

Shall mean an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.

REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [1]

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/ [2]

REGULATION (EU) 2019/942 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [3]

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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [4]

Assurance level

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0765
[2] https://www.acer.europa.eu/
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0942
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

Means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [5]

Authorities responsible for the management of cyber crises

Authorities designated or established pursuant to Article 9(1) of Directive (EU) 2022/2555 on the management of cyber crises. Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [6]

CER Directive

On December 14, 2022, the European Union adopted the European Parliament and Council Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC

CER Directive. [7]

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 [8]

Conformity assessment

Shall mean the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

Regulation (EC) 765/2008 of the European Parliament and of the Council [9]

Conformity assessment body

Shall mean a body that performs conformity assessment activities including calibration, testing, certification and inspection.

Regulation (EC) 765/2008 of the European Parliament and of the Council [10]

Conformity self-assessment

Means an action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [11]

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 [12]

Critical-impact asset

Means an asset that is necessary to carry out a critical-impact process.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [13]

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. [14]

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02008R0765-20210716
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02008R0765-20210716
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [15]

Critical-impact perimeter

Means a perimeter defined by an entity referred to in Article 2(1) [16] 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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [17]

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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [18]

Critical-impact threshold

Means the values of the electricity cybersecurity impact indices referred to in Article 19(3) b [19], above which a cyber-attack on a business process will cause critical disruption of cross-border electricity flows.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [20]

Cross-border flow

Means a physical flow of electricity on a transmission network of a Member State that results from the impact of the activity of producers, customers, or both, outside that Member State on its transmission network.

Regulation (EU) 2019/943 of the European Parliament and of the Council [21]

Cyber attack

Cyber-attack means a malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorised access to, or make

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_2
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_19
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02019R0943-20240716

unauthorised use of, an asset.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [22]

Cyber threat

Means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [23]

Cyber threat

"Cyber threat" as defined in Article 2, point 8 of Regulation REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [24]

Threat means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

Cyberattack

A security incident as defined in Article 3, Paragraph 14 of REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [25]

A malicious ICT-related incident in which a threat actor attempts to destroy, disclose, modify, disable, steal, gain unauthorized access to, or make unauthorized use of an asset.

Cybersecurity

Means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [26]

Cybersecurity control

Means the actions or procedures carried out with the purpose of avoiding, detecting, counter-

[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=CELEX:32019R0881
[24] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881

acting, or minimising cybersecurity risks.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [27]

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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [28]

Cybersecurity operation centre (CSOC)

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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [29]

Cybersecurity vulnerability management

Means the practice of identifying and addressing vulnerabilities.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [30]

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.

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

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 [31]

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/ [32]

REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [33]

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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [34]

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 [35]

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[32] https://eudsoentity.eu/
[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=OJ:L_202401366
[35] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D1117(01)

Electricity crisis

Means a present or imminent situation in which there is a significant electricity shortage, as determined by the Member States and described in their risk-preparedness plans, or in which it is impossible to supply electricity to customers.

REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [36]

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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [37]

Entity

Means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [38]

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 cybersecurity certification scheme

Means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [39]

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

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0941
[37] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[39] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881

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/ [40]

REGULATION (EU) 2019/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [41]

European Union Agency for Cybersecurity (ENISA)

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

High-impact asset

Means an asset that is necessary to carry out a high-impact process.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [42]

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. [43]

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [44]

High-impact perimeter

Means a perimeter defined by any entity listed in Article 2(1) [45] 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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [46]

High-impact process

[40] https://www.entsoe.eu/
[41] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943
[42] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[43] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_19
[44] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[45] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_2
[46] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

Means any business process carried out by an entity for which the electricity cybersecurity impact indices are above the high-impact threshold.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [47]

High-impact threshold

Means the values of the electricity cybersecurity impact indices referred to in Article 19(3)b [48], above which a successful cyber-attack on a process will cause high disruption of cross-border electricity flows.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [49]

ICT

Information and Communications Technology.

