entsoe EU DSO Entity

Supporting document for the Network Code for cybersecurity aspects of cross-border electricity flows

14 January 2022

1 PURPOSE AND OBJECTIVES OF THIS SUPPORTING DOCUMENT

1.1 PURPOSE OF THIS DOCUMENT

This document has been developed jointly by the European Network of Transmission System Operators for Electricity (ENTSO-E) and the EU DSO entity to accompany the Network Code on Cybersecurity (NCCS) and should be read in conjunction with that Network Code.

This document provides all interested parties with information about the rationale for the approach set out in the NCCS, outlining the reasons that led to the requirements specified in it. The document has been developed in recognition of the fact that the NCCS, which will become a legally binding document after its adoption by the European Commission, inevitably cannot provide the level of detailed explanation which some parties may desire.

1.2 STRUCTURE OF THE DOCUMENT

This document is structured as follows:

1 PURPOSE AND OBJECTIVES OF THIS SUPPORTING DOCUMENT

2 PROCEDURAL ASPECTS

3 PRINCIPLES, STRUCTURE AND SCOPE OF THE DRAFTING OF THE NCCS

4 FRAMEWORK GUIDELINE ON CYBERSECURITY

5 TITLE I - GENERAL PROVISIONS

6 TITLE II - GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

7 TITLE III – RISK MANAGEMENT AT UNION AND REGIONAL LEVEL

8 TITLE IV - COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

9 TITLE V - RISK MANAGEMENT AT MEMBER STATE LEVEL

10 TITLE VI - RISK MANAGEMENT AT ENTITY LEVEL

11 TITLE VII - HARMONISED CYBERSECURITY PROCUREMENT REQUIREMENTS

12 TITLE VIII - ESSENTIAL INFORMATION FLOWS, CYBERSECURITY INCIDENT AND CRISIS MANAGEMENT

13 TITLE IX - ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

14 TITLE X - PROTECTION OF INFORMATION

15 TITLE XI - FINAL PROVISIONS

Sections 6 to 16 describes for each provision of NCCS the objectives that the NCCS sets out to achieve by means of the defined requirements. These Sections aims at providing the reader the basis for understanding the requirements set in the chapters marked above of the NCCS.

1.3 LEGAL STATUS OF THE DOCUMENT

This document accompanies the NCCS and is provided for information purposes only. Consequently, this document is not legally binding.

2 PROCEDURAL ASPECTS

2.1 INTRODUCTION

This section provides an overview of the procedural aspects of the development of the NCCS. It explains the legal framework within which the NCCS is developed and focuses on the roles and responsibilities assigned to ENTSO-E and the EU DSO entity. It also explains the next steps in the process of developing the NCCS.

2.2 THE FRAMEWORK FOR DEVELOPING THE NCCS

The NCCS is the first Network Code that will be developed according to the new rules established by the Regulation (EU) 2019/943, in particular as set out in Article 59 were responsibilities in the formal network code development process are assigned to ENTSO-E, the EU DSO entity and ACER. The NCCS will be the first network code that is to be (co)drafted by ENTSO-E and the EU DSO entity and for which a specific drafting committee with the involvement of a limited number of the main stakeholders had to be set up by ENTSO-E.

The legal role of ENTSO-E and the EU DSO entity in Network Code development according to Regulation (EU) 2019/943 (Source: ENTSO-E):

- Article 28 ENTSO for Electricity shall act with a view to establishing a well-functioning and integrated internal market for electricity; Article 52 EU DSO entity shall promote the completion and functioning of the internal market for electricity
- Article 59 Establishment of Network Codes: network code to be in accordance with ACER framework guidelines, network code will become binding, establishment of drafting committee, Article 31 and 56: extensive stakeholder consultation
- Article 59 (2) (e) Scope of network code sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

According to Article 59 of Regulation (EU) 2019/943, the network code development process is structured with different responsibilities of ENTSO-E, the EU DSO entity, ACER and the European Commission.

NCCS development process (Source: ENTSO-E):

- European Commission request to ACER to submit a non-binding framework guideline
- ACER elaborates the framework guideline in consultation with stakeholders, in particular with ENTSO-E and EU DSO entity and submits framework guideline to European Commission
- European Commission requests ENTSO-E in close cooperation with the EU DSO entity to elaborate NCCS according to ACER framework guideline
- ENTSO-E convenes drafting committee and consults jointly with the EU DSO entity the stakeholders on the draft NCCS before submitting its final proposal for the NCCS to ACER for revision
- ACER consultation and submit the NCCS to European Commission

- European Commission adopts NCCS as delegated act

The NCCS has been drafted by ENTSO-E and the EU DSO entity to meet the requirements of the non-binding ACER framework guideline on cybersecurity published by ACER on 27 July 2021. ENTSO-E and the EU DSO entity cooperated throughout the whole drafting process on equal footing and paid utmost attention to the involvement of the main affected stakeholders, in particular via the drafting committee and during the consultation process.

ENTSO-E was formally requested by the European Commission to submit a proposal for a network code on cybersecurity on 23 July 2021. The deadline to submit the NCCS is 14 January 2022, i.e. the whole formal network code development process is to be finalised within less than 6 months.

3 PRINCIPLES, STRUCTURE AND SCOPE OF THE DRAFTING OF THE NCCS

3.1 BACKGROUND

Following Regulation (EU) 2019/943, ENTSO-E and the EU DSO entity have drafted the NCCS to set out clear and objective principles for sector-specific rules for cyber security aspects of cross- border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

The ACER framework guideline took into account some high-level objectives and the extensive preparatory work completed so far (e.g. the recommendations of the Smart Grid Task Force Expert Group 2 report and the recommendations of the European Network of Transmission System Operators for Electricity (ENTSO-E) and Distribution System Operator (DSO) associations included in the final report). Nevertheless, the framework guideline diverges from some of the recommendations. In line with Article 59(9) of Regulation 2019/943 the NCCS follows the principles set out in the ACER framework guideline.

3.2 GUIDING PRINCIPLES

The guiding principles of the NCCS are to determine common sound cybersecurity requirements in order to maintain security of electricity supply and ensure the highest level of cybersecurity protection in the electricity sector.

Energy technologies embedding digital components and the security of the associated supply chains are important for the continuity of essential services and for the strategic control of critical energy infrastructure. The NCCS will therefore contribute actively to the strategic objectives set in the "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade".

Regulation (EU) 2019/943 assigns specific responsibilities with regard to cybersecurity to Transmission System Operators ('TSOs') and Distribution System Operators ('DSOs'). Moreover, their European associations ENTSO-E and the EU DSO entity shall promote cyber security in cooperation with relevant authorities and regulated entities.

Furthermore, the NCCS will also cover responsibilities of very diverse bodies at Union level (e.g. ACER, ENISA, ENTSO-E, EU DSO entity), regional level (e.g. RCCs) and national level (e.g. NEMOs, NRAs, RP-NCAs, CS-NCAs, CSIRTs). The NCCS will define the shared responsibilities between the different institutions at national, regional and Union level with regard to the risk assessments, the information flows in case of a cybersecurity incident and monitoring of the operational reliability of the NCCS.

The NCCS also limits the collection of information to a reasonable amount, provides for achievable deadlines for stakeholders to submit such information and strives to avoid double notification.

3.3 STRUCTURE

In order to set out clear and objective requirements for cybersecurity, the NCCS is structured as follows:

- Title I: General provisions;
- Title II: Governance for cybersecurity risk management;
- Title III: Risk management at Union and at regional level;

- Title IV: Common electricity cybersecurity framework;
- Title V: Risk assessment at member state level;
- Title VI: Risk management at entity level;
- Title VII: Harmonised cybersecurity procurement requirements;
- Title VIII: Essential information flows, cybersecurity incident and crisis management;
- Title IX: Electricity cybersecurity exercise framework;
- Title X: Protection of information;
- Title XI: Final provisions.

3.4 LEVEL OF DETAIL

The NCCS should achieve the necessary level of harmonization at Union level, while allowing at the same time for more detailed provisions at the regional/national level where necessary. The NCCS should also ensure its applicability taken into account future developments and new applications. Hence, the NCCS will focus inter alia on:

- common minimum requirements,
- an integrated approach for risk assessments,
- a common cybersecurity framework, and
- clear responsibilities with regard to the protection and exchange of information.

The level of detail in the NCCS does not allow for all rules and methodologies to be included in the network code itself, but provides for a clear time line and principles to develop in following steps the requirements, criteria, methodologies and performance indicators, once the NCCS has entered into force.

3.5 SCOPE OF THE NCCS

According to Article 58 of Regulation (EU) 2019/943 the NCCS shall

a) ensure a minimum degree of harmonisation;

b) take into account regional specificities, where appropriate; and

c) not go beyond what is necessary for the purposes of point (a).

The right of the Member States to establish national network codes which do not affect cross-zonal trade is not limited.

The NCCS applies within the Union. For this reason, issues concerning third countries are not in the scope of the NCCS. Notwithstanding, cybersecurity protection does not stop at the Union's borders. A secure system requires the involvement of third country parties. The Union, its Members States, European and national institutions and TSOs should support third countries in applying similar cybersecurity rules as set out in the NCCS. ENTSO-E should facilitate cooperation between the Union TSOs and third country TSOs.

Considering the importance of cybersecurity and that cybersecurity does not stop at borders, the NCCS has a large scope of application meaning that the minimum cybersecurity requirements have to be applied by many public and private entities in the electricity sector, including national and European

administrative bodies. The main criteria to determine the scope of the NCCS is not the size of an entity but the criticality of its activity with regard to its impact on cross-border electricity flows. Thus, under certain conditions also micro and small-sized enterprises may be in the scope of the NCCS.

Any entity or third party to whom responsibilities have been delegated or assigned with a relevant cybersecurity impact on cross-border electricity flows has to apply the NCCS requirements.

Overview of entities that are in the scope of the NCCS:

Public and private entities

(a) Electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944;

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

(c) electricity digital market platforms as defined in Article 4(28) of this Regulation;

(d) critical service providers as defined in Article 4(12) of this Regulation;

(k) managed security service provider or 'MSSP' as defined in Article 4(43) of this Regulation;

(m) computer security incident response teams or 'CSIRTs' established pursuant to Article 9 of Directive (EU) 2016/1148;

European bodies

(f) the ENTSO for Electricity established pursuant to Article 28 of Regulation (EU) 2019/943;

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

(h) the European Union Agency for the Cooperation of Energy Regulators or 'ACER' established by Regulation (EU) 2019/942;

(n) the European Union Agency for Cybersecurity or 'ENISA' established pursuant to Regulation (EU) 2019/881;

Regional bodies

(e) regional coordination centres or 'RCCs' as defined in Article 2(63) and as established pursuant to Article 35 of Regulation (EU) 2019/943;

National bodies

(i) regulatory authorities or 'NRAs' as defined in Article 59 of Directive (EU) 2019/944;

(j) national competent authorities for risk preparedness or 'RP-NCA' established pursuant to Article 3 of Regulation (EU) 2019/941;

(l) national competent authorities on the security of network and information systems or 'CS-NCA' as designated pursuant to Article 8 of Directive (EU) 2016/1148;

Other

(o) any entity or third party to whom responsibilities have been delegated or assigned.

ACER is responsible for the monitoring of the correct implementation of the NCCS. Enforcement power lies within the NRAs in each Member State of the Union.

3.6 CHALLENGES FOR THE NCCS

As technology is evolving constantly and digitalization of the electricity sector is progressing rapidly, the NCCS therefore strives not to be detrimental to innovation and not to constitute a barrier to the access of new entities to the electricity market and the subsequent use of innovative solutions that contribute to the efficiency of the electricity system. Notwithstanding, all new systems, processes and procedures shall respect cyber security requirements. In order to identify new trends and possible future risk in cybersecurity, a regular, reporting, the so-called "Cross-Border Electricity Cybersecurity Risk Assessment" is foreseen in the NCCS, performed at least every three years.

3.7 INTERACTION OF THE NCCS WITH THE MAIN CYBERSECURITY LEGISLATION IN THE UNION

The NCCS will built upon already existing cybersecurity legal requirements and will strive to complement these in order to increase cybersecurity for the electricity sector in the Union. In particular the general rules on security of network and information systems laid down in Directive (EU) 2016/1148 of the European Parliament and of the Council ('NIS Directive') is complemented by the NCCS by ensuring that cybersecurity incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans.

Moreover, the NCCS is to be drafted in parallel when some of the main legislation on cyber security is under revision (in particular the NIS 2.0 Directive). The outcome of the negotiations between the European co-legislators and the European Commission will therefore not be known, when ENTSO-E and the EU DSO entity have to submit the final NCCS to ACER for review. Therefore, ENTSO-E and the EU DSO entity strive to ensure as much coherence and consistency and compatibility as possible with the legislative changes that are discussed in parallel.

3.8 WORKING WITH STAKEHOLDERS

The legally binding nature of the NCCS once adopted by the European Commission implies that the requirements set out in the NCCS can have a fundamental bearing on stakeholder businesses. As such, ENTSO-E and the EU DSO entity recognised from the beginning of the formal network code development process the importance of engaging with stakeholders at an early stage in an open and transparent manner.

Prior to the official network code development process, informal work under the lead of the European Commission on cybersecurity started in February 2020, which concluded with a technical report beginning of 2021. Following this informal process, the TSOs and DSOs with the support of ACER, the European Commission and ENISA already set up in March 2021 several joint subgroups to elaborate the technical content of the main areas that were to be covered by the ACER framework guideline and subsequently the network code.

