entsoe

EU DSO Entity

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

28 October 2021

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.

The documents provide 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 PROVISIONS OF THE NCCS

6 GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

7 RISK MANAGEMENT AT UNION WIDE AND REGIONAL LEVEL

8 COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

9 RISK MANAGEMENT AT NATIONAL LEVEL

10 RISK MANAGEMENT AT ENTITY LEVEL

11 HARMONISING PRODUCT AND SYSTEM REQUIREMENTS AND VERIFICATION

12 ESSENTIAL INFORMATION FLOWS INCIDENT AND CRISIS MANAGEMENT

13 ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

14 FINAL PROVISIONS

15 ANNEXE A basic cybersecurity hygiene requirements

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 has to be set up by ENTSO-E. Figure 1 illustrates the Network Code development process as set out in the Regulation (EU) 2019/943.

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 promote the completion and functioning of the internal market for electricity
- Article 59 Establishment of Network Codes: NC to be in accordance with ACER FG, NC will become binding, establishment of drafting committee, Article 31 and 56: extensive stakeholder consultation
- Article 59 (2) (e) Scope of NC 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 and the EU DSO entity, ACER and the European Commission.

NCCS development process (Source: ENTSO-E):

- EC request to ACER to submit a non-binding FG
- ACER elaborates FG in consultation with stakeholders, in particular with ENTSO-E and EU DSO entity and submits FG to EC
- EC requests ENTSO-E in close cooperation with the EU DSO entity to elaborate NCCS according to ACER FG

- ENTSO-E convenes drafting committee and consults with EU DSO entity the stakeholders on NCCS before submitting final NCCS to ACER for opinion
- ACER consultation and recommendation to EC to adopt the NCCS
- EC 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 framework guideline on cybersecurity published by ACER on 27 July 2021. ENTSO-E and the EU DSO entity are cooperating throughout the whole drafting process on an equal footing and pay attention to the involvement of the main affected stakeholders, in particular in the drafting committee and 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 drafting process is to be finalised within 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 019/943 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. This Regulation 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) 2019/843 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. RCC) 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 cyber incident and monitoring of the operational reliability of the NCCS.

The NCCS also limits to the collection of information to a reasonable amount, provides for achievable deadlines for stakeholders to submit such information and 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, incident and crisis management;
- Title IX: Electricity cybersecurity exercise framework;
- Title X: Protection of information exchanged in the context of this data processing;
- Title XI: Final provisions.

3.4 LEVEL OF DETAIL

In order to 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, and with the view of drafting the NCCS in way to ensure its applicability taken into account future developments and new applications, 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 a second step the requirements, criteria, methodologies and performance indicators in a second step, 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 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, TSOs and DSOs should support third countries in applying similar cybersecurity rules as set out in the NCCS. ENTSO-E and the EU

DSO Entity should facilitate cooperation between the Union TSOs and DSOs and third country TSOs and DSOs.

Considering the importance of cybersecurity and that cybersecurity does not stop at boarders, 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 its 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.

Also entity or third parties to whom responsibilities have been delegated or assigned with a relevant cybersecurity impact on the cross-border electricity flow have 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 the Electricity Market Directive

(b) NEMOs as defined in Article 2(7) and (8) of Electricity Market Regulation

(c) Electricity digital market platforms as defined in Article 4(12) number 14 of this Regulation

(d) Critical service providers as defined in Article 4(12) number 6 of this Regulation;

(k) Security Operation Centres (‘SOCs’);

(m) Computer Security Incident Response Team (‘CSIRT’);

European bodies

(f) the European Network of Transmission System Operators for Electricity (‘ENTSO-E’);

(g) the European Network of Distribution System Operators for Electricity (‘EU-DSO entity’);

(h) the Agency for the Cooperation of Energy Regulators (‘ACER’);

(n) the European Union Agency for Cybersecurity (‘ENISA’)

Regional bodies

(e) Regional Coordination Centres (RCCs) established pursuant to Article 35 of the Electricity Market Regulation

National bodies

(i) National Regulatory Authorities ('NRAs');

(j) National Competent Authorities for Risk Preparedness ('RP-NCA');

(l) National Competent Authorities for cybersecurity in Energy ('CS-NCA');

ACER is responsible for the monitoring of the correct implementation of the NCCS. Enforcement power lies within the National Regulatory Authorities (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 electricity 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, at least bi-annual, reporting, the so-called "Cross-Border Electricity Cybersecurity Risk Assessment" is foreseen in the NCCS.

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'). The NCCS complements the NIS Directive by ensuring that cyber-incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans.

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 led 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 cyber experts with the support from 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 DD August 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 network code drafting committee in order to participate actively in the monthly meetings to review progress.

ENTSO-E and the EU DSO entity are launching the public consultation on the NCCS draft for one month. They will organise a public stakeholder workshops, as well as ad-hoc meetings and exchange of views with all interested parties when necessary.

4 FRAMEWORK GUIDELINE ON CYBERSECURITY

4.1 INTRODUCTION

During the informal process to prepare recommendation 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 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 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.

5 PROVISIONS OF THE NCCS

5.1 INTRODUCTION

This section describes for each provision of NCCS the objectives that the NCCS sets out to achieve by means of the defined requirements.

This section aims at providing the reader the basis for understanding the requirements set in the chapters marked above of the NCCS.

5.2 GENERAL PROVISIONS

Article 1 - Subject Matter

This article subject of the NCCS limited 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 electricity undertakings in the Union.

Furthermore it is clarified who has to apply the basic cyber hygiene requirements that are listed in Annexe A of the NCCS. In particular micro and small enterprises that are neither critical-risk nor high risk entities, should still implement minimum requirements with regard to cyber hygiene. The concerned micro and small enterprises have to comply with the said requirements 12 months after their adoption. This leaves sufficient time for them to adapt their internal processes and procedures.

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. Such terms are capitalised and their definitions are not repeated in the NCCS.

ENTSO-E and the EU DSO entity are ensuring consistency with definitions used in other Union legislation as well as other related documents and are striving to grant easy access to the full body of definitions. Terms that are already defined in other Union legislation are thus not included in the legal text of the NCCS.

Article 5 Adoption of methodologies

This article describes the approval procedures and the regulatory oversight of 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 other network codes and guidelines.

Article 6 Publication of methodologies on the internet

This article clarifies that the approved methodologies have to published in order to be available to all entities that fall under the scope of the NCCS and to any interested stakeholder.

Article 7 Stakeholder involvement

Stakeholder is key to success for the implementation of the NCCS. Therefor this articles clarifies how stakeholder involvement is to be organised in addition to the public consultations that will be organised for the methodologies..

Article 8 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 methodologies.

Article 5 – Recovery of Costs

According to this article, costs arising from the NCCS to system operators subject to network tariff regulation (both TSOs and DSOs), where this may be relevant, are 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 6 – 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 undertakings 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 7 Confidentiality classification

This article refers to the principle that all information exchanged among all stakeholders for the implementation of the network code shall be protected. The classification system is specified in Article 7.

This article introduce the notion of classification and protection in order to bind the classification and the appropriate measures set to grant the appropriate level of protection regarding the classification.