ICT process

Means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [50]

ICT product

Means an element or a group of elements of a network or information system.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [51]

ICT service

Means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [52]

[47] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[48] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_19
[49] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[50] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[51] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881
[52] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881

Incident

Means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [53]

Incident handling

Means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [54]

Large-scale cybersecurity incident

Means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [55]

Legacy ICT system

Means an ICT system that has reached the end of its lifecycle (end-of-life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity.

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [56]

Managed security service provider

Means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [57]

[53] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[54] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[55] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[56] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554
[57] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

Managed service provider

Means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [58]

Mapping matrix

Developed in accordance with COMMISSION DELEGATED REGULATION (EU) 2024/1366 Art.34 [59], that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks.

Member state

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

National accreditation body

Shall mean the sole body in a Member State that performs accreditation with authority derived from the State.

REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [60]

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)

[58] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[59] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_34
[60] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02008R0765-20210716

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

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 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [61].

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [62]

Near miss

Means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [63]

Network and information system

Means:

Article 6 point (1): . an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972; . any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or . digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [64]

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.

[61] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[62] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[63] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[64] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

COMMISSION IMPLEMENTING DECISION (EU) 2017/179 [65]

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.

Originator

Means an entity that initiates an information exchange, information sharing or information storage event.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [66]

OT (Operation Technology)

OT is the combination of production automation, machine-to-machine communication and data collection.

Procurement specifications

Means the specifications that entities define for the procurement of new or updated ICT products, ICT processes or ICT services.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [67]

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 [68]

Representative

[65] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017D0179
[66] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[67] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[68] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0943

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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [69]

Risk

Means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [70]

Risk impact matrix

Means a matrix used during risk assessment to determine the resulting risk impact level for each risk assessed.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [71]

Risk Preparedness National Competent Authority (RP-NCA)

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

Security of network and information systems

Means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [72]

Significant cyber threat

Means a cyber threat which, based on its technical characteristics, can be assumed to have the

[69] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[70] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[71] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[72] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [73]

Single point of contact at entity level (SPOC)

Means single point of contact at entity level as designated under Article 38(1) point (c); [74]

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [75]

Stakeholder

'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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [76]

Standard

Means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory.

REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [77]

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, established in accordance with Article 36 of Regulation (EU) 2019/943.

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 [78]

[73] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[74] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_38
[75] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[76] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[77] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1025
[78] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944

Technical specification

Means a document that prescribes technical requirements to be fulfilled by a product, process, service or system and which lays down one or more of the following.

REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [79]

The Reportable Cyberattack

Every critical-impact and high-impact organization must, without undue delay but **no later than four hours** after becoming aware that a cyber attack is reportable, share relevant information regarding the reportable cyber attack with its CSIRTs and competent authority, as per (NCCS Article 38 Paragraph 2 [80]).

According to (NCCS Article 38 Paragraph 3 [81]), information related to a cyber attack is considered reportable if the affected organization's assessment determines that, based on the classification scale outlined in (NCCS Article 37 Paragraph 8 [82]), the attack's **severity ranges from "high" to "critical."** The classification of security incidents is communicated by the single organizational point of contact designated under paragraph 1(c).

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 inter-connections 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 [83]

Union-wide Critical-Impact Process

Any electricity sector process, possibly involving multiple entities, where a cyber-attack may be deemed critical during the Union-wide cybersecurity risk assessment.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [84]

Union-wide High-Impact Process

[79] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1025
[80] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[81] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[82] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37
[83] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944
[84] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366

Any electricity sector process, possibly involving multiple entities, where a cyber-attack may be deemed high during the Union-wide cybersecurity risk assessment.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [85]

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.

COMMISSION DELEGATED REGULATION (EU) 2024/1366 [86]

Unpatched, actively exploited vulnerability

A vulnerability as defined in Article 6, point 15 of Directive DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [87] 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.

Vulnerability

Means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat.

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [88]

[85] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[86] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366
[87] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
[88] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

Resources

FILE 1

Provisional list of Union-wide high-impact and critical-impact processes

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

files/Supporting document Provisional list of Union-wide high-impact and critical-impact processes.pdf

FILE 3

Provisional Electricity Cybersecurity Impact Index (ECII)

files/Provisional ECII.pdf

FILE 4

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

files/Supporting document provisional ECII.pdf

Solutions

Question 1:

A ENISA

B ACER

C ENTSO-E ✓

D EU DSO

Feedback if the answer is correct:

Correct ENTSO-E is responsible for the EU-wide risk assessment reports.