Moreover, the network development process as set out in Article 59 of Regulation 2019/943 foresees an extensive stakeholder involvement as well as the set-up of a specific drafting committee to support ENTSO-E and the EU DSO entity in the drafting of the NCCS. ENTSO-E and the EU DSO entity are fully aware of the necessary involvement of stakeholders throughout the network code drafting process.

Pursuant to Article 59 (10) of Regulation (EU) 2019/943 ENTSO-E convened on 08 September 2021 the drafting committee to kick of the formal drafting process. Taking into consideration the suggestions on the stakeholders listed in Article 59 and in the European Commission's letter to ENTSO-E dated 23 July 2021, ENTSO-E formally requested these relevant stakeholders to nominate a representative to the drafting committee in order to participate actively in the monthly meetings to review progress.

ENTSO-E and the EU DSO entity launched a public consultation from 12 November to 10 December

2021 on the NCCS draft for one month. Two public stakeholder workshops were organised on 19 November and 08 December 2021. ENTSO-E and the EU DSO entity held as well ad-hoc meetings and exchanged views with interested parties when necessary.

4 FRAMEWORK GUIDELINE ON CYBERSECURITY

4.1 INTRODUCTION

During the informal process to prepare recommendations on cybersecurity which was led by the European Commission, representatives of ENTSO-E and the EU DSO entity participated actively in the discussions.

In accordance with Article 59(4) of Regulation 2019/943, on 28 January 2021 the European Commission invited ACER to draft a framework guideline for a network code on cybersecurity, taking into account high-level objectives and the extensive preparatory work completed so far (e.g. the recommendations of the Smart Grid Task Force Expert Group 2 report and the recommendations of the ENTSO-E and the Distribution System Operator (DSO) associations included in the final report.

This Framework Guideline was subject to public consultation for two months. During this period, ENTSO-E and EU DSO entity participated in the discussions led by ACER and submitted in addition their responses to ACER's written public consultation.

The NCCS sets the pan-European requirements for cybersecurity aspects with regard to cross-border electricity flows. The requirements described in the NCCS have been formulated with the aim of increasing cybersecurity in the Union and in line with the general principles of the ACER framework guideline.

4.2 DEVIATIONS AND OMISSIONS

In developing the NCCS, there are a limited number of areas where an alternative approach has been chosen in the NCCS to the one set out in the ACER framework guideline. These deviations are described in an Excel spreadsheet provided as an Annex to this supporting document.

5 TITLE I - GENERAL PROVISIONS

Article 1 SUBJECT MATTER

This article is subject of the NCCS limited scope to sector-specific rules for cybersecurity aspects of cross-border electricity flows.

Article 2 SCOPE

This article defines the scope of application of the NCCS by listing the entities to which the NCCS applies. It also specifies the conditions according to which micro and small sized enterprises fall under the scope of the NCCS and the provisions according to which the NCCS applies to critical service providers not established in the Union but that deliver services to entities in the Union.

The NCCS does not apply to micro and small enterprises that are neither critical-impact nor high-impact entities.

This article defines how the Regulation shall apply to critical service providers not established in the Union and how a designated representative withing the Union shall be determined.

Article 3 OBJECTIVES

In this article the overall objectives of the NCCS and the principles that are followed in the NCCS are described.

Article 4 DEFINITIONS

This article lists the most important definitions required for the NCCS. Where possible, ENTSO-E and the EU DSO entity have used terms which have been previously defined in Union legislation that is already in force.

ENTSO-E and the EU DSO entity are striving to ensure consistency with definitions used in other Union legislation as well as other related documents and to grant easy access to the full body of definitions.

Article 5 ADOPTION OF TERMS AND CONDITIONS OR METHODOLOGIES

This article describes the approval procedures of and the regulatory oversight over the terms and conditions or the methodologies that are to be developed by ENTSO-E and EU DSO entity and submitted to approval to ACER. It follows the same approval procedures as in other existing network codes and guidelines.

Article 6 STAKEHOLDER INVOLVEMENT

Stakeholders are the key to success for the implementation of the NCCS. Therefore, this article clarifies how stakeholder involvement is to be organised in addition to the public consultations that will be organised for the developed of terms and conditions or methodologies.

Article 7 PUBLIC CONSULTATION

This article specifies the scope and duration of the public consultations that are to be carried out and also how comments from stakeholders are to be considered when finalising the proposals for the terms and conditions or methodologies.

The regional cybersecurity risk treatment plans and the cross-border electricity cybersecurity risk assessment report are excluded from the list for public consultation due to their confidential nature.

Article 8 RECOVERY OF COSTS

According to this article, costs arising from the NCCS to system operators subject to network tariff regulation (both TSOs and DSOs), are, where relevant, considered as part of regulated costs. Each party must demonstrate with sufficient proof to its NRA that these costs are efficient, reasonable and proportionate.

Article 9 CONFIDENTIALITY OBLIGATIONS

While transparency and access to relevant information is important, but, commercially sensitive information as well as sensitive information on critical process must be sufficiently protected.

A lot of information would be exchanged for the full implementation of the NCCS, as such this article depicts the global obligation of confidentiality between entities regarding to information exchange in order to perform and carry their duties under the network code.

The requirements of this article lay down the necessary rules for the needed protection of information.

Article 10 MONITORING

ACER is responsible for the monitoring of the implementation of the NCCS in accordance with Article 32(1) of Regulation (EU) 2019/943. ENISA will cooperate with ACER, and ENTSO-E and the EU DSO entity will support ACER in this task.

The monitoring assesses in particular whether:

- the NCCS implementation contributes to the political objectives set by the co-legislators in their "Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade";
- the NCCS standards have been implemented by the high-impact and critical-impact entities.

In its monitoring ACER will also assess whether additional measures beyond the ones described in the NCCS may be necessary to prevent risks for the electricity sector.

This article also specifies that the rules of the collection of information are to be determined by ACER within 12 months from the entry into force of the NCCS. ENISA, ENTSO-E and the EU DSO entity will support ACER in defining those rules and they also advise ACER with regard to the reasonable timeframe to collect such information from the entities to whom the NCCS applies.

Finally, ACER will define entity performance indicators that allow assessing operational reliability that can be related to cybersecurity matters.

Article 11 BENCHMARKING

This article describes the different steps to be followed by ACER, ENISA and the NRAs to prepare and

carry out the benchmarking to assess whether current investments in cybersecurity provide expected results. This article also specifies the protection of sensitive information to which Union and national administrative bodies will have access to.

Article 12 AGREEMENTS WITH TSOS NOT BOUND BY THIS REGULATION

As cybersecurity does not stop at national and Union borders, the TSOs of the Union may strive to agree with TSOs outside the Union to apply the NCCS requirements.

Article 13 COOPERATION BETWEEN CS-NCAs, NRAs and CSIRTs of a Member State

At Member State level , the competent authorities for cybersecurity (CS-NCA), the national regulatory authorities (NRAs) and the computer security incident response teams (CSIRTs) are the main bodies involved in the implementation of the NCCS. This article arranges the cooperation between these bodies.

6 TITLE II - GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

Risk management is performed at three levels (see diagram below).

- At Union and regional level by ENTSO-E and the EU-DSO entity supported by a cybersecurity risk working group (Title III);
- At national level by the CS-NCA and NRA (Title IV);
- At entity level by every high-impact and critical-impact entity identified by the CS-NCAs (Title VI).

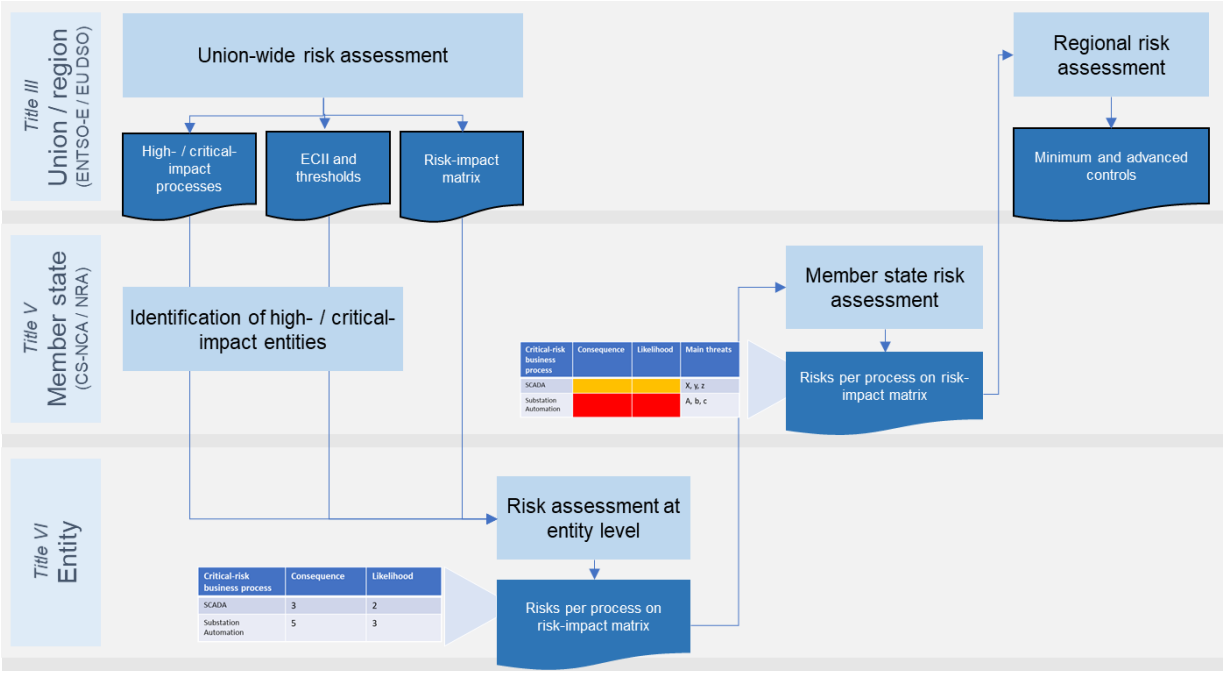


Figure 1: Cybersecurity risk assessment activities at different levels.

Article 14 CYBERSECURITY RISK WORKING GROUP

Currently there is no organization in Europe performing cross-border electricity flow cybersecurity risk identification, evaluation, and treatment. Individual entities do perform their own company and wider national cybersecurity risk assessments (in many cases based on self-regulation), but no one is looking at the overall Union-wide cybersecurity risk picture. To address this issue the Network Code creates a cybersecurity risk working group representing the interests of the main affected stakeholders, including the interests of all high-impact and critical-impact entities.

The cybersecurity risk working group (a) advises ENTSO-E and the EU DSO entity during the Union-wide cybersecurity risk assessment and the regional cybersecurity risk assessments; (b)helps collect the required information and (c) perform the analyses. ENTSO-E and the EU DSO entity are responsible for operating the cybersecurity risk working group and provide appropriate resources to properly assess cross-border electricity flow cybersecurity risk.

ENTSO-E and the EU DSO entity shall invite a limited number of the main stakeholders to the cybersecurity risk working group, to ensure the appropriate consideration of the interests of all affected

entities. Representatives from existing EU associations will also be invited to involve as many stakeholders as possible.

Article 15 CYBERSECURITY RISK MONITORING BODY

ACER shall establish a cybersecurity risk monitoring body consisting of representatives of ACER, ENISA, CS_NCAs, NRAs ad RP-NCAs. The European Commission can act as an observer. The cybersecurity risk monitoring body advises ACER when monitoring the implementation of the cybersecurity standards and adopting the terms and conditions or methodologies..

Article 16 CYBERSECURITY RISK ASSESSMENT METHODOLOGIES

ENTSO-E in cooperation with the EU DSO entity will define methodologies for the risk assessments at Union, regional and national level. At entity level, each entity is allowed to select its own risk assessment methodology subject to certain requirements (Article 33).

For measuring consequences, the cybersecurity risk assessment methodology shall use the consequence categories from the system operation guideline[1], operational security, frequency quality and the efficient use of the interconnected system and resources. In this way, metrics developed from the system operation guideline can be reused.

Note that ENTSO-E in cooperation with the EU DSO e only defines the high-impact and critical-impact processes, the ECII and the methodologies. The identification of the high-impact and critical-impact entities is left to the CS-NCAs (Article 31).

Article 17 CYBERSECURITY RISK ASSESSMENT CYCLE

The cybersecurity risk assessments are organized in a cycle that repeats every three years after the transitional period described in Article 50, see Figure 2.

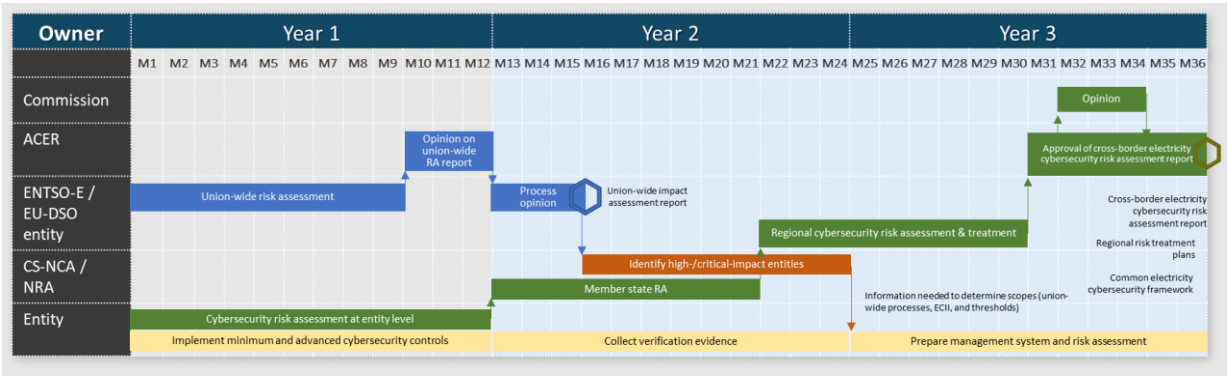


Figure 2: Cybersecurity risk assessment cycle.