This article is not meant to overlap dispositions described in Article 7, so it was restrained to the essential principle above described.

Article 11 Information Confidentiality Classification and Protection

This Articles sets out the basic principles for the classification of information and the protection of the information with regard to cybersecurity and cross-border electricity aspects. This Article is completed by TITLE X which sets out more specific provisions on information sharing and classification.

Article 12 – 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-risk and critical-risk entities;
- The size cap to determine if an undertaking is to be considered as a critical-risk or a high-risk enterprise does not directly or indirectly cause a systemic cybersecurity risk for cross-border electricity flows.

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 bay 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 13 Benchmarking

This article describes the different steps to follow 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 14 – Agreements with TSOs and DSOs not bound by this Regulation

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

6 GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

Articles 15 and 16 CYBERSECURITY RISK WORKING GROUP AND MONITORING BODY

Currently there is no organization in Europe performing cross-border electricity flow cybersecurity risk identification, evaluation, and treatment. Individual TSOs and DSOs do perform their own company and wider National type cyber risk assessments, but no one is looking at the overall union-wide bigger cyber risk picture. To address this the Network Code for Cybersecurity creates:

- A cybersecurity risk working group representing the interests of the main affected stakeholders, including all high-impact and critical-impact entities. The group advises ENTSO-E and the EU DSO entity during the Union-wide cybersecurity risk assessment and the regional cybersecurity risk assessment. They help to collect the required information and perform he analyses. ENTSO-E and the EU DSO entity are responsible for operating the working group and provide appropriate resources to properly assess cross-border electricity flow cyber risk.

- A cybersecurity risk monitoring body representing the interests of the EU Commission and agencies, EU member states and other relevant governmental or energy sector body or association. The monitoring body advises ACER when they review the work of the cybersecurity risk working group.

ENTSO-E and the EU DSO entity shall invite a limited number of participants to the working group, to protect its effectiveness. Representatives from EU associations will be invited if these exist to involve as many stakeholders as possible.

The scope of the cybersecurity risk working group is 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 electricity undertakings are out of scope.

Article 17 CYBERSECURITY RISK ASSESSMENT METHODOLOGIES

For the network code on cybersecurity, risk management is performed at three levels (see **Error! Reference source not found.**):

- At union-wide and regional level by a cybersecurity risk working group led by ENTSO-E and the EU-DSO entity (Section 7)

- At national level by the CS-NCA (Section 99)

- At entity level by every high-impact and critical-impact entity identified by the CS-NCA (Section 10)

The cybersecurity risk working group will define methodologies for the risk assessments at union-wide, regional and level. At entity level, each entity is allowed to select their own risk assessment method subject to certain requirements (Section **Error! Reference source not found. Error! Reference source not found.**).

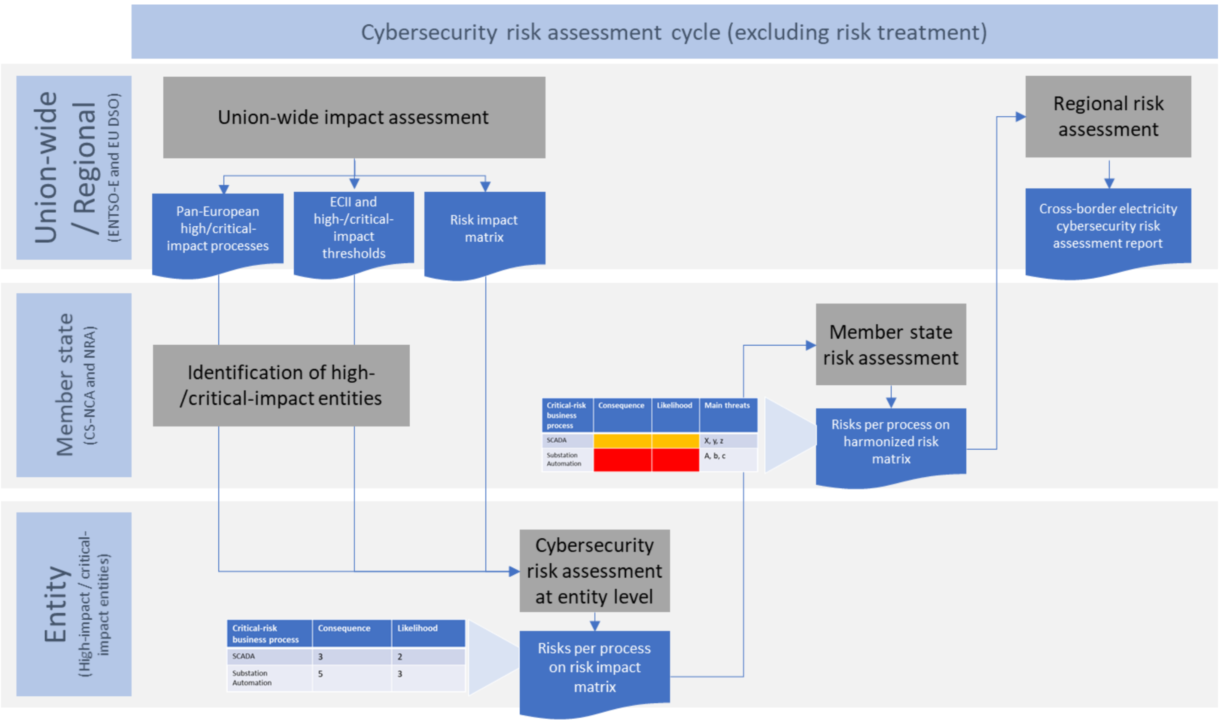

Cybersecurity risk assessment cycle (excluding risk treatment)
Union-wide / Regional
(ENTSO-E and EU DSO)
Union-wide impact assessment
Pan-European high/critical-impact processes
ECII and high-/critical-impact thresholds
Risk impact matrix
Regional risk assessment
Cross-border electricity cybersecurity risk assessment report
Member state
(CS-NCA and NRA)
Identification of high-/critical-impact entities
Member state risk assessment
Critical-risk business process
Consequence
Likelihood
Main threats
SCADA
X, y, z
Substation Automation
A, b, c
Risks per process on harmonized risk matrix
Entity
(High-impact / critical-impact entities)
Cybersecurity risk assessment at entity level
Critical-risk business process
Consequence
Likelihood
SCADA
3
2
Substation Automation
5
3
Risks per process on risk impact matrix

Figure 1: Cybersecurity risk assessment activities at different levels.

- For measuring consequences, the cybersecurity risk assessment method shall use the consequence categories from operations network code; operational security, frequency quality and the efficient use of the interconnected system and resources. In this way, metrics developed from the operations network code can be reused.

- Note that the cybersecurity risk working group only defines a method to calculate the ECII. The calculation of the ECII values is left to the CS-NCA and NRA, possibly with support of the entities (Section 9.2).

Article 18 RISK ASSESSMENT CYCLE

The cybersecurity risk assessments are organized in a cycle that repeats every two years after the transitional period described in Section 14.2, see Figure 2.