Feedback if the answer is incorrect:

Incorrect. The correct answer is ENTSO-E.

Question 2:

A It only applies to IT systems

B It covers the security of both OT and IT systems ✓

C It is not legally binding for the member states

D It only applies to electricity-generating companies

Feedback if the answer is correct:

CorrectThe NCCS ensurems the protection of both OT and IT systems in the European electricity sector.

Feedback if the answer is incorrect:

Incorrect. The correct answer is: It covers the security of both OT and IT systems.

Question 3:

The right matching:

Pair 1:

ENTSO-E

European Network of Transmission System Operators for Electricity

Pair 2:

ACER

Agency for the Cooperation of Energy Regulators

Pair 3:

NIS-2

European Cybersecurity Directive for the protection of information systems

Feedback if the answer is correct:

GreatThe terms have been correctly matched.

Feedback if the answer is incorrect:

Incorrect. Check the descriptions of the terms and try again.

Question 4:

The right matching:

Pair 1:

ENTSO-E

Preparation of Union-wide cybersecurity risk assessment report

Pair 2:

ACER

Providing opinions on methodologies

Pair 3:

EU DSO

Supporting distribution system operators

Pair 4:

ENISA

Regular Union-wide cybersecurity exercise

Feedback if the answer is correct:

Great jobAll organizations have been correctly matched with their roles.

Feedback if the answer is incorrect:

Incorrect. Check the roles of the organizations and match them again.

Question 5:

The right order:

1. Elaboration of provisional ECII
2. Compilation of a provisional list of high-impact and critical impact entities
3. Development of controls prescribed by relevant European and international standards and national regulations

Feedback if the answer is correct:

Correct order: Development of provisional ECII, List of organizations, List of standards.

Feedback if the answer is incorrect:

Incorrect. The chronological order is: Elaboration of provisional ECII, List of entities, List of standards.

Question 6:

The right grouping:

Risk Assessment

- Development of cybersecurity risk methodologies
- Regional risk assessment reports
- Union-level high-impact processes and Union-level critical impact processes
- ECII, as well as high-impact and critical impact thresholds

Supply Chain Security

- Assessment of the risk profile of suppliers
- Processes for the secure and controlled design, development, and manufacturing of ICT products, ICT services, and ICT processes
- Traceability of the application of cybersecurity requirements from the development through manufacturing to delivery of ICT products, ICT services, or ICT processes
- Background checks of personnel dealing with sensitive information or having access to the organization's high-impact or critical impact assets

Feedback if the answer is correct:

Correct. The elements of the cybersecurity framework have been correctly grouped

Feedback if the answer is incorrect:

Incorrect. Check the descriptions of the categories, and try again.

Question 7:

A Risk assessment related to the implementation of new IT systems

B Development of a risk impact matrix

C Identification and management of risks affecting cross-border electricity flows ✓

D Ensuring regulatory compliance

Feedback if the answer is correct:

CorrectThe main objective of the NCCS risk assessment process is to identify and manage risks affecting cross-border energy flows.

Feedback if the answer is incorrect:

Incorrect. The correct answer is: Identification and management of risks affecting cross-border electricity flows.

Question 8:

A Consequences

B Probability

C Thresholds

D List of suppliers ✓

Feedback if the answer is correct:

CorrectThe list of suppliers is not part of the Risk Impact Matrix.

Feedback if the answer is incorrect:

Incorrect. The correct answer is: List of suppliers.

Question 9:

A Electronic Component Integration Index

B Electricity Cybersecurity Impact Index ✓

C European Cyber Defence Index

D Risk Tool Selection Index

Feedback if the answer is correct:

CorrectECII stands for Electricity Cybersecurity Impact Index.

Feedback if the answer is incorrect:

Incorrect. The correct answer is: Electricity Cybersecurity Impact Index.

Question 10:

The right matching:

Pair 1:

Union Level

Risk Impact Matrix

Pair 2:

Regional Level

Preparation of regional risk assessment reports

Pair 3:

Member State Level

Identification of high-impact and critical impact organizations

Feedback if the answer is correct:

GreatEach level has been correctly matched with its corresponding task.