In Figure 2, the top-down risk assessments are shown in blue, and the bottom-up risk assessments in green. The top-down and bottom-up assessments are performed in parallel to be able to fit all activities in three years.

[1] COMMISSION REGULATION (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation

Counting from the beginning of the cybersecurity risk assessment cycle, the Union-wide cybersecurity risk assessment report is due after 15 months, and the cross-border electricity cybersecurity risk assessment report is due at the end of the third year.

The CS-NCA can start the identification of the high-impact and critical-impact entities after the Union-wide cybersecurity risk assessment is completed (Article 31). The entities would be identified in month 24 of the cycle. This would give newly identified high-impact and critical-impact entities 12 months to prepare for the start of the next cycle.

7 TITLE III – RISK MANAGEMENT AT UNION AND REGIONAL LEVEL

The risk assessment at the highest levels (Union-wide / regional) is conducted in two phases:

- A Union-wide cybersecurity risk assessment. The impact assessment only considers the consequences of cyber-attacks, but not the likelihood. The assessment works top down. From a European perspective, it determines the high-impact and critical-impact processes needed to maintain cross-border electricity flows, and what the possible consequences of a cyber-attack on such processes would be.
- Regional risk assessments. Each regional risk assessment aggregates data on the likelihood of attacks from all Member States within each system operation region. The likelihood data summarizes the state of threats, countermeasures, and vulnerabilities. Combined with the impact from the Union-wide cybersecurity risk assessment, the total cybersecurity risk level can then be determined.

The scope of the Union-wide and regional cybersecurity risk assessments is limited to cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. Only cyber-attacks with a malicious intent are considered. The risk of cyber-attacks that cause legal, financial or reputational damage to entities are out of scope.

Article 18 UNION-WIDE CYBERSECURITY RISK ASSESSMENT

The Union-wide cybersecurity risk assessment is performed at the start of the cybersecurity risk assessment cycle to provide the information needed for the entities to start the bottom-up risk assessment process.

The Union-wide cybersecurity risk assessments prepares for the other risk assessment steps as follows:

- It allows the CS-NCA to identify the high-impact and critical-impact entities in their Member State by using the list of Union-wide high-impact and critical-impact processes, the ECII, and the high-impact and critical-impact thresholds (Article 31).
- It allows entities to determine the scope for their risk assessments from the list of Union-wide high-impact and critical-impact processes (Article 33).
- It provides a risk-impact matrix that entities and CS-NCA use to aggregate the risks during the bottom-up risk assessment process from entity level to national level and then to regional level.

Note on definitions
Generally, the network code follows the definitions on risk assessments from ISO/IEC 27005. For instance, the network code uses “likelihood” rather than “probability”. The terms “consequence” and “impact” are however used interchangeably. ISO/IEC 27005 uses “consequence”.

The network code differs from the framework guidelines as it classifies entities only based on consequences, not based on risks (as risks are considered as a consequence in combination with likelihood). The ECII considers only the consequences of cyber-attacks because this should be the main criterion to determine what controls entities must apply. The likelihoods should not be considered.

Suppose for instance that a major TSO takes very strong security measures, so that the likelihood of a cyber-attack becomes negligible. The risk would then also be low. But the TSO should still be considered as a critical-impact entity that has to comply with the network code.

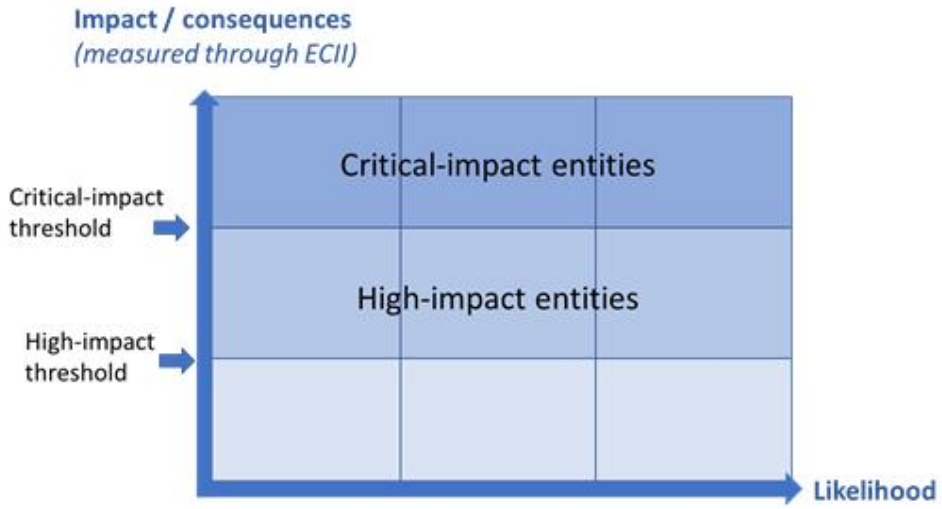


Figure 3: Classification of entities based on impact.

Other reasons not to consider the likelihood is that it is hard to measure objectively as it depends on threat information that is open to interpretation, and that the likelihood may change very quickly. If a major zero day vulnerability is discovered or a new threat actor emerges, the likelihood can increase significantly in one day. The impact measures are generally more stable.

Article 19 REGIONAL CYBERSECURITY RISK ASSESSMENT

The regional cybersecurity risk assessment integrates the results from the top-down Union-wide cybersecurity risk assessment with the bottom-up approach through the risk assessments at entity and Member State level. Based on the integrated risks, risk treatment options are selected. The risk assessment results are then reported in the cross-border electricity cybersecurity risk assessment report.

The input for the regional cybersecurity risk assessments is the assessment by each CS-NCA of the cybersecurity risks per Union-wide high-impact and critical-impact process, coming out of the Member State level risk assessments. The risks are all mapped to the same risk-impact matrix .

To help ENTSO-E and the EU DSO entity interpret these risks per process, the CS-NCAs also provides a list of threats causing the risks, and a list of recommended controls to mitigate the identified risks. .

Information on assets is aggregated on the level of business processes. In cybersecurity risk assessments, assets can be classified into (a) primary assets, such as business processes and information, and (b) supporting assets, such as hardware, software, staff, and sites. The supporting assets are very different from entity to entity.

Article 20 REGIONAL CYBERSECURITY RISK TREATMENT AND ACCEPTANCE

This article describes (a) in which timeframe the regional risk treatment plans have to be developed by ENTSO-E in cooperation with the EU DSO entity and the RCCs; (b) what these plans should include; (c) when they are to be updated.

Article 21 CROSS-BORDER ELECTRICITY CYBERSECURITY RISK ASSESSMENT REPORT

The cross-border electricity cybersecurity risk assessment report summarizes all information on cybersecurity risks, including:

- the list of Union-wide impact and critical-impact business processes identified in the Union-wide cybersecurity risk assessment;
- for each of these processes an estimate of the risk of the process being compromised from the regional cybersecurity risk assessment;
- a summary of the cyber threats and incident information from the information sharing activities (Article 38 and 39).

The report also gathers information on the status of the implementation of the cybersecurity measures and essential information flows as well as experiences from the cybersecurity exercises.

The cross-border risk assessment report contains the list of Union-wide high-impact and critical-impact business processes. In this point the network code differs from the ACER framework guideline, that was requesting a high-level risk asset inventory instead . ENTSO-E and the EU DSO entity thinks however that the processes are the right type of assets to consider at this level. Processes are more easily linked to the risks to cross-border electricity flows on a European level than more detailed supporting assets, such as systems or components.

Gathering more detailed information on assets would also require substantial effort from ENTSO-E and the EU DSO entity. Different entities will implement processes in different systems, and usually also use different names for the same systems. So, converting detailed information on assets from entities into a useful, harmonized format would require extensive analysis.

Gathering more detailed information on assets also creates a risk that this information is compromised. Especially a list of legacy systems in use would be an ideal target list for attackers.

8 TITLE IV - COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

Article 22 SCOPE OF THE COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

The ENTSO-E and the EU DSO entity will define a common electricity cybersecurity framework with the measures that the entities must take to mitigate the cybersecurity risks. The framework consists of four parts:

- minimum cybersecurity controls that shall be applied by all high-impact and critical-impact entities inside the high-impact perimeter;
- advanced cybersecurity controls that shall be applied by all critical-impact entities inside the critical-impact perimeter ;
- an electricity controls to standards mapping matrix ('ECSMM') that maps the controls from (a) and (b) to selected European and international standards and national legislative frameworks .
- cybersecurity management systems.

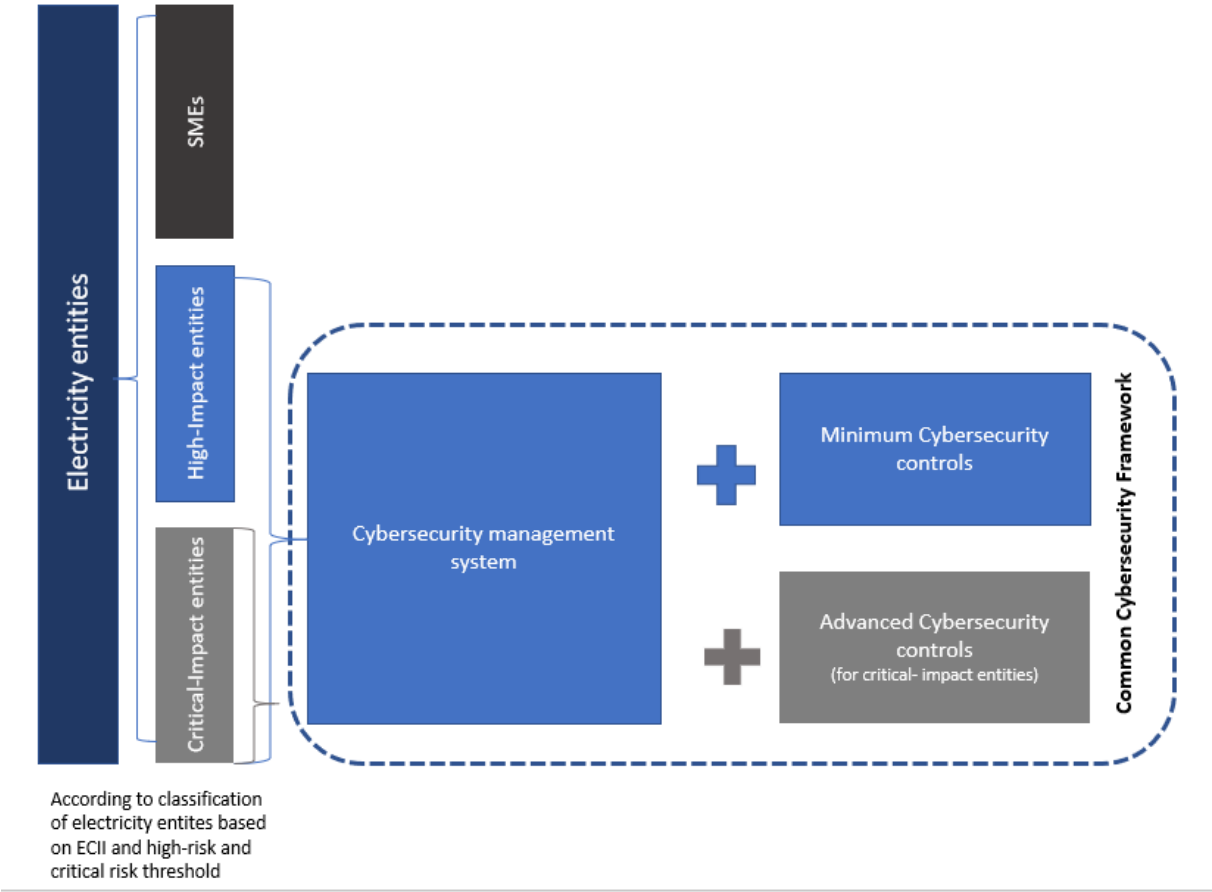


Figure 4: Scope of the common electricity cybersecurity framework.

The scope of the common electricity cybersecurity framework within an entity is determined by two perimeters (Figure 5):

- The minimum cybersecurity controls must be applied within the **high-impact perimeter** which must contain all high-impact assets and allow entities to control access to them at the perimeter.
- The advanced cybersecurity controls must be applied within the **critical-impact perimeter** which must contain all critical-impact assets and allow entities to control access to them at the perimeter.

The cybersecurity management system must cover everything inside the high-impact and critical-impact perimeters.