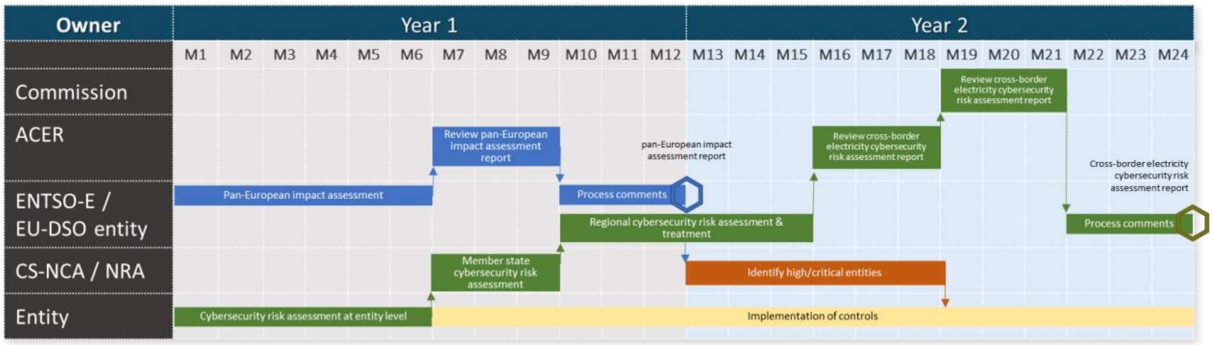


Figure 2: Cybersecurity risk assessment cycle.

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 two years.

The main deliverables of the cybersecurity risk assessment are the Union-wide cybersecurity risk assessment report at the end of the first year, and the cross-border electricity cybersecurity risk assessment report at the end of the second year.

The CS-NCA and NRA can start the identification of the high-impact and critical-impact entities after the Union-wide cybersecurity risk assessment is completed, as they need the outcomes of this assessment (see Section **Error! Reference source not found.**). The entities would be identified in month 18 of the cycle. This would give newly identified high-impact and critical-impact entities 6 months to prepare for the start of the next cycle.

7 RISK MANAGEMENT AT UNION WIDE AND REGIONAL LEVEL

The risk assessment at the highest level (union-wide / regional) is conducted in two phases (see Figure 3):

- A Union-wide cybersecurity risk assessment. The impact assessment only considers the consequences of cyber-attacks, 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 would be of a cyber-attack on such processes.
- A regional risk assessment. The regional risk assessment aggregates data on the likelihood of attacks from all member states within the region. The likelihood data summarizes the state of threats, countermeasures, and vulnerabilities. Combined with the impact from the first phase, the total risk level can then be determined.

The steps from ISO/IEC 27005:2011 are divided over these two phases as shown in Figure 3.

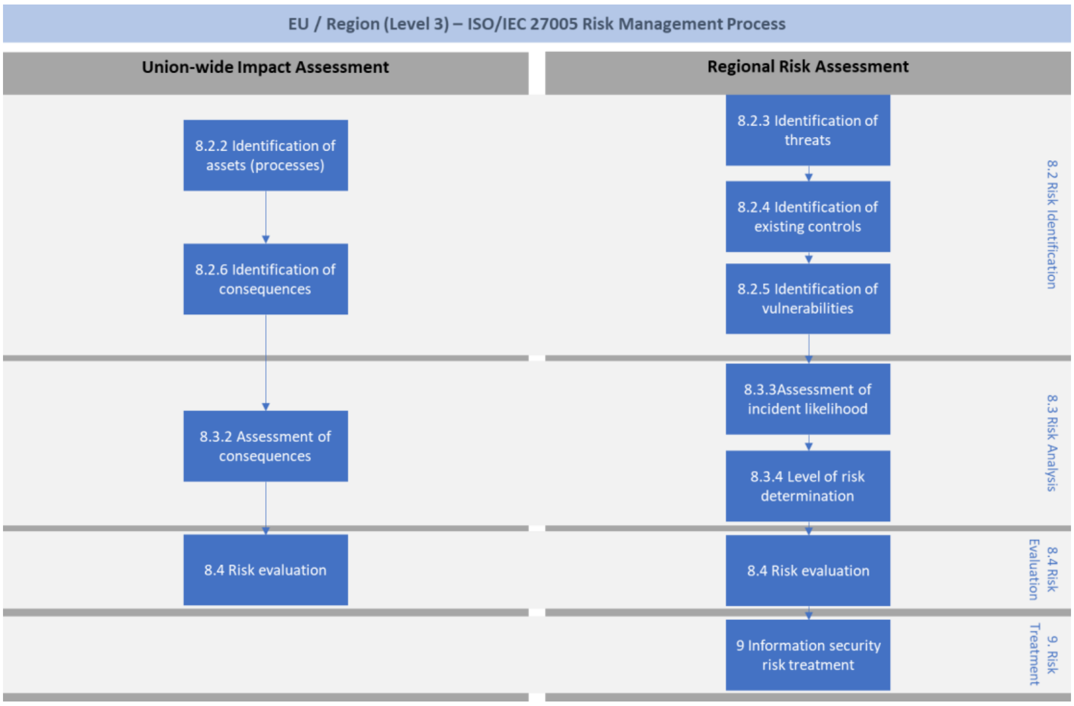

EU / Region (Level 3) – ISO/IEC 27005 Risk Management Process
Union-wide Impact Assessment
Regional Risk Assessment
8.2.2 Identification of assets (processes)
8.2.6 Identification of consequences
8.3.2 Assessment of consequences
8.4 Risk evaluation
8.2.3 Identification of threats
8.2.4 Identification of existing controls
8.2.5 Identification of vulnerabilities
8.3.3Assessment of incident likelihood
8.3.4 Level of risk determination
8.4 Risk evaluation
9 Information security risk treatment
8.2 Risk Identification
8.3 Risk Analysis
8.4 Risk Evaluation
9. Risk Treatment

Figure 3: Process steps in the union-wide and regional risk assessment.

7.1 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 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 determine what the high-impact and critical-impact entities in their member state are by providing a list of Union-wide high-impact and critical-impact processes, the ECII, and the high-impact and critical-impact thresholds (see Section **Error! Reference source not found.**).
- It allows entities to determine the scope for their risk assessments from the list of Union-wide high-impact and critical-impact processes, as explained in Section **Error! Reference source not found.**.
- It provides a harmonized cybersecurity risk 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 in that it classifies entities only based on impact, not on risk (see **Error! Reference source not found.**). The ECII only consider only the consequences of cyber-attacks because the drafting team thinks this should be the main criterion to determine what controls entities must apply. The likelihoods should not matter. 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 critical and be regulated under the network code.