Feedback if the answer is incorrect:

Incorrect. Check the roles of the levels, and try again.

Question 11:

The right matching:

Pair 1:

Supply Chain Threats

Assessment of the risk profile of suppliers

Pair 2:

Cascading Effects of Cyber Attacks

Analysis of real-time systems

Pair 3:

Risks of Outdated Systems

Updating cybersecurity strategies

Feedback if the answer is correct:

GreatThe threats have been correctly matched with the appropriate processes.

Feedback if the answer is incorrect:

Incorrect. Try matching the threats and processes again.

Question 12:

The right matching:

Pair 1:

Risk Impact Matrix

A tool for analyzing consequences and probability

Pair 2:

Risk Mitigation Plan

An entity level action plan for managing risks

Pair 3:

Cyber Attack Scenario

Modeling of possible attacks

Feedback if the answer is correct:

Great jobEvery term has been matched with its correct definition.

Feedback if the answer is incorrect:

Incorrect. Check the definitions of the terms, and try again.

Question 13:

The right order:

1. Union Level
2. Regional Level
3. National Level
4. Entity Level

Feedback if the answer is correct:

Correct order: Union Level, Regional Level, National Level, Entity Level.

Feedback if the answer is incorrect:

Incorrect. Try the correct order of the levels again.

Question 14:

The right order:

1. Determination of consequences
2. Analysis of probabilities
3. Application of thresholds
4. Categorization of risks

Feedback if the answer is correct:

Correct order: Consequences, Probabilities, Thresholds, Categorization.

Feedback if the answer is incorrect:

Incorrect. Check the order of the steps, and try again.

Question 15:

The right grouping:

Union Level

- Development of risk impact matrix

- Union-level high-impact processes and union-level critical impact processes

Regional Level

- Preparation of regional risk assessment reports
- Regional cybersecurity risk mitigation plans

National Level

- Identification of high-impact entities
- National risk assessment reports

Feedback if the answer is correct:

GreatEach level has been correctly grouped with its respective tasks.

Feedback if the answer is incorrect:

Incorrect. Check the levels and their tasks, then try again.

Question 16:

A All cyberattacks

B All malicious cyberattacks

C All malicious cyberattacks classified as "high" or "critical" ✓

Feedback if the answer is correct:

GreatAll malicious cyberattacks classified as "high" or "critical" need to be reported

Feedback if the answer is incorrect:

Incorrect. Check the answers again

Question 17:

A They must be reported to the competent authority immediately

B They must be reported to the CSIRT within 2 hours

C They must be reported to both the CSIRT and the competent authority within 4 hours ✓

Feedback if the answer is correct:

GreatThey must be reported to both the CSIRT and the competent authority within 4 hours

Feedback if the answer is incorrect:

Incorrect. Check the answers again

Question 18:

A High-impact and critical impact emtities must establish CSOC capability (even if outsourced) ✓

B Only critical impact entities must establish CSOC capability (even if outsourced)

C High-impact and critical impact entities must establish CSOC capability (cannot be outsourced)

Feedback if the answer is correct:

GreatHigh-impact and critical impact emtities must establish CSOC capability (even if outsourced)

Feedback if the answer is incorrect:

Incorrect. Check the answers again

Question 19:

A Physical and/or logical demarcation determined by the organization (e.g., fence, server room, firewall, proxy server, etc.) that encompasses all high-impact assets and any other assets within this demarcation. ✓

B Physical and/or logical demarcation determined by the organization (e.g., fence, server room, firewall, proxy server, etc.) that encompasses all critical, high-impact assets and any other assets within this demarcation.

C Physical demarcation determined by the organization (e.g., fence, server room, firewall,

proxy server, etc.) that encompasses all high-impact assets and any other assets within this demarcation.

Feedback if the answer is correct:

Great Physical and/or logical demarcation determined by the organization (e.g., fence, server room, firewall, proxy server, etc.) that encompasses all high-impact assets and any other assets within this demarcation.

Feedback if the answer is incorrect:

Incorrect. Check the answers again