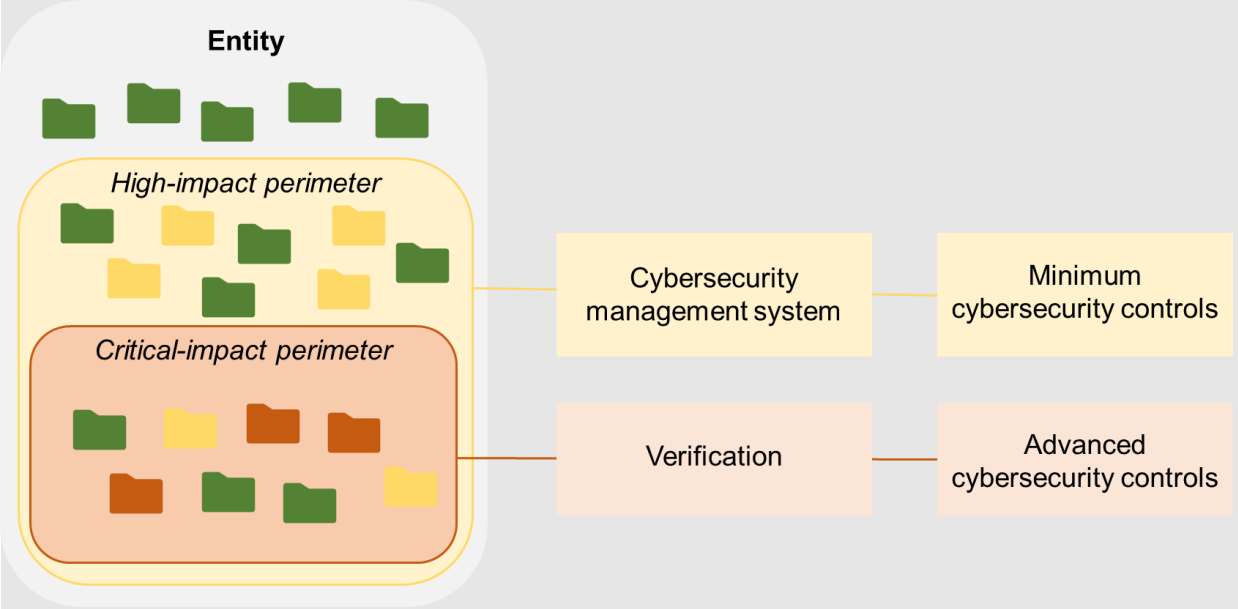


Figure 5: High-impact and critical-impact perimeters inside an entity.

Entities can determine the perimeters based on the outcomes of the Union-wide cybersecurity risk assessment as follows:

1. Identify all business processes within the entity supporting the Union-wide high-impact and critical-impact processes.
2. For each business process from step 1, determine the possible consequences if the asset is compromised using the ECII. This step is performed as part of the risk assessment at entity level (Article 33).
3. If the ECII is above the high-impact threshold, the process is considered high-impact. If the ECII is above the critical-impact threshold, the process is considered critical-impact.
4. Determine all the high-impact assets as the assets needed for the high-impact processes, and critical-impact assets as the assets needed for the critical-impact processes.
5. Determine the high-impact perimeter containing all high-impact assets, and the critical-impact perimeter containing all critical-impact assets, so that access control can be applied at the boundaries.

The perimeters in step 5 can be both physical and logical. The physical perimeter would usually consist of walls, fences, doors, and gates surrounding the high-impact or critical-impact assets. The logical perimeter would consist for instance of firewalls, gateways, proxy servers, and stepping stones.

Note that the high-impact and critical-impact perimeters may contain assets that are not needed for high-impact and critical-impact processes. The minimum cybersecurity controls still apply to these assets. Similarly, the critical-impact perimeter may contain high-impact assets. The advanced cybersecurity controls still apply to these assets.

Critical-impact entities may have separate high-impact and critical-impact perimeters. The critical-impact perimeter would be contained within the high-impact perimeter.

Within 12 months after the finalisation or update of the minimum and advanced cybersecurity controls, all entities listed in Article 2(1) shall during the risk treatment step apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Article 23 DEROGATIONS FROM THE MINIMUM AND ADVANCED CYBERSECURITY CONTROLS

The NCCS recognises that there may be a need for temporary derogations from some of these controls. The entity that has identified a need for a derogation may file a request for derogation to its NRA and CS NCA, when it can demonstrate the costs of implementing the appropriate cybersecurity controls significantly exceed the benefits; or when it can provide a risk treatment plan demonstrating how the remaining risk is mitigated. .

Article 24 VERIFICATION OF THE COMMON CYBERSECURITY REQUIREMENTS

Based on the ACER framework guideline, the Network Code shall ensure 3 possible ways of verification for the implemented controls:

1. Verification through third party certification by a conformity assessment body;
2. Verification by a peer review process by a critical-impact entity;
3. Inspections by the CS-NCA or NRA based on a framework of legal obligations.

The last two options are implemented through the national verification schemes defined in Article 32.

As the Network Code on Cybersecurity shall ensure a minimum level of cybersecurity in all Member States, the verification through third party certification is the most appropriate. Cybersecurity audits performed by independent third-parties are necessary to eliminate any conflicts of interest during the audit.

Using a third party to conduct audits allows for fresh eyes and a different approach to research, review and analyse the entities' security controls. A well prepared and well executed audit can make a substantial difference in the prevention of cybersecurity incidents.

In general, the audit process should explicitly ensure a comparable duration and depth, a comparable quality and the independency of the audit. Only by ensuring the mentioned points a comparable baseline standard for the audits can be ensured.

Regulators should be allowed to choose a verification framework for the legal obligations or the peer-review in their country but they have to ensure and constantly proof that the quality is equivalent to a certification by a third party.

Article 25 CYBERSECURITY INSPECTIONS

Besides verifying the implementation of the common electricity cybersecurity framework through the options described in Article 24, CS-NCA can also perform inspections or request additional information to assess the cybersecurity measures taken by an entity. Measures for supervision or for enforcement imposed on critical-impact entities and high-impact entities have to be effective, proportionate and dissuasive, considering the circumstances of each individual case.

Article 26 CYBERSECURITY MANAGEMENT SYSTEM

The network code requires that all entities set up a cybersecurity management system system (ISMS, e.g. based on ISO/IEC 27001) to manage the cybersecurity risks and the implementation of cybersecurity controls. Requiring a management system is expected to be more effective and cost-efficient than only requiring the implementation of the minimum and advanced cybersecurity controls. These cybersecurity management systems are more effective because it makes top management at entities explicitly responsible for managing cybersecurity risks and for the effectiveness of the cybersecurity controls. It also defines policies, methodologies, processes and tools to ensure sustainable information security within the entities. This includes the introduction of specific procedures and the implementation of organizational measures that must be continuously controlled, monitored, and improved.

The cybersecurity management system ensures the continuous improvement of cybersecurity. Such a loop is needed to ensure that entities maintain their target level of security in the long run, especially in larger organizations that can have problems in implementing controls. Policies will not always be followed, or they may not achieve their intended goals. Incidents may show that important controls were missing. Entities must have a structural way, as well as processes to deal with such problems, and to involve their management to ensure that the necessary resources are available for these tasks.

The cybersecurity management system is more cost-efficient because audit time can be reduced as audits would focus on the correct and effective implementation of the cybersecurity management system itself. If the management system is working well, it will over time ensure the effective implementation of the cybersecurity controls.

The network code includes general requirements to a cybersecurity management system, mainly derived from the ISO/IEC 27001 standard. The network code does however not require that this standard is followed. Cybersecurity management systems based on other standards can be considered if they meet these requirements.

Article 27 MINIMUM AND ADVANCED CYBERSECURITY SUPPLY CHAIN SECURITY CONTROLS

Supply chain security risks are a major threat to the electricity sector and are expected to increase in the coming years. The Network Code therefore includes special measures on both sides for the entities as well as for critical service providers to address these risks. The controls in Article 27 shall be applied by all high-impact and critical-impact entities excluding the critical service provider. Specific measures for critical service providers are listed in Article 28.

To ensure that the supply chain risks and respective controls are adopted to current threats, three mandatory measures are included in the network code:

- Supply chain threats are considered in the regional cybersecurity risk assessment and entity-level risk assessment;
- Based on the regional cross-border risk assessment, high-impact and critical-impact entities must implement supply chain security controls as part of the minimum and advanced cybersecurity controls;

- Critical service providers must take specific measures to ensure supply chain security (Article 28).

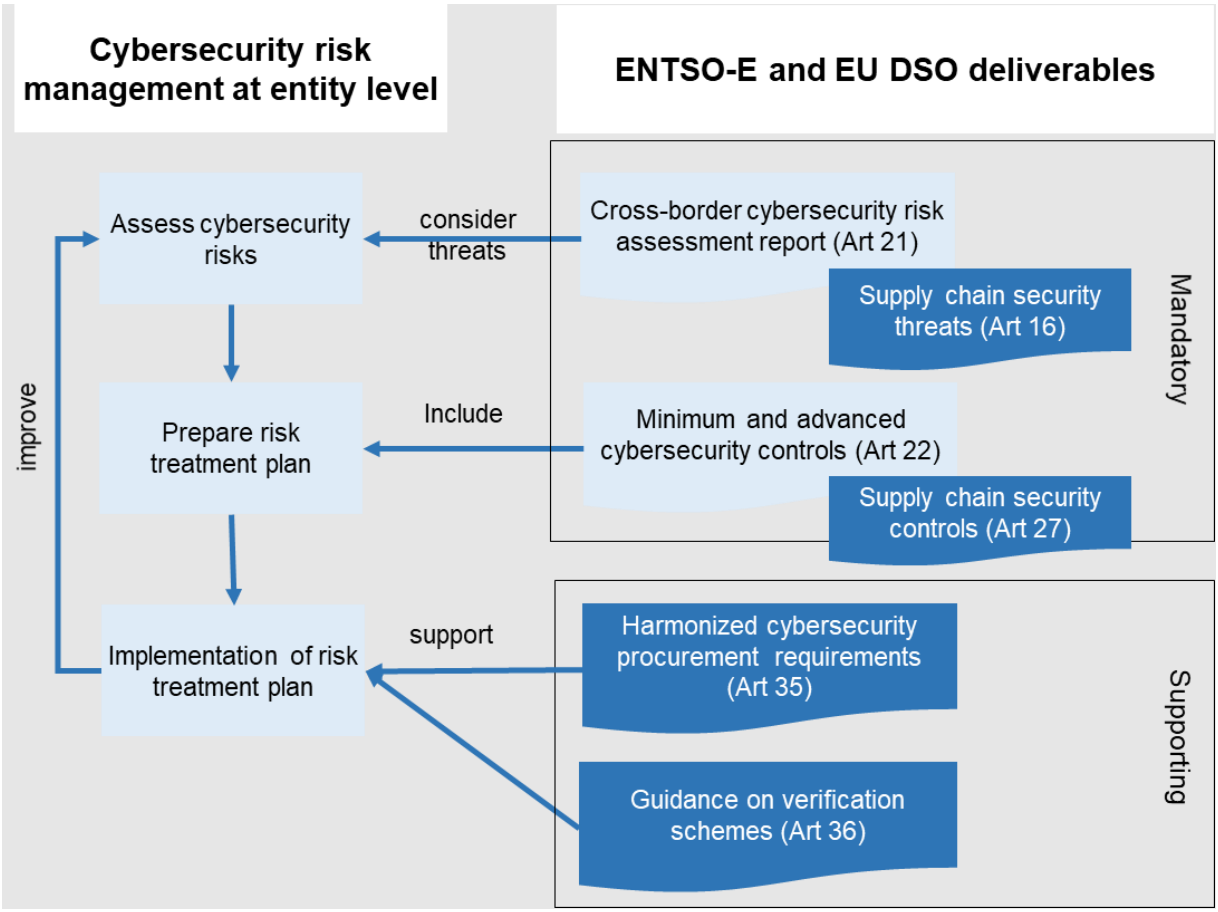
Additionally, to support the implementation of the supply chain security controls at entity level, ENTSO-E and the EU DSO entity will develop harmonized security requirement sets and guidance on European cybersecurity certification schemes. 11

The measures have been integrated in the risk assessments and common electricity cybersecurity framework as shown in Figure 6, so that they can be implemented with limited additional effort.

Note on definitions

The network code sections on supply chain security uses the definitions of *ICT products*, *ICT services*, and *ICT processes* from the Cybersecurity Act. These definitions also cover products, services, and processes for OT systems, such as SCADA systems, substations and distribution automation systems, or smart metering systems. These definitions are used to build upon existing legislation.

The network code does not explicitly distinguish between IT and OT systems. Different entities use different definitions from "IT" and "OT", and generally the borders between the two are blurry. OT systems are more often more affected by problems with legacy equipment. These problems can however be resolved during implementation of the controls. For instance, the minimum and advanced cybersecurity controls can follow ISO/IEC 27019 and IEC 62443 for OT systems. The harmonized cybersecurity procurement requirements can include specialized requirement sets for OT equipment.