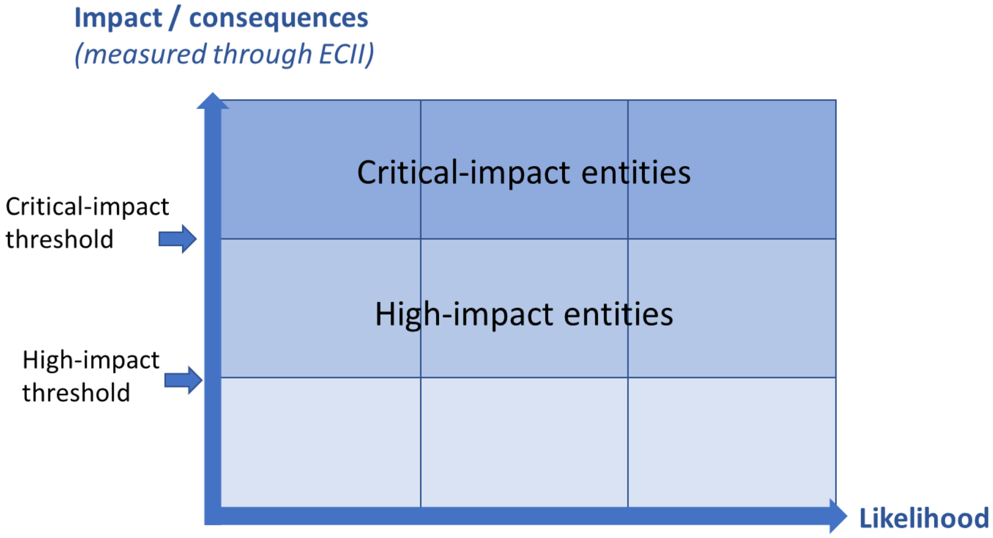


Figure 4: Classification of entities based on impact.

Other reasons to not 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 network code processes cannot cope with such quick changes. The impact measures are generally more stable.

7.2 REGIONAL CYBERSECURITY RISK ASSESSMETN AND TREATMENT

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 levels. Based on the integrated risks, risk treatment options are selected. The risk treatment includes the minimum and advanced cybersecurity controls in the common electricity cybersecurity framework (Section 8). The risk assessment and risk treatment plan are then reported together in the Cross-border electricity cybersecurity risk assessment report.

The input for the regional cybersecurity risk assessment is the assessment by each CS-NCA of the cybersecurity risks per Union-wide high-risk and critical-risk process, coming out of the member state level risk assessment. The risks are all mapped to the same harmonized risk matrix to make the easier to aggregate.

To help the working group interpret these risk per process, CS-NCA also provide a list of threats causing the risks, and a list of recommended controls to mitigate the risks. More sensitive information could be provided in workshops with the CS-NCA.

Information on assets is aggregated on the level of business processes. In cybersecurity risk assessments, assets can be classified into primary assets, such as business processes and information assets, and supporting assets, such as hardware, software, personnel, and sites. The supporting assets are very different for different entities. Creating an aggregated asset inventory for supporting assets would hence take considerable effort.

Such a detailed inventory is also not needed. To determine the minimum and advanced cybersecurity controls and the high-impact and critical-impact entities, the working group only needs to know the cybersecurity risks per business process. These risks are hence determined in the regional risk assessment.

8 COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

The cybersecurity risk working group will define a common electricity cybersecurity framework with the measures entities should take to mitigate the cybersecurity risks. The framework consists of four parts:

- Minimum cybersecurity controls applicable inside the high-impact perimeter
- Advanced cybersecurity controls applicable inside the critical-impact perimeter
- An Electricity Controls to Standards Mapping Matrix (ECSMM) that maps the controls from (2) and (3) to selected international standards and national legislative frameworks

See Section 10.1 for an explanation of the high-impact and critical-impact perimeters.

The cybersecurity risk working group will based the cybersecurity hygiene requirements on the work of ENISA. The hygiene requirements should include only basic requirements that can be fulfilled also by small enterprises without large amounts of extra costs The measures are not directly linked to the regional risk assessment. Hence, they will not be updated after every risk assessment cycle. They are only updated if developments in defensive methodologies lead to cost-effective new measures applicable to all entities. The basis can be for instance the review of cyber-hygiene practices that ENISA published in 2016.The cybersecurity risk working group selects the minimum and advanced security controls based on the cross-border cybersecurity risk assessment at regional level. The cybersecurity risk working group will select the minimum and advanced cybersecurity controls from international standards. The primary source will be ISO/IEC 27002 and ISO/IEC 27019.

The working group will provide mappings in the ECSMM from the cybersecurity controls to other 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 IEC 62443 standard and the NIST Cybersecurity framework will be included in the ECSMM in the transitional phase, as these are the most commonly used standards. Other standards may be added on request of electricity entities afterwards.

CS-NCA and NRA may create mappings form the cybersecurity controls to national regulation for the ECSMM. The cybersecurity risk working group will not develop such mapping itself, as it does not have the resources and legal expertise to do this for all member states. The cybersecurity risk working group will validate the mappings before adding them to the ECSMM. To aid in the validation, the CS-NRA or NRA must provide a verification by a conformity assessment body that the mapping is correct and covers all cybersecurity controls.

8.1 MINIMUM AND ADVANCED CYBERSECURITY SUPPLY CHAIN SECURITY CONTROL

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 to address these risks. These measures are mandatory.

The measures have been integrated in the risk assessment and common electricity cybersecurity framework as depicted in figure 1 and as follows:

- Supply chain risks are considered in the regional cross-border risk assessment
- Based on the regional cross-border risk assessment, supply chain security controls are included in the common cybersecurity controls
- Supply chain threats identified in the regional risk assessment are included in the threats that entities should consider in the entity-level risk assessment

Additionally, to support the implementation of the supply chain security controls at entities, the cybersecurity risk working group will develop harmonized security requirement sets and verification schemes (see Section 0).

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 covers products, services, and processes for OT systems, such as SCADA systems, substations and distribution automation systems, or smart metering systems. The definitions are used to stay close to the existing legislation.