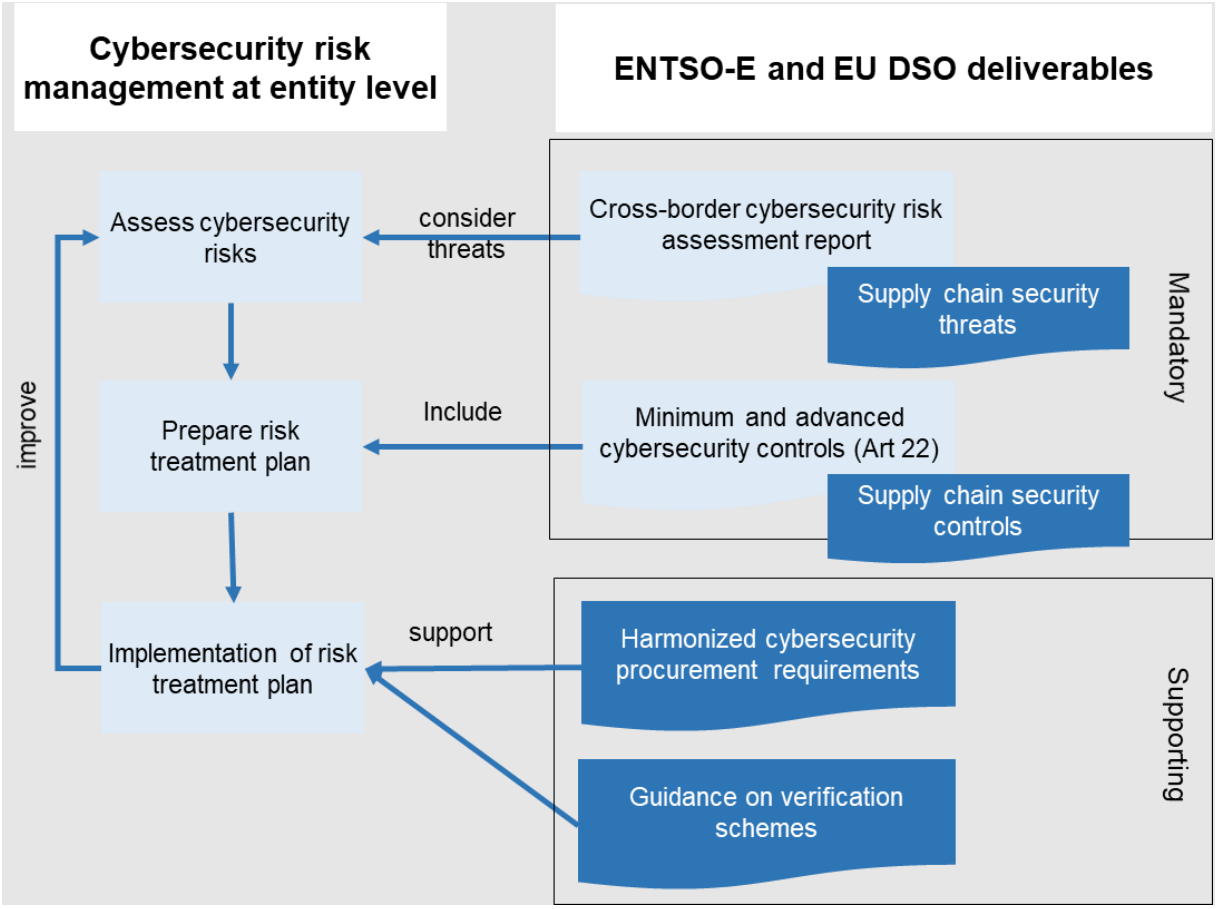


Figure 6: Cybersecurity supply chain security controls in the network code.

Supply chain threats are considered at two levels. ENTSO-E and the EU DSO entity must consider supply chain threats when they conduct the regional cybersecurity risk assessments. The methodology for these assessments will include a list of such cyber threats . Article 16 includes supply chain threats that must be included in this list. The list is based on the threats identified by in the ACER framework guidelines, and extended with the input of the drafting committee and of stakeholders during the public consultation.

High-impact and critical-impact entities must consider supply chain threats in their own risk assessments. The entities are required to implement the common supply chain security controls, as explained below. But these controls may not be enough to mitigate their supply chain risks, for instance because an entity has to deal with highly motivated threat actors or because a supply chain incident would have extreme impact. In that case, the entity will be required to take additional entity-specific controls to mitigate the risks.

A list of supply chain threats that entities must consider will be provided in the cross-border electricity cybersecurity risk assessment report. Note that the report will not available for the first risk assessment at entity level, as the report is prepared later in the risk assessment cycle. So, in the first risk assessment cycle after the transition period, the entities should consider supply chain security threats, but without having a prescriptive list of certain threats . In the following cybersecurity risk assessment cycles, entities can use the cross-border electricity cybersecurity risk assessment report that came out of the previous cybersecurity risk assessment cycle. The minimum and advanced cybersecurity controls will include supply chain controls. The supply chain security controls concern organizational measures that high-impact and critical-impact entities must take when procuring new ICT products, ICT services, or ICT processes.

The regional cross-border risk assessments will result in a set of updated minimum and advanced supply chain security controls. These controls will be revised every three years as part of the regional risk assessments. Hence, they can be adjusted to counter new threats or use newly developed security measures. But these controls may not be enough to mitigate the supply chain risks of an entity, for instance because an entity has to deal with highly motivated threat actors or because a supply chain incident would have extreme impact. In that case, the entity will be required to take additional entity-specific controls to mitigate the risks.

The controls do not contain technical requirements to the ICT products, ICT services, or ICT processes. They only require entities to define, use and verify such requirements during procurement. Entities may define their own technical requirements suitable to their specific situation, based on the entity-level risk assessments. Harmonized technical requirements are developed by the ENTSO-E and the EU DSO entity to support entities in this task and make it easier and more cost-effective to procure secure equipment. 0Entities may however define their own technical requirements suitable to their specific situation. For instance, they may set additional requirements based on the entity-level risk assessments.

To ensure completeness, the supply chain security controls shall cover the controls listed in Article 27(2). The controls are based on the ACER framework guideline, and cover the entire procurement process for high-impact and critical-impact entities as shown in Figure 7.

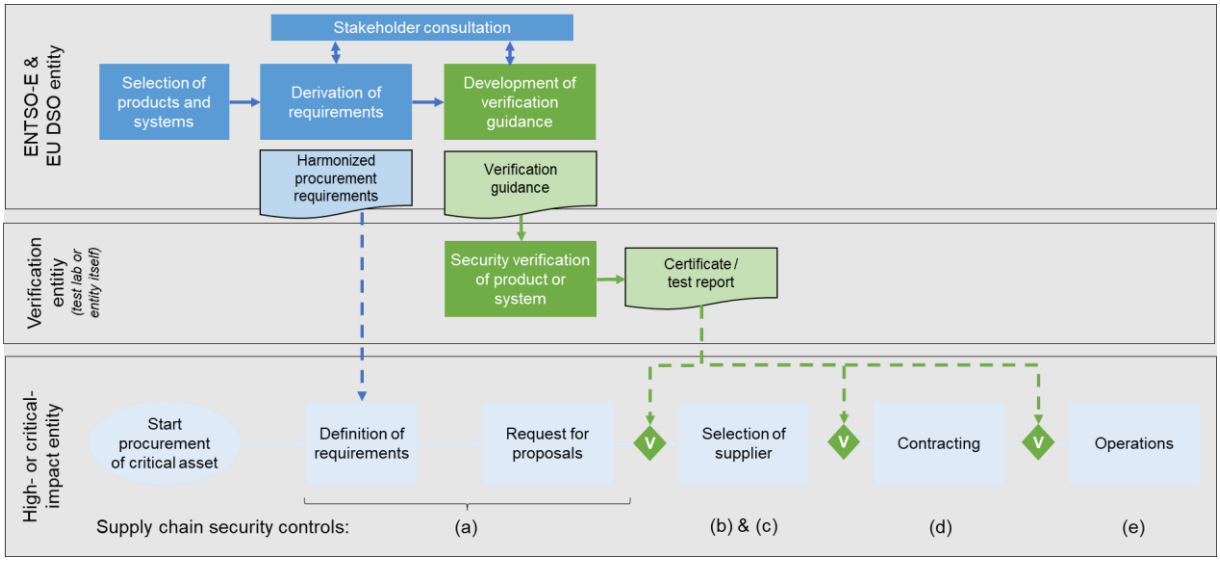


Figure 7: Supply chain security controls in the network code mapped to the procurement process at a high-impact or critical-impact entity. The letters in the lowest row refer to the topics in Article 27 (2) Verification steps are in green and are only mandatory for critical-impact entities. Possible verification steps are marked with a green 'V'.

The supply chain security controls require that critical-impact entities verify the implementation of the security requirements to ICT products, ICT services, and ICT processes that will be used as critical-impact assets. They may apply verification at different steps in the procurement process (see Figure 7), as long as they verify the product or system before they take it into operation.

Verification may be done through the European cybersecurity certification schemes that are being developed by ENISA under the Cybersecurity Act. If a suitable European certification scheme will become available, products can become certified, which would make the procurement and verification process of entities much easier. ENTSO-E and the EU DSO entity will support critical-impact entities in applying the certification schemes by developing sector-specific guidance 11.

The European cybersecurity certification schemes are under development. Certified ICT products, ICT services, and ICT processes will likely not be available for all types of critical-assets for several years. Hence, critical-impact entities are also allowed to select and organize their own verification activities, such as penetration testing, self-assessments, functional testing, review, or audits. Verification may be performed at different steps in the procurement process (see Figure 7), as long as they verify the product or system before they take it into operation.

Critical-impact entities must however ensure that the verification activities are sufficient to provide assurance that the ICT product, ICT service or ICT process can be used to mitigate the risks identified in the risk assessment at entity level. For penetration testing, this would for instance mean that all high-impact cyber threats are included in the scope of the test, and that the time allocated to the test is in line with the level of the threat actors the asset should be resilient to.

Article 28 SECURITY MEASURES FOR CRITICAL SERVICE PROVIDERS

Critical service providers are key to improving cybersecurity in the electricity sector. Supply chain attacks originate at the level of the critical service provider and could simultaneously affect a high number of different entities within the scope of the network code. Thus, these cyber attacks could pose a high risk for cross-border electricity flows. For this reason, Article 28 lists specific measures that are to be implemented by critical service providers. These specific measures should preventively increase the security of the ICT-product, ICT-service and ICT-process , reduce detection and response times at entity level and increase the cybersecurity in mitigating supply chain attacks.

Note on definitions

The network code includes under critical service providers not just providers of ICT services and ICT processes, but also of ICT products; i.e. manufacturers of smart grid equipment or software companies also fall under this category. Critical service providers are the providers needed for the critical-impact processes.

The security measures for critical service providers have the following key objectives:

- Implementation of processes for secure design, development and production to enhance the security level of provided products;
- Implementation of vulnerability management to reduce the time to detect any relevant vulnerability and to react by providing support to the operating entity;
- Protection of customer assets and information to mitigate threats mainly by insider attackers.

The network code treats critical service providers as a separate category, distinct from entities. The general requirements for critical-impact entities do not apply to critical service providers. Instead, explicit requirements are included in Article 28.

The expansion of the scope to include also critical service providers may affect many (worldwide) service providers. Concerns were raised during the public consultation that strong requirements on critical service providers could damage the competitiveness of European companies. The network code mitigates these risks in the following way:

- The intervention in the market is reduced by the restrictive definition of critical service provider in this network code. Only if a compromise of the ICT product, ICT service or ICT process may result in an incident for a critical-impact process, the service provider is considered as being a critical service provider. In this sense, non-critical subcomponents of a critical-system are not included in the scope of Article 28.

- Within the critical service provider, the implementation of these specific measures is limited to risks for critical-impact processes.
- The identification of critical service providers is done by objective criteria through the entities and reported in a confidential way in the risk assessment report (article 34).

The requirements included in the network code for critical service providers are based on several sources, including IEC 62443-2-4, and IEC 62443-4-2, the recommendations in the ENISA report on the *Threat Landscape for Supply Chain Attacks*, and responses in the public consultation.

Article 29 ELECTRICITY CONTROLS TO STANDARDS MAPPING MATRIX

ENTSO-E and the EU DSO entity supported by the working group will provide mappings in the ECSMM from the minimum and advanced cybersecurity controls to other European and international standards commonly used in the electricity sector. The mapping will make it easier for high-impact and critical-impact entities to apply the controls.

The CS-NCAs and NRAs may provide mappings from the minimum and advanced cybersecurity controls.that are part of national regulation to ENTSO-E and the EU DSO entity in order to include them in the ECSMM. ENTSO-E and the EU DSO entity will not develop such mappings themself, as it does not have the resources and legal expertise to do this for all Member States.

9 TITLE V - RISK MANAGEMENT AT MEMBER STATE LEVEL

At Member State level the CS-NCA are responsible for managing the risk by performing two main activities. Derived from the top-down assessment, CS-NCA must identify critical risk entities using the output of the Union-wide cybersecurity risk assessment on high-impact and critical-impact processes and ECII. The second activity is to perform a Member State risk assessment with the input received from the entity risk assessments.

Article 30 MEMBER STATE CYBERSECURITY RISK ASSESSMENT

The national cybersecurity risk analysis aggregates the risk assessments of all high-risk and critical-risk entities in the Member State, so that the results can be used in the regional cybersecurity risk assessments.

The main input to the analysis is from each entity an estimate of the cybersecurity risks to each Union-wide high-risk and critical-risk process. All risks are mapped to the same harmonized risk matrix . Additionally, the entity will provide a summary of threats, existing controls and vulnerabilities.

To be able to have a complete overview over the current risk situation in Europe, the CS-NCAs supported by the CSIRTs collect information about the risks, security incidents, and the current implementation status of the existing cybersecurity controls.

The information gathered is minimized to what is needed for the regional risk assessment. Gathering more information by default would increase the risk of sensitive information leaking. CS-NCA and NRA can always request information from entities, if needed.

The information in the report shall not be linked to specific entities or assets in the report. The estimate of the risk shall be given as an estimate of the consequences and likelihood according to the risk-impact matrix.

Article 31 IDENTIFICATION OF HIGH-IMPACT AND CRITICAL-IMPACT ENTITIES

Based on the Union-wide cybersecurity risk assessment, the CS-NCAs identify the high-impact and critical-impact entities or a group of entities as a whole which can cause a significant impact.

The CS-NCA and NRA can create a list of potential high-impact and critical-impact entities based on the list of Union-wide high-impact and critical-impact processes.

The CS-NCA then need to determine which of these entities are high-impact and critical-impact by determining their ECII. If the information needed to calculate the ECII is already available to the CS-NCA, they can determine the ECII themselves. Otherwise, they will need to request additional information from these entities. They could also ask the entities themselves to calculate the ECII and then validate the results.

The CS-NCA notify entities when they have been identified as high-impact or critical-impact, so that the entities know that they need to implement the minimum or advanced cybersecurity controls.

Article 32 NATIONAL VERIFICATION SCHEMES

The entity shall verify compliance through (a) certification or an audit by an independent conformity assessment or (b) a national verification scheme.

The verification scheme can be developed by the CS-NCA and the NRA and can be conducted through peer reviews or through inspection and supervision by the CS-NCA and the NRA.

The verification schemes can be used to integrate existing supervision methodologies by the CS-NCA, for instance developed for the NIS Directive. Requirements are included on the schemes to ensure they provide the same level of assurance as certification by a conformity assessment body. These requirements are based on international standards for audits and certification, in particular ISO/IEC 17021 and ISO/IEC 27006.

10 TITLE VI - RISK MANAGEMENT AT ENTITY LEVEL

Article 33 CYBERSECURITY RISK MANAGEMENT AT ENTITY-LEVEL

The minimum and advanced cybersecurity controls should mitigate the cybersecurity risk of a typical high-impact or critical-impact entity; but each entity may face risks specific to their situation that are not sufficiently mitigated by these controls. The network code therefore requires all high-impact and critical-impact entities to perform their own cybersecurity risk management. At entity level, all high-impact and critical-impact entities must implement cybersecurity risk management.

The network code only sets requirements to the cybersecurity risk assessment methodologies at entity level. It does not require that entities to use a specific methodology.

Requiring a specific cybersecurity risk assessment methodology would lead to disproportional costs. Most entities are already performing cybersecurity risk assessments. Many are required to do so under the NIS Directive. Requiring the entities to use a specific methodology would require entities to train their staff for a new methodology and to carry out the risk assessments, that they have already performed, again.

For the effectiveness of the network code, it is however critical that entities perform the cybersecurity risk assessments in the right way. Entities need to reliably identify and assess the risks to select the right security controls. CS-NCA need reliable and consistent information to be able to perform the risk analysis at national level.

The network code ensures the reliability and consistency of the cybersecurity risk assessments at entity level through two requirements:

- Requirements on the cybersecurity risk assessment steps derived from the ISO/IEC 27005:2018 standard. These requirements ensure that entities perform all the steps needed to properly assess the risks.
- A requirement that all risks are mapped to a risk impact matrix in the Union-wide cybersecurity risk assessment. The matrix ensures that all relevant consequences are analysed using objective measures. It also ensures that CS-NCA get consistent cybersecurity risk assessment reports from the entities, so that they can more easily assess the cybersecurity risks at national level.

The risk assessment methodologies at Union, regional, and Member State level will also be based on ISO/IEC 27005. So, the methodologies at all levels will be similar, as required by the ACER framework guideline.

Article 34 REPORTING ON THE RISK ASSESSMENT AT ENTITY LEVEL

Entities must report the outcomes of their risk assessments to the CS-NCA. The risks are aggregated on the level of Union-wide high-impact and critical-impact processes. In this way, entities only report aggregated information needed for the risk assessment at Member State level. More detailed risk information is not reported, as it could be highly sensitive.

Information about the implementation of controls is reported as input for the cross-border electricity cybersecurity risk report.

Critical-impact entities also notify their critical service providers to the CS-NCAs .

11 TITLE VII - HARMONISED CYBERSECURITY PROCUREMENT REQUIREMENTS

To support high-impact and critical-impact entities in implementing the supply chain security controls, the network code tasks the ENTSO-E and the EU DSO entity, supported by the cybersecurity risk working groups, to develop:

- harmonized security requirement sets for products and systems;
- guidance on European cybersecurity certification schemes to determine if a product or system meets these requirements.

Article 35 HARMONIZING SECURITY PROCUREMENT REGUIREMETNS FOR ICT PRODUCTS, ICT SERVICES AND ICT PROCESSES

Article 27 requires high-impact and critical-impact entities to define cybersecurity procurement requirements for their ICT products, ICT services and ICT processes. Defining such requirements often requires significant effort. Entities need to analyse the possible threats , and select measures to mitigate them. These measures should take into account what is currently feasible in the market, often requiring entities to do a market consultation or a Request for Information.

Article 35 tasks ENTSO-E and the EU DSO entity with developing harmonized cybersecurity procurement requirements sets that the entities may use as a basis for their product security requirements in the procurement phase. In this way, entities can more easily and efficiently fulfil their obligations under Article 27. Moreover, the harmonized requirement sets are created, by providing elaborated and reviewed requirement sets that have been reviewed by many experts notably from TSOs, DSOs, industry, ENTSO-E and the EU DSO entity. By using these harmonised requirement sets during procurement, high-impact and critical-impact can be sure to request effective and suitable security features. Thus, the ore entities can use harmonised security procurement requirements the higher the level of cybersecurity in the electricity sector.

During the preparation of the network code, different ways were considered to support entities in procuring ICT products, ICT services and ICT processes respecting the supply chain security controls as defined in Article 27. These include the development of procurement protocols and templates, and the possibly mandatory use of a European certification scheme.

ENTSO-E and the EU DSO entity have opted for harmonized cybersecurity procurement requirements as this is the easiest and most cost-effective way to support entities in procuring secure ICT products, ICT services and ICT processes. Entities can integrate these requirement sets into their procurement processes without major changes. Procurement templates and protocols would be more difficult to integrate, as they could require amendments to national laws and changes in the procurement strategies of entities.

As these requirement sets are aligned with the cybersecurity controls and reviewed by all relevant stakeholders it can be expected that many if not all entities use them. A survey by ENTSO-E has shown that many TSOs are already trying to use existing documents and standards, such as IEC 62443 and the BDEW Whitepaper, in procurement. When entities will be required to use cybersecurity procurement requirements, many can be expected to look for such ready-made sets.

Harmonizing the security requirement sets in the electricity sector will lower development costs, as suppliers get a clear direction for their security roadmaps. They only need to implement the requirements once for all entities using them. So, products and systems meeting the requirements should become

readily available at competitive prices. Entities will hence be further encouraged to use such requirements.

ENTSO-E and the EU DSO entity will create a public document with requirements that entities can use directly in their procurement documents, such as requests for proposals. Entities could either copy the requirements to their documents or add a reference to the ENTSO-E and the EU DSO entity document. To allow entities to use the requirement sets with minimal (or preferably no) modifications, the sets would be developed for specific products or systems, such as SCADA systems, RTUs, IEDs, or cloud platforms.

Working with representatives of all critical-impact entities, ENTSO-E and the EU DSO entity will select products and systems for which they will develop requirement sets . Significant effort is required to develop such requirements and verification schemes. So, it will not be possible to cover all products and systems in the critical-impact perimeter. The number of products and systems covered will grow over time.

The harmonized cybersecurity procurement requirements sets will not be updated every risk assessment cycle. This would likely require too much effort for ENTSO-E and the EU DSO entity to develop the requirements, and for suppliers to adapt to the new requirements every three years. The requirements sets should only be updated if there are major changes in the risks or technologies.

The ENTSO-E and the EU DSO entity will first define a reference architecture describing the products and services at critical-impact entities. The goal is to agree on a common naming for products and systems. Different entities and suppliers often use different names for similar products and systems. The IEC 62351 standard and the SGAM model, used in the cross-border risk assessment, can be the basis for the reference model.

Based on a consultation with critical-impact entities through a questionnaire or workshops, candidate products and systems will be selected.

The candidates are then analysed on how beneficial it would be to have harmonized requirements. This analysis involves multiple factors, such as:

- the criticality of the product or system according to the Union-wide cybersecurity risk assessment and the regional cybersecurity risk assessment;
- the cost of security for the product or system;
- the possible savings in harmonization, depending for instance on the degree of customization for entities and the number of suppliers in the market.

The ENTSO-E and the EU DSO entity will then make a proposal for the products or systems to work on, consulting relevant stakeholders in the cybersecurity risks working group and cybersecurity risk monitoring body.

The ENTSO-E and the EU DSO entity will then create a set of security requirements for the selected product or system based on the union-wide cybersecurity risk assessment and the regional cybersecurity risk assessments. Requirements are selected that allow entities to sufficiently mitigate the identified threats and that allow them to implement the common controls. If the controls for instance require entities to monitor the security of a system, the security requirements should ensure that the system generates and exports the necessary logs.

Requirements will be selected as much as possible from international standards or other sources already in use in the sector, such as:

- IEC 62443-2-4 and the BDEW Whitepaper for requirements to system integrators;
- IEC 62443-3-3 and the BDEW Whitepaper for requirements to systems;
- IEC 62443-4-1 for secure software development requirements;

- IEC 62443-4-2 for technical requirements to products;
- IEC 62351 for interoperability requirements in systems using the IEC 60870-5-104, ICCP or IEC 61850 protocols;
- ISO/IEC 27001 for securing supplier assets and infrastructure;
- ISO/IEC 15408 (Common Criteria) for components or parts with high assurance requirements.

ENTSO-E and the EU DSO entity will follow a holistic approach focusing on the security of the entire system rather than individual components, as described in the SGTF EG2 recommendation[2]. The procedure will be to develop a defence-in-depth architecture for the systems used in critical-impact processes. This architecture should take into account the business requirements and the processes used by the system. It should also take into account the security restrictions seen in operational technology systems, such as real-time requirements and the need to integrate legacy systems. Requirements for components are derived from the architecture.

Another advantage of the harmonised requirement sets is that they can also be used as the basis for subsequent certification of products. The requirements sets provide input for the protection profiles for certification schemes because they are reviewed, approved and used by many entities and based on the outcomes of different risk assessments.

ENTSO-E and the EU DSO entity will involve industry from an early stage to ensure that the certification approach is feasible. Industry associations and suppliers of the ICT product, ICT service, or ICT process, will be involved in workshops and asked to review the documents. Where needed ENTSO-E and the EU DSO will coordinate with other stakeholders, such as ENISA and European or international standardization bodies.

ENTSO-E and the EU DSO entity will start developing the requirements sets and schemes when the network code enters into force. They will gradually develop them for more products and systems. If no requirement set is available for a product or systems, high-impact and critical-impact entities are expected to developed their own requirements. They can use international standards or adapt a harmonized requirement set for another product or system.

Article 36 GUIDANCE ON EUROPEAN CYBERSECURITY CERTIFICATION SCHEMES FOR ICT PRODUCTS, ICT SERVICES AND ICT PROCESSES

Article 24 requires that critical-risk entities verify ICT products, ICT services, and ICT processes against the cybersecurity procurement requirements before they are taken into operations as critical-impact assets. Entities may organize their own verification activities, such as penetration tests or self-assessments. But defining the right activities, requires substantial technical knowledge. The verification activities often need to be performed by external auditors or testing companies, often at high cost. Moreover, entities are often testing the same ICT product, ICT service, or ICT process without knowing it.

Therefore, Article 36 tries to streamline the verification by tasking ENTSO-E and the EU DSO to develop guidance on European cybersecurity certification schemes. Certification of products ensures that there are clear verification activities for each requirement set. Tests and audits only need to be performed once for all entities using a product or system. Entities also know before selecting a product that it has been verified against the requirements, so that they are sure that they get a secure product.

[2] Smart Grid Task Force Expert Group 2: "*Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management*", June 2019. Section 7.2.5.

European cybersecurity verification schemes will be used for harmonization, as they would offer the greatest cost reduction and would benefit from the certification infrastructure that the ENISA and the EU are creating. ENTSO-E and the EU DSO entity would provide guidance on how to apply these certification schemes in the electricity sector.

The guidance could take two forms:

- a profile extending the certification scheme to ICT products, ICT services and ICT systems used by critical-impact entities. Examples of such profiles would be protection profiles for the EUCC scheme[3] ("Common Criteria") or a generic Component Context Analysis for the *Industrial Automation & Control Systems Components Cybersecurity Certification Scheme* under development by the Joint Research Centre, or the profiles under development for IEC 62443. The profile would include the harmonized cybersecurity procurement requirements for the ICT product, ICT service, and ICT system together with requirements on how it should be evaluated.
- guidance on how a product should be evaluated. They could require certain types of tests to be performed, certain threats to be considered in penetration testing, or set rules for assessing the exploitability of vulnerabilities found. The SOG-IS group has been successful with this approach in applying Common Criteria to smart cards.

When developing the guidance, ENTSO-E and the EU DSO entity will work closely together with ENISA. They will involve industry from an early stage on to ensure that the certification approach is feasible. And where needed they will coordinate with other stakeholders, such as test labs and European or international standardization bodies.