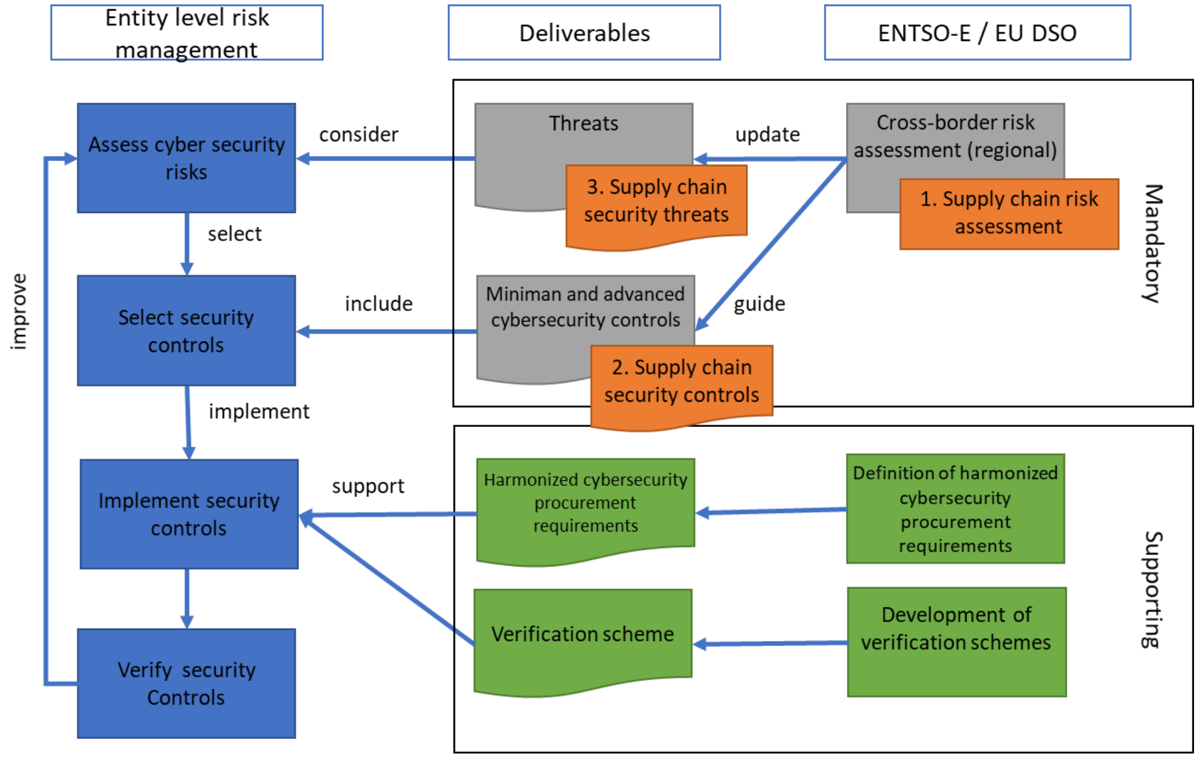

Entity level risk management
Deliverables
ENTSO-E / EU DSO
Assess cyber security risks
consider
Threats
update
Cross-border risk assessment (regional)
3. Supply chain security threats
1. Supply chain risk assessment
Mandatory
select
improve
Select security controls
include
Miniman and advanced cybersecurity controls
guide
2. Supply chain security controls
implement
Implement security controls
support
Harmonized cybersecurity procurement requirements
Definition of harmonized cybersecurity procurement requirements
Supporting
Verification scheme
Development of verification schemes
Verify security Controls

Figure 5: Supply chain security measures in the Common Security Framework. The mandatory measures (in orange) are described in Section ***Error! Reference source not found.****. The supporting measures (in green) are described in Section 0.*

8.2 SUPPLY CHAIN RISKS IN THE REGIONAL RISK ASSESSMENT

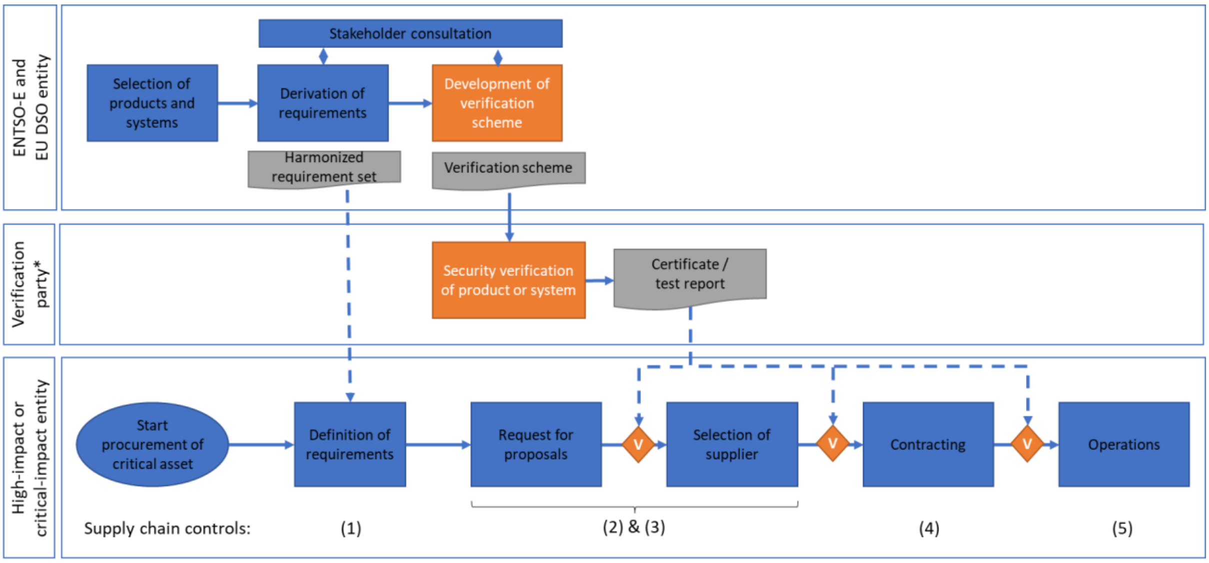
The network code requires the cybersecurity risk working group to consider supply chain threats when they conduct the cross-border regional risk assessment. The most important threats identified by ACER in the framework guidelines are explicitly listed for consideration.

8.3 SUPPLY CHAIN SECURITY CONTROLS

The regional cross-border risk assessment will result in an updated set of supply chain security controls included in the common cybersecurity controls. The supply chain security controls concern organizational measures that high-impact and critical-impact entities must take to acquire new products and systems. These controls will be revised every two years as part of the regional risk assessment. Hence, they can be adjusted to counter new threats or use newly developed security measures.

The controls do not contain technical requirements to the products and systems. They only require entities to define, use and verify such requirements during procurement. Harmonized technical requirements are developed by the cybersecurity risk working group to support entities in this and make it easier and more cost-effective to procure secure equipment (Section 0). Entities 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 should meet certain principles given in the article *Supply chain security controls* of the network code. The principles are based on the recommendations given by ACER in the framework guidelines. The controls are designed to cover the entire procurement process for high-impact and critical-impact entities as shown in Figure 6.


ENTSO-E and EU DSO entity
Stakeholder consultation
Selection of products and systems
Derivation of requirements
Development of verification scheme
Harmonized requirement set
Verification scheme
Verification party*
Security verification of product or system
Certificate / test report
High-impact or critical-impact entity
Start procurement of critical asset
Definition of requirements
Request for proposals
V
Selection of supplier
V
Contracting
V
Operations
Supply chain controls:
(1)
(2) & (3)
(4)
(5)

*The verification party could be an independent test lab or auditor, but could also be the entity itself or the supplier in case of self-assessment

Figure 6: Supply chain security controls in the network code mapped to the procurement process at a high-impact or critical-impact entity. Verification steps are in orange and are only mandatory for critical-impact entities. Possible verification steps are marked with an orange 'V'.

8.4 ADVANCED COMMON SECURITY CONTROLS

Critical-impact entities are additionally required to verify the implementation of the security requirements to products and systems. They may apply verification at different steps in the procurement process, see Figure 6, as long as they verify the product or system before they take it into operation.

The cybersecurity risk working group supports critical-impact entities by developing harmonized verification methodologies, see Section 11.

8.5 SUPPLY SHAIN RISKS IN THE ENTITY-LEVEL RISK ASSESSMENT

High-impact and critical-impact entities must consider supply chain threats in their own risk assessments. As a baseline, entities are required to implement the common supply chain security controls. 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.

9 RISK MANAGEMENT AT NATIONAL LEVEL

At national 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 ECRI. The second activity is to perform a member state risk assessment with the input received from the entity risk assessments.