[3] Common Criteria based European candidate cybersecurity certification scheme

12 TITLE VIII - ESSENTIAL INFORMATION FLOWS, CYBERSECURITY INCIDENT AND CRISIS MANAGEMENT

The network code strives to take utmost into account existing legislation and structures, in particular provisions of the NIS Directive, in order to avoid overlaps. Therefore, the network code refers, whenever possible, to existing legislation and national and Europeans structures .

Article 37 SCOPE OF TITLE VIII

Article 37 describes the possible alignment with the national legislation to implement the NIS Directive

Article 38 ROLE OF PUBLIC AUTHORITIES CONCERNING INFORMATION SHARING

About CSIRT-NCA

The NIS Directive stipulates that the Member States shall designate which national body - the CSIRT or the CS-NCA is in charge of the information exchange . As Member State implementation differs across the Union, therefore the NCCS refers to :

‘CSIRT-NCA’ meaning the CSIRT or the CS-NCA when designated by the Member State as the authority to whom entities shall notify incidents or cyber attacks pursuant to Article 14(3) of Directive (EU) 2016/1148.

About methodology and timelines

CSIRT are not required to work 24/7. Thus, among the three categories of information that CSIRT should share (Art.38(3, 4 or 5)), only reportable cybersecurity incidents are to be shared within 18 hours from receipt of the information.

The NCCS foresees stricter timelines for sharing information on reportable cybersecurity incidents than NIS Directive in order to adapt the information sharing to the need of the electricity sector where information sharing is in many cases close to real time.

Reportable cybersecurity incidents are incidents with the most serious impact leading to a cross-border electricity crisis (level 2 or 3 according to ENTSO E's incident classification scale methodology - level 3 meaning full blackout in Europe). The methodology to determine which cybersecurity incident will have to be considered as a reportable cybersecurity incident will be developped by ENTSO-E and the EU DSO entity in cooperation with ENISA and CSIRT (Art. 38(7)) within 12 months after the entry into force of the network code.

The cybersecurity incident classification scale methodology will include provisions to analyse:

1. the criticality of the asset perimeter concerned by the incident: the critical-impact perimeter could be a possible criterion (i.e. the perimeter including assets that could lead to a level 2 or 3 cross-border electricity crisis if they are corrupted); and

Scale 0 Noteworthy incident		Scale 1 Significant incident		Scale 2 Extensive incident		Scale 3 Major incident / 1TSO	
Priority/Short definition (Criterion short code)		Priority-Short definition (Criterion short code)		Priority-Short definition (Criterion short code)		Priority-Short definition (Criterion short code)	
#20	Incidents on load (L0)	#11	Incidents on load (L1)	#2	Incidents on load (L2)	#1	Blackout (OB3)
#21	Incidents leading to frequency degradation (F0)	#12	Incidents leading to frequency degradation (F1)	#3	Incidents leading to frequency degradation (F2)		
#22	Incidents on transmission network elements (T0)	#13	Incidents on transmission network elements (T1)	#4	Incidents on transmission network elements (T2)		
#23	Incidents on power generating facilities (G0)	#14	Incidents on power generating facilities (G1)	#5	Incidents on power generating facilities (G2)		
		#15	N-1 violation (ON1)	#6	N violation (ON2)		
#24	Separation from the grid (RS0)	#16	Separation from the grid (RS1)	#7	Separation from the grid (RS2)		
#25	Violation of standards on voltage (OV0)	#17	Violation of standards on voltage (OV1)	#8	Violation of standards on voltage (OV2)		
#26	Reduction of reserve capacity (RRC0)	#18	Reduction of reserve capacity (RRC1)	#9	Reduction of reserve capacity (RRC2)		
#27	Loss of tools and facilities (LT0)	#19	Loss of tools and facilities (LT1)	#10	Loss of tools and facilities (LT2)		

2. the severity, the depth and the surface of the cyber attack by answering the following questions:
    a. What is the position of the cyber attack in the kill chain? E.g. the knowledge base of MITRE ATT&CK could be useful.
    b. How many assets are providing the same service? Are they all corrupted? How could other similar assets be corrupted?

The methodology should mix both approaches to determine whether the incident should be classified as a reportable incident:

		Critical asset			
		Scale 0 Noteworthy incident	**Scale 1** Significant incident	**Scale 2** Etensive incidents	**Scale 3** Major incident
MITRE ATT&CK	**Reconnaissance** **Ressource Development** **Initial access**	Medium	Medium	To follow	Important
	Execution **Persistence**	To follow	To follow	Important	High
	Privilege escalation **Defense Evasion** **Credential access** **Discovery**	To follow	Important	High	Critical
	Lateral Movement **Collection**	Important	High	Critical	Critical
	Command and control **Exfiltration** **Impact**	High	Critical	Critical	Critical

Only the riskiest incidents with possible effects on cross-border electricity flows will be reported. It is to be expected that there are only a few incidents in Europe each year with possible cross-border effect. But in such eventuality, CSIRTs are expected to be ready to provide a massive response to support

quickly critical-impact entities, whenever it will be necessary. Depending on the inherent risk, the reaction within Europe should be the same in each Member State and involving all CSIRTs.

The NCCS sets out the following principles:

- Alert (Art. 38(3)(d)): The CSIRT impacted shall share to the CSIRT Network the information within eighteen (18) hours;
- Investigate (Art. 38(3)(b)): The CSIRT shall be responsible for proactively verifying and finding any other similar incident in the Union reported to other CSIRTs, to correlate information in order to eventually enrich existing information as well as strengthen and coordinate cybersecurity responses.;
- Protect (Art. 38(4) and Art. 38(3)(c)): The CSIRT shall not disseminate information and withhold it as long as the information constitutes a high risk and could harm, hinder or disrupt the investigation of an ongoing cyber-attack; and
- Prevent (Art. 38(3)(e)): The CSIRT shall disseminate relevant technical information related to this incident, to the electricity entities in order for them to organize effectively their cybersecurity defence within two (2) hours.

About zero day vulnerability (Art.38(5))

Responsible Disclosure (also known as coordinated vulnerability disclosure) of a zero-day-vulnerability is a vulnerability disclosure model in which a vulnerability or an issue is disclosed only after a period of time that allows for the vulnerability or issue to be patched or mitigated on another way. This period distinguishes the model from full disclosure. After finding a mitigation measure (like a patch) a full disclosure will inform all effected entities and give them the chance to mitigate the vulnerability in their environment. A full disclosure without having a mitigation measure, gives attackers the chance to miss-use the vulnerability without the chance for effected entities to protect themselves.

Common tool

The information sharing described in Art. 38(8) will request entities to share quickly and efficiently information in three steps:

- an entity with its CSIRT;
- CSIRT with the CSIRT Network (i.e. all CSIRTs together);
- each CSIRT to the entities of its Member State-

The following principle should be applied:

- The environment must be trustable and highly secured;
- Only selected participants (according to each step) shall have access on a need-to-know basis;
- Participants should have the possibility to change the information between each step (anonymization) but it should be easy to use the information from the previous step

The common tool described in the Art. 38(8) could:

- facilitate the exchange of information between participants for information sharing;
- propose a solution to share information during crisis; and
- log all incidents or vulnerabilities and let the electricity sector quickly find all the necessary information.

According to the complexity of such a tool, it is not possible to implement it in a short time period. Within 2 years after entry into force of the network code, ENTSO-E and the EU DSO entity carry out a feasibility study to analyse in cooperation with ENISA, CSIRT and main stakeholders the a feasible

solution for such a tool, ways to finance such a tool and a possible owner of such a tool responsible for maintaining it .

Article 39 ROLE OF HIGH-IMPACT AND CRITICAL-IMPACT ENTITIES CONCERNING INFORMATION SHARING

Not every high-impact and critical-impact entities has to implement a CSOC team, but each must have CSOC capabilities within their entities available; for instance, in an operational team. Entities can also use their own CSOC team or a MSSP .

An incident is classified as a "reportable cybersecurity incident" by the responsible representative (for instance the CISO) of the critical-impact or high-impact entity. When an incident is classified as a reportable incident by the representative, the entity has 4 hours to report the reportable incident to its national CSIRT. A good practice could be to design and document such a classification process by the entity during the first year of the implementation of the NCCS.

Article 40 DETECTION OF CYBERSECURITY INCIDENTS AND HANDLING OF CYBERSECURITY INCIDENT RELATED INFORMATION

To handle an incident having impact on cross-border electricity flows, the critical-impact and high impact entities should be supported by the CS-NCA, CSIRTs, the CSIRT network, the ENTSO for Electricity, the EU DSO entity, the RCCs and ENISA.

Article 41 CRISIS MANAGEMENT

The crisis management should follow established European crisis management procedures, in particular the ones laid down in the NIS Directive. ENTSO-E and EU DSO Entity expects European cyber lisison organisation network (EU – CyCLONe) to play a major role in crisis management in the electricity sector once NIS 2 Directive will be adopted.

If a cybersecurity cross-border crisis is declared, the NCCS stipulate that the CSIRT-NCA, with the CSIRT-NCAs from the affected Member States shall jointly create an ad hoc cybersecurity crisis coordination group ('coordination group') and define the participants. This coordination group should consist at least of:

- competent national authorities such as CSIRTs or CS-NCAs ; and
- high-impact or critical-impact entities affected by the cybersecurity cross-border crisis

The coordination group should support the high-impact and critical-impact entities to manage the cybersecurity cross-border crisis by providing e.g. expertise, information, communication.

Article 42 CRISIS MANAGEMENT PLANS AND BUSINESS CONTINUITY

Crisis management plans have to be developed by

- ACER for the Union level;
- the NRAs for the Member state level; and
- The critical-impact and high-impact entities for the entity level.

Critical-impact and high-impact entities have to integrate their crisis management plans into their business continuity plans.

-The results of the risk assessment at Member State and regional level are an important input for the creation or the adaptation of the business continuity plans of these entities as well as of the crisis management plans of ACER and each NRA.

Article 43 CYBERSECURITY EARLY WARNING CAPABILITIES FOR THE ELECTRICITY SECTOR

The ECEWC shall focus on innovation in methodologies and follow trends in digital development. The ECEWC should apply latest technology to achieve those objectives in an efficient way.

The ECWC will develop organically from existing situational awareness and early warning capabilities and solutions. The ECWC should be part of the feasibility study on the common tool for information sharing (Art. 38(8)).

Two kinds of information will be released by the ECWC:

- public information (Art. 43(2)(g)): this information could be publicly released e.g. on an internet website ;
- specified information about identified risks: the information will be sent to the concerned CSIRT (Art. 43(2)(f)). The CSIRT will then liaise with the relevant entities (Art. 43(3))

13 TITLE IX - ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

Article 44 CYBERSECURITY EXERCISES AT ENTITY AND MEMBER STATE LEVEL

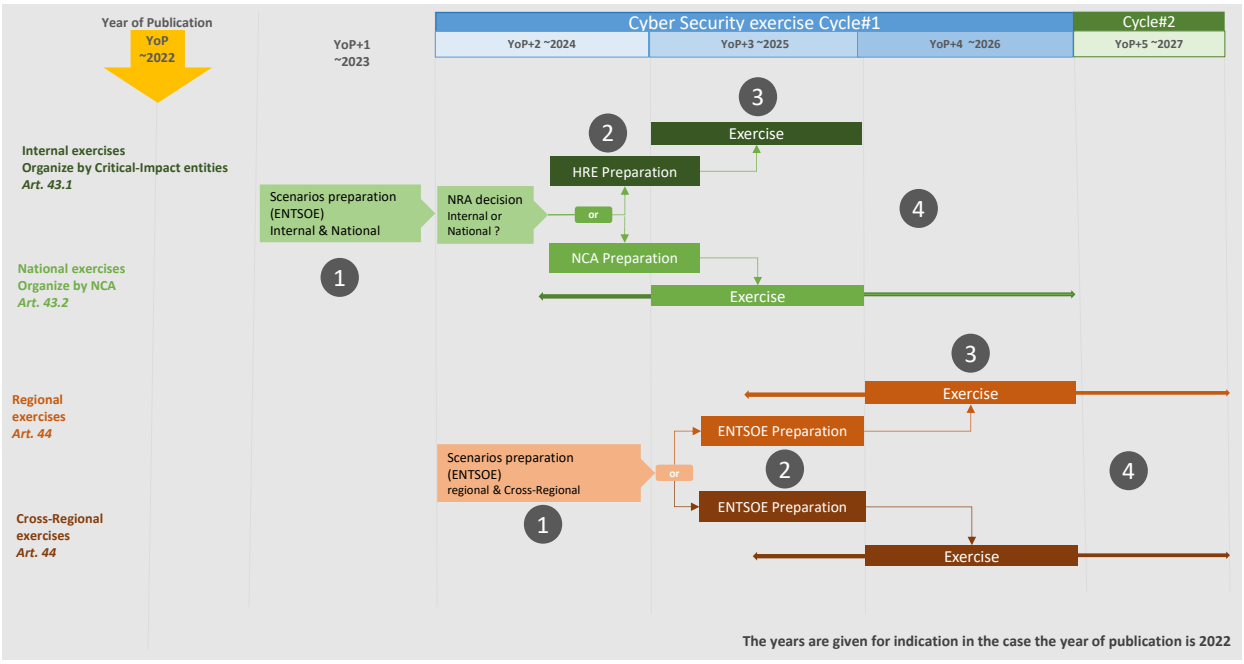
This article set out how the cybersecurity exercises shall be organised at entity or at Member State level. ENTSO-E and the EU DSO entity define the scenarios and make proposals for the cybersecurity assessment methodologies, including templates that could be used. The exercise at entity level may be replaced be an exercise at national level, if the NRA decides so.