9.1 NATIONAL CYBERSECURITY RISK ANALYSIS

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 assessment.

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 to make them easier to aggregate. Additionally, the entity will provide a summary of threats, existing controls, and vulnerabilities.

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 more information from entities if they need it, through their mandate for cybersecurity inspections.

9.2 IDENTIFICATION OF HIGH-IMPACT AND CRITICAL-IMPACT ENTITIES

Based on the Union-wide cybersecurity risk assessment, the CS-NCA and NRA identify the high-impact and critical-impact entities within their member state.

The CS-NCA and NRA can create a long-list of potential high-impact and critical-impact entities based on the list of Union-wide high-impact and critical-impact processes. The working group will include in the list the types of entities involved in each process.

The CS-NCA and NRA 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 and NRA, they can determine the ECII themselves. Otherwise, they will need to request additional information to the entities. They could also ask the entities themselves to calculate the ECII and then validate the results.

The CS-NCA and NRA 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.

9.3 NATIONAL VERIFICATION SCHEMES

The network code requires that critical-impact entities verify the implementation of their management system and the advanced cybersecurity controls in one of three ways: through certification, through peer review, or through legally obligated inspection and supervision.

Certification is done by conformity assessment bodies supervised by the national accreditation body. The last two options are supervised by the CS-NCA in national verification schemes.

The verification schemes can be used to integrate existing supervision methodologies by the CS-NCA, for instance developed for the NIS directive, into the network code. 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 RISK MANAGEMENT AT ENTITY LEVEL

Article 30 DEROGATIONS FROM THE MINIMUM AND ADVANCED CYBERSECURITY CONTROL

Within 6 months after the finalisation of the minimum and advanced cybersecurity controls, all entities shall apply the minimum cybersecurity controls within the high-risk perimeter and advanced cybersecurity controls within the critical impact perimeter. Nevertheless the NCCS recognises that there may be a need for temporary derogations from some of these requirements. The entity that wants 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 benefit; when it can provide a reisk treatment plan demonstrating how the remaining risk is mitigated or when results of the risk assessment of the entity do not show any direct or indirect impact on cross-border electricity flows.

At entity level, all high-impact and critical-impact entities must implement cybersecurity risk management and a cybersecurity management system. Additionally, high-impact entities must implement the minimum security controls, and critical-impact entities must implement the minimum and advanced security controls. See Figure 7. The scope to which each of these measures applies is determined by the different perimeters within an entity.

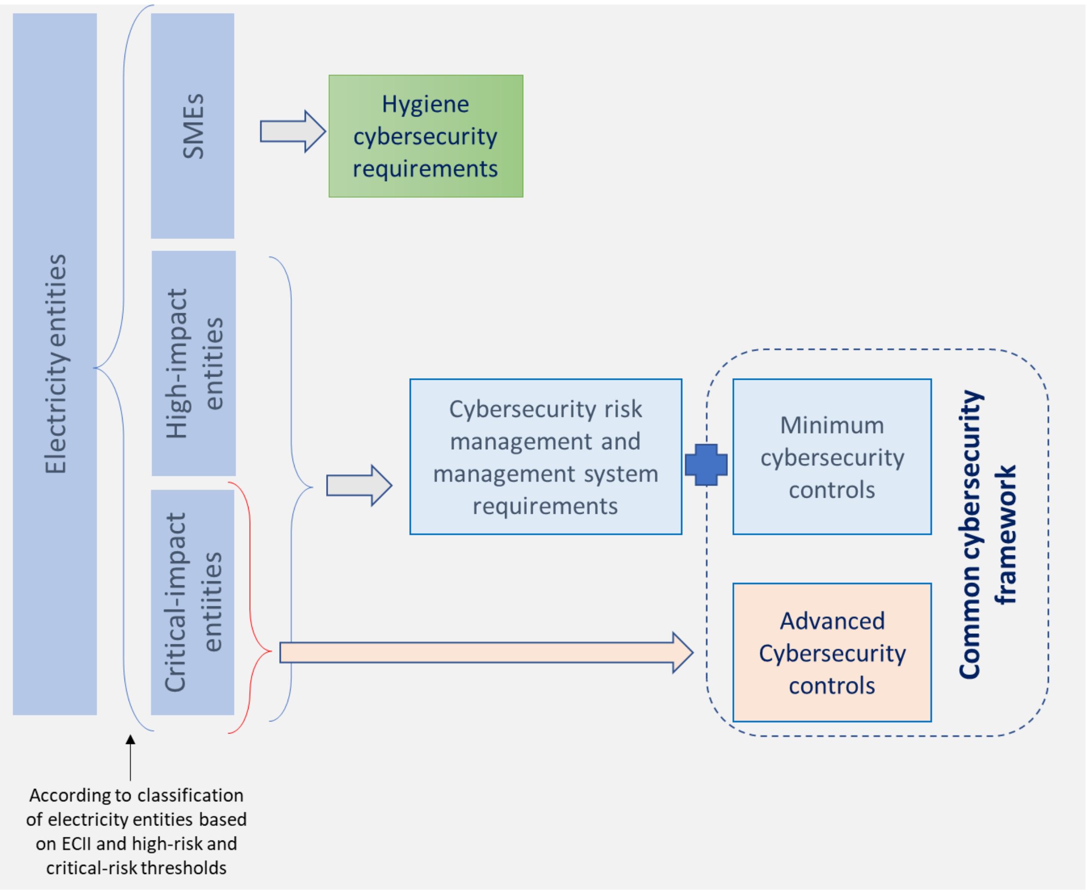

Electricity entities
SMEs
High-impact entities
Critical-impact entiities
Hygiene cybersecurity requirements
Cybersecurity risk management and management system requirements
Minimum cybersecurity controls
Advanced Cybersecurity controls
Common cybersecurity framework
According to classification of electricity entities based on ECII and high-risk and critical-risk thresholds

Figure 7: Risk management measures at entity level.

10.1 PERIMETERS AND SCOPE

The scope of the network code inside an entity is determined by three perimeters: the electricity cybersecurity perimeter, the high-impact perimeter and the critical-impact perimeter (Figure 9).

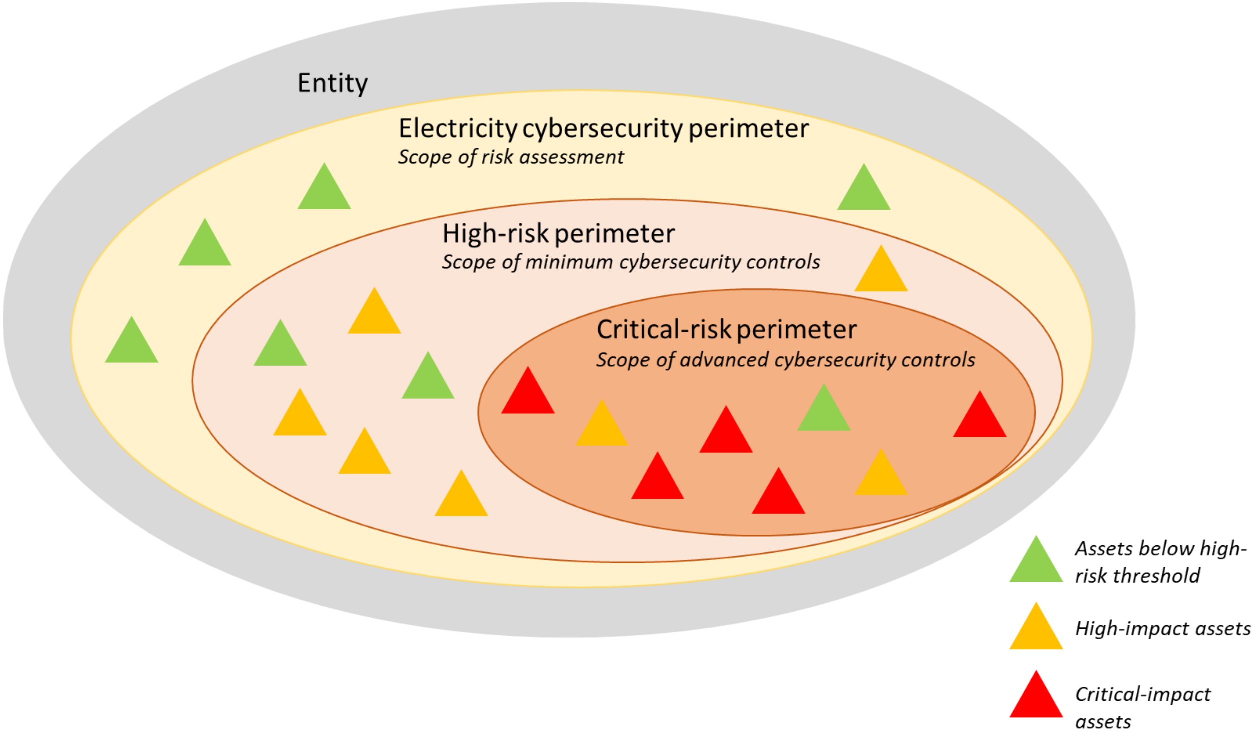

Entity
Electricity cybersecurity perimeter
Scope of risk assessment
High-risk perimeter
Scope of minimum cybersecurity controls
Critical-risk perimeter
Scope of advanced cybersecurity controls
Assets below high-risk threshold
High-impact assets
Critical-impact assets

Figure 9: High-impact and critical-impact perimeters inside entities.

The table below explains how these perimeters are defined and used:

Perimeter	Use	Definition
Elecriticy cybersecurity perimeter	Defines the scope of the cybersecurity risk assessment	Contains all assets needed for union-wide high-impact and critical-impact processes
High-impact perimeter	Defines the scope of the minimum cybersecurity controls	Contains all high-impact assets and allows entities to control access to them at the perimeter
Critical-impact perimeter	Defines the scope of the minimum cybersecurity controls	Contains all critical-impact assets and allows entities to control access to them at the perimeter

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

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

- Determine the electricity cybersecurity perimeter by identifying all assets supporting the union-wide high-impact and critical-impact processes.
- For each business process inside the electricity cybersecurity perimeter, 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.

- If the ECII is above the high-impact (resp. critical-impact) threshold, the process is considered as high-impact (resp. critical-impact).
- Determine all the high-impact (resp. critical-impact) assets as the assets needed for the high-impact (resp. critical-impact) processes.
- Determine a perimeter containing all high-impact (resp. 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 consists for instance of firewalls, gateways, proxy servers, and stepping stones.

The perimeter can be determined by identifying the physical and network security zones that contain the high-impact and critical-impact methodologies. A zoning model such as defined in the IEC 62443 method can be useful for this purpose.

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

Similarly, the critical-impact perimeter may contain high-impact asset. The advanced cybersecurity control 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 critical-impact perimeter.

10.2 CYBERSECURITY RISK MANAGEMETN 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 assessments.

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

Requiring a specific cybersecurity risk assessment method 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 method would require entities to retrain their personnel to a new method and to redo the risk assessments that they have already been performed.

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 and NRA 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 27005:2011 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 harmonized cybersecurity risk matrix defined by the cybersecurity risk working group in the Union-wide cybersecurity risk assessment. The matrix ensures that all relevant consequences are analyzed using objective measures. It also ensures that CS-NCA and NRA 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 the Union-wide, regional, and member state level will also be based on ISO/IEC 27005. So, the methodologies at all level will be similar, as required by the framework guidelines.

10.3 CYBERSECURITY MANAGEMENT SYSTEM

The network code requires that all entities set up a cybersecurity management system system (ISMS, e.g. 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. The management system is more effective because it makes top management at entities explicitly responsible for managing cybersecurity risks and 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. Security becomes part of the entities DNA – this goes far beyond the simple implementation of controls.

The management system creates an internal feedback loop (“plan-do-check-act cycle”) in which entities look for problems in the effectiveness of controls and fix them continuously. Such a loop is needed to ensure that essential undertakings maintain their target level of security in the long run. specially in larger organization there will potentially be 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. Electricity undertakings must have a structural way, as well as implemented processes to deal with such problems, and to involve management to ensure resources are available for this.

The management system is more cost-efficient because audit time can be restricted. Audits would focus on the correct and effective implementation of the management system itself. If the management system is working well, it will over time ensure the effective implementation of the cybersecurity controls. So, not all controls need to be audited in detail be an independent party. Instead, the party can take a random sample of control to verify that internal control processes in the entity are working correctly.

The network code includes general requirements to a management system, mainly derived from the ISO/IEC 27001 standard. The network code does however not require that this standard is followed. Management systems based on other standards, should also be able to meet these requirements.

10.4 VERIFICATION OF THE COMMON CYBERSECURITY REQUIREMENTS

Based on the Framework Guideline the Network Code shall ensure 3 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 an independent third-party
3. Inspections by the CS-NCA or NRA based on a framework of legal obligations

As the network code on Cybersecurity shall ensure a minimum level of Cybersecurity for all European 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 of 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 a 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 verified framework of legal obligations or the peer-review in their country but they have to ensure and constantly proof that the quality is equivalent to a third party certification.

10.5 CYBERSECURITY INSPECTIONS

Measures for supervision or enforcement imposed on critical-impact entity and high-impact entity have to be effective, proportionate and dissuasive, considering the circumstances of each individual case.

Therefor network code ensures that CS-NCAs and/or NRAs, where exercising their supervisory tasks and have the power to subject critical-impact and high-impact entities to:

a) on-site individual and coordinated multi-site joint inspections and off-site supervision, including random checks, especially following a cybersecurity incident, or when the network of CSIRTs will signal an imminent risk related to cybersecurity of critical systems, processes, operations that take part to the cross-border electricity flows;

b) random inspections aimed to verify the conformity on risk assessments and of their results;

requests of information necessary to assess the cybersecurity measures adopted by a critical-impact / high-impact entity, including documented cybersecurity policies, as well as compliance with minimum or advanced requirements.

11 HARMONISING PRODUCT AND SYSTEM REQUIREMENTS AND VERIFICATION

To support high-impact and critical-impact entities in implementing the supply chain security controls, the network code tasks the cybersecurity working group with two activities:

- Developing harmonized security requirement sets for products and systems
- Developing verification methodologies to determine if a product or system meets these requirements

This section describes why the working group was tasked with these activities, and how it plans to perform them.