Article 45 REGIONAL OR CROSS-REGIONAL CYBERSECURITY EXERCISES

This article set out how the cybersecurity exercises shall be organised at regional or at cross-regional level. ENTSO-E in cooperation with, the EU DSO entity and the concerned RCC in organising such exercises per system operation region or at cross-regional level. ENTSO-E and the EU DSO entity build the scenarios and make proposals for the cybersecurity assessment methodologies, including templates that could be used.

Cybersecurity exercise cycle

The overall target is that each critical-risk entity shall have at least two cybersecurity exercises within every 3 years: one exercise at entity or at Member State level (green cycle in the illustration here-after) and one exercise at regional level or at cross regional level (brown cycle in the illustration here-after).



The process will follow the principles of state of the art and the cybersecurity assessment methodologies approved by ACER:

1. define: first, the ENTSO-E will define the methodologies and the scenarios for the exercises, in the best case based on the result of the risk assessment or other actual risk scenarios;
2. organize: second, the organiser will prepare the exercise. Organisers can use the scenarios proposed by ENTSO-E or use their own;
3. perform: third, the organizer with the participants will perform the exercise; and then
4. analyse: finally, the organizer will analyse the outcome of the exercise, draw up a lesson-learnt report and develop recommendations jointly with participants.

The roles of each stakeholder are summarised in the table below:

	Internal	National	Regional	Cross-Regional
1. Propose the scenarios:				
In charge	**ENTSO-E in cooperation with EU DSO entity**			
Shall consult	ACER & ENISA		Commission advice of ACER, ENISA & JRC	
Due date	31/12/YoP+1*		31/12/YoP+2*	
2. Organize the exercises:				
In charge	**Critical-Risk Entity**	**NRA** with the technical support of CS-NCA	**ENTSO-E** In coordination with EU.DSO entity and the concerned RCCs	
Consultation / support		CS-NCA, RP-NCA	ENISA	
3. Perform the exercise				
Year of the exercise	YoP+3*		YoP+4*	
Organizer	Critical-Risk Entity	NRA	ENTSO-E in coordination with EU.DSO entity & RCCs	
Participants	Critical-Risk Entity	Designated** by the NRA	Designated** by ENTSO-E in coordination with EU DSO entity	
Potential participants (by order):	Critical-Risk Entity CSIRT NRA	CSIRT Critical-Risk Entities	RCC CSIRT Critical-Risk Entities	RCC CSIRT Critical-Risk Entities
4. Lessons learnt & recommendations				
In charge to monitor:	Critical-Risk Entity	**NRA**	**ENTSO-E in coordination with** EU DSO entity and the concerned RCCs	
In charge to implement:	Critical-Risk Entity	Participants	Participants	

Table 1 Summary of Art. 44 and Art. 45 provisions

(*) this cycle will be repeated every 3 years

(**) The participants in national, regional and cross-regional exercises will be designated by the organizer. According to the type of exercise and the expected results, not all entities may be designated. Following the obligation to report to CSIRT and/or CS-NCA (according to the Member State) during a crisis, the participation of several entities in the cybersecurity exercises will probably be necessary in the exercises at Member State and regional level.

Article 44(2) and Article 45(4) provide the NRA and ENTSO-E the possibility to organise exercises jointly within other cybersecurity exercises. Organizing cybersecurity exercises jointly with other organisation should be considered as a good practice that can avoid multiplying cybersecurity exercises. Participating in too many exercises could damage the quality of the exercises done and the expected benefits.

Article 46 INTERNAL, NATIONAL, REGIONAL OR CROSS-REGIONAL CYBERSECURITY EXERCISES

Implementation of recommendations issued from the lessons learnt is not mandatory but the NCCS stipulates that the organizer must have access to the necessary information.

14 TITLE X - PROTECTION OF INFORMATION

Article 47 BASIC PRINCIPLES AND MINIMUM STANDARDS

Principles for identifying Protected Information and the associated protective measures

The provisions of paragraphs 1 to 5 define the principles applicable for classification of information to be protected. The criteria for information classification according to this network code are defined as part of the common electricity cybersecurity framework.

The classification criteria defined for information to be protected (i.e. the Protected Information) will be associated to the following basic common properties of information to be protected and thus to be assessed for classification:

- Confidentiality
- Integrity
- Availability

Non-repudiation i.e. the authenticity of an information exchange, may be included as a separate property for classification.

Classification is the evaluation process performed by assessing a possible impact if the protection of the properties of the information is compromised. For the purpose of classification in the context of the NCCS, the classification criteria defined shall include predefined set of classification levels, each associated with a category of impact and an impact severity level.

If needed for the purpose of protection of information exchanged in the context of the NCCS, the classification criteria shall include separate predefined sets of classification levels for the integrity, availability or non-repudiation properties. This should be identified as part of the risk management process applied for the information to be exchanged.

The provisions of paragraphs 6 to 11 apply to classification and protection of information within the scope of Article 9 i.e. all confidential information received, exchanged or transmitted pursuant to this Regulation.

Categories for information classification

The protected information is classified based on its category:

- NCCS Classified Information,
- NCCS Sensitive Information, and
- NCCS Unrestricted Information.

The category NCCS Unrestricted Information shall be used for all information not within the scope of confidential information i.e., without legal restrictions on disclosure or any information intended for public disclosure.

The Union and the Member States have already defined legally binding classification levels for confidentiality, including requirements for protective measures which includes governmental authorization processes with mandatory security clearance of individuals and mandatory security accreditation of organizations and information systems. The impact levels defined reflects the consequences related to the interests of the European Union and its Member States. The use of classification processes defined by European Union and its Member States are mandatory for the bodies

and the agencies of the European Union and its Member States, thus the NCCS have provisions for these classification schemes, collectively defined within the confidentiality category NCCS Classified Information.

The category NCCS Sensitive Information is defined to include classification of all confidential information not included in the category NCCS Classified Information. This includes information or material the entities defined in Article 2 must protect because of legal obligations laid down in the Treaties or in legal acts adopted in implementation thereof, and/or because of its sensitivity (e.g. security and commercially sensitive and confidential information of the organization).

Authorization of entities

The provisions of paragraph 7 are included to restrict:

1. the number of entities to be authorized for handling NCCS Classified Information, and
2. the obligations of protection to be applied only for entities authorized for handling this category of Protected Information.

The procedures for qualifying an entity for authorization and the rules for authorization shall be defined in the common electricity cybersecurity framework in order to ensure that the entities will have predictability on future obligations and that the legal obligations will be proportionate to the responsibilities defined by their operative task in the implementation of the NCCS. This is important for all entities not already legally mandated to be authorized according to other European Union or its Member States' legislations.

Article 48 RULES FOR MARKING AND PROTECTING INFORMATION

This article states the rules for marking information classified for confidentiality protection in order to ensure that the need for protection is clearly communicated and understood by all entities handling the information exchanged or transmitted pursuant to this Regulation in order to protect the information.

The principle for marking is that the sending entity shall be able to specify the classification level, the identity of the classifying entity (normally the entity providing the original information) and additional restrictions of authorized use and limitations applicable to distribution or releasability (e.g. publication) to be applied for protection by the receiving entities.

Confidentiality category	**Classification level**	**Classifying entity identification**	**Dissemination label**
NCCS Classified Information	Mandatory	Mandatory	Optional - not applicable for incident handling acc. to Title VIII
NCCS Sensitive Information	Mandatory	Mandatory	Mandatory if used for incident handling acc. to Title VIII
NCCS Unrestricted Information	Mandatory	Mandatory if used for incident handling acc. to Title VIII	Mandatory if used for incident handling acc. to Title VIII

Table 2 Summary of Art. 48 provisions

Information in the category NCCS Classified Information will not be used for exchange of information between entities in the purpose of incident handling according to provisions of the NCCS Title VIII due to the lack of communication systems authorized for this category. Current regulation applicable for this category will require both end systems and communication networks to be authorized for multi-level classified information. Thus, if the development of specific tools for this task are necessary, will be assessed in the feasibility study pursuant to Article 37 (7).

Article 49 PROTECTION OF INFORMATION EXCHANGED IN THE CONTEXT OF TITLE VIII

This article states more explicitly the use of the classification level, the identity of the classifying entity and the dissemination label for the purpose of handling incidents according to the provisions of Title VIII.

Application of the classification categories

The table below contains a preliminary indicative application of the classification categories according to Article 46 (6) for information mandated by this Regulation according to the ACER Framework Guidelines for the NCCS.

Classification category	**Normative classification criteria**
NCCS Classified Information	The category includes, but may not be restricted to information classified according to: • The Commission Decision (EU, Euratom) 2015/444, i.e, 'European Union Classified Information' (hereafter 'EUCI') or the applicable equivalent national classification, that is to say any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States. This category may apply for • The transitional lists of "critical-risk"/ "high-risk" entities (Article 50) • The lists of the temporary issued derogations from the minimum and advanced cybersecurity requirements (Article 30) • The full and confidential Cross-Border Electricity Cybersecurity Risk Assessment Report (Article 21)

Classification category	Normative classification criteria
• NCCS Sensitive Non-Classified Information	• The category includes, but may not be restricted to: • information or material the entities defined in Article 2 must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as stated in Art 10 of this Regulation, (as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001 read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EU) 2016/679) and sensitive information regulated by applicable Member State regulations. • • The category may also apply to • The Cybersecurity inspection reports (Article 25) •

Table 3 Application of the classification categories.

15 TITLE XI - FINAL PROVISIONS

Article 50 TRANSITIONAL PERIOD

A transitional period of 18 months is foreseen between when the network code enters into force and before the first risk assessment cycle (see Figure 8).

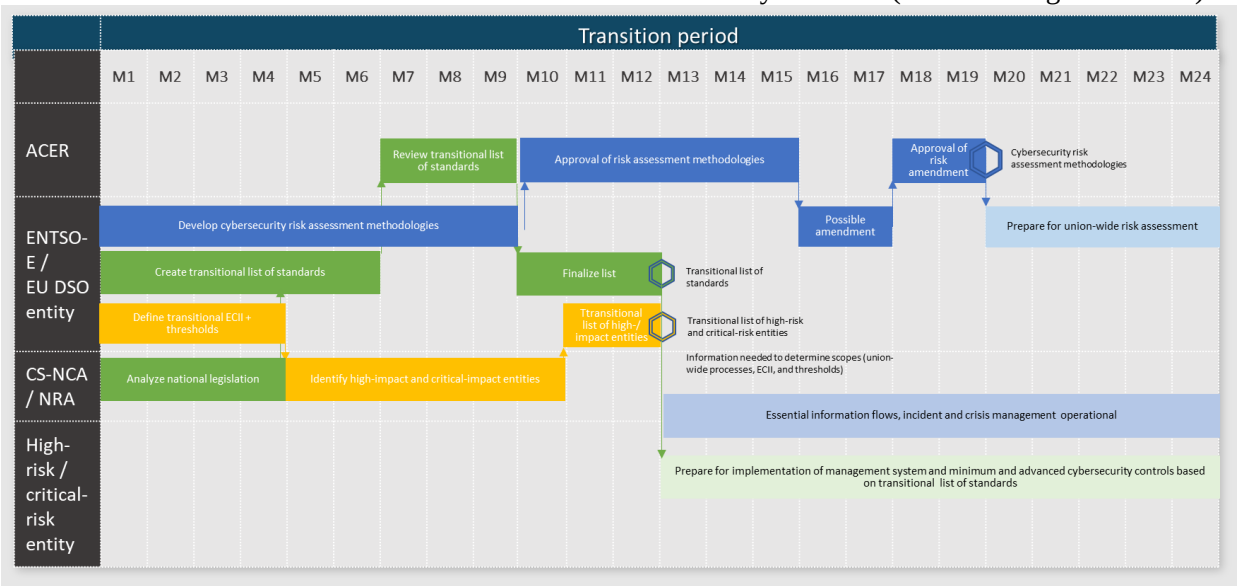


Figure 8: Transition period before the first cybersecurity risk assessment cycle.

During the transition period different terms and conditions or methodologies needed for the first risk assessment cycle have to be developed.

- ENTSO-E and EU DSO entity will deliver a transitional cybersecurity impact index (transitional ECII;
- Using these, the CS-NCA then determines the transitional list of high-impact and critical-impact entities in their Member State. ENTSO-E and the EU DSO entity then compile the national lists into a single Union-wide list. The list is used to identify the entities that must start a cybersecurity risk assessment at entity level at the start of the first risk assessment cycle.
- Based on the transitional ECII, CS-NCAs and NRAs will develop a transitional list of high-impact and critical-impact entities;
- ENTSO-E and the EU DSO entity will develop a transitional list of high-impact and critical-impact processes;
- ENTSO-E and the EU DSO entity will develop a transitional list of international standards that entities can use to prepare for the implementation of the network code. These include standards for the risk assessment at entity level, and standards with controls that are expected to be equivalent to the minimum and advanced cybersecurity controls. National legislation is included in the transitional list of standards if it is provided by the CS-NCA to ENTSO-E and the EU DSO entity.

Article 51 ENTRY INTO FORCE

The NCCS will enter into force 20 days after its publication in the Official Journal of the European Union. However, the application of different parts of the NCCS will need the development of methodologies and set of rules. The different timelines to develop such rules are laid down in the respective articles.