11.1 HARMONIZING SECURITY PROCUREMENT REGUIREMETNS FOR ICT PRODUCTS, ICT SERVICES AND ICT PROCESSES

During the preparation of the network code, different ways were considered to support entities in procuring products and systems with which they can implement the cybersecurity controls. These include the development of procurement protocols and templates, and the possibly mandatory use of a European certification scheme. The drafting team has chosen for procurement requirements and verification schemes, because it considers them the easiest and most cost-effective way for entities to procure secure products and systems.

Entities can integrate requirement sets into their procurement processes without major changes. Procurement templates and protocols would be more difficult to integrate, as they would require adaptations to national laws and procurement strategies at entities.

If the cybersecurity working group produces requirement sets aligned with the cybersecurity controls and reviewed by ACER and ENISA, many if not most entities can be expected to use them. A survey by ENTSO-E has shown that most TSOs are already using security requirements in procurement. All entities will be required to do so by the supply chain security controls in the network code. Entities will look for existing standards for these requirements. Most TSOs are now for instance using the IEC 62443 standard or the BDEW whitepaper.

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 the requirements.

- **DELIVERABLE**

The cybersecurity risk working group 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 working group 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.

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 for requirements to system integrators
- IEC 62443-3-3 for technical 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
- The BDEW whitepaper

• METHODOLOGY

Working with representatives of all critical-impact entities, the working group selects which products and systems they will develop requirement sets for. Significant effort is required to develop the 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 working group will first define a reference architecture describing the products and services at critical-impact entities. Different entities and suppliers often use different names for similar products and systems. To be able to harmonize them, a common naming must be agreed. 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 and verification. This analysis involves multiple factors, such as:

- The criticality of the product or system according to the cross-border 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 working group will then make a proposal for the products or systems to work on. They will ask ACER and ENISA for a recommendation on this proposal. ENTSO-E and the EU-DSO entity will make a final decision.

The working group will then create a set of security requirements for the selected product or system based on the cross-border risk assessment. 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.

11.2 VERIFICATION SCHEMES FOR ICT PRODUCTS, ICT SERVICES AND ICT PROCESSES IN THE ELECTRICITY SECTOR

The working group will develop a verification scheme to assure if a product or system meets the security requirements.

Harmonizing the verification schemes further lowers the costs and reduces risks during procurement. With a clear verification scheme 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.

European cybersecurity verification schemes will be used in the verification scheme whenever possible, as they would offer the greatest cost reduction and would benefit from the certification infrastructure that the ENISA and the EU are creating. The cybersecurity working group is however allowed to choose other verification methodologies if suitable schemes are not yet available.

- **DELIVERABLE**

A verification scheme is a method to verify (part of) the harmonized security requirements in such a way that the verification results can be reused by different entities. The verification scheme will usually be linked to a specific requirements sets, but could also cover multiple sets.

The cybersecurity working group would create a document describing the scheme, covering:

- The methodologies to be used to verify the requirements
- The measures to ensure that the methodologies are used consistently
- The approach for sharing results of the verification

A scheme may use various verification methodologies, such as penetration tests, documentation reviews, audits, code reviews, self-assessments, maturity models, and functional tests. Measures to ensure consistency can include rules for keeping evidence, accrediting only certain parties to do the verification, and peer reviews between these parties. Results could be shared through a certificate, a public test report, or a test report that the supplier only shares with parties procuring the product or system.

Ideally, a European cybersecurity certification scheme (as defined in the Cybersecurity Act) is used to verify all the requirements. The verification scheme then is simply the same as the certification scheme. If the requirements for instance derive from IEC 62443-4-1 and 4-2, it may be possible in the future to verify them using the ICCS scheme for industrial components, now under development by the JRC. To use the certification scheme, the requirement set would have to be developed in a specific format, such as a generic Component Context Analysis for the ICCS scheme.

If no European cybersecurity certification scheme is available to verify all requirements, the verification scheme can still use the certification schemes in two ways:

- By requiring a certificate to verify part of the requirements or part of the product or system. For instance, if a data concentrator uses a secure element to protect against physical threats, the verification scheme could require the secure element to be certified under the EUCC scheme.

- By adapting a certification scheme through sector-specific guidelines. The guidelines can specify 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 vulnerabilities found. The SOG-IS group has been successful with this approach in applying Common Criteria to smart cards.

- **METHODOLOGY**

The ENTSO-E and the EU DSO entity will develop a verification methodology for each set of harmonized security procurement requirements.

For the verification methodologies, ENTSO-E and the EU DSO entity will start with the current methodologies entities are using to verify requirements for the product or system. They will adjust the methodologies based on the cross-border risk assessment at regional level. The depth and coverage of the methodologies should be enough to provide assurance that the identified threats are mitigated.

The measures to ensure consistency and approach for sharing results is developed in workshops with security specialists and procurement officers from entities, and suppliers. The choices depend not only on the security risks, but also on the structure of the market for the product or system. For larger more mature markets, more formal methodologies such as certification may be applied. For innovative and emerging markets, more lightweight methodologies could be applied.

12 ESSENTIAL INFORMATION FLOWS INCIDENT AND CRISIS MANAGEMENT

Article 37: Role ole of CSIRTs and Competent Authority if a cyber-incident or cyber attack

Paragraph1: The target in this title VIII is to follow NIS Directive with “competent authority or CSIRT” responsible to collect and disseminate information

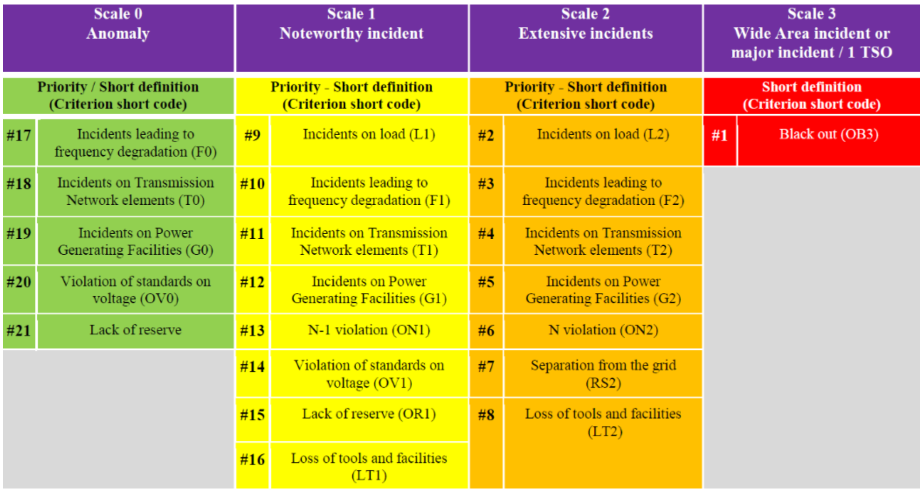
Paragraph3: one appointed CSIRT can delegate responsibility for one electricity entity to one other appointed CSIRT.
It may be particularly appropriate for multi-national Electricity Entities with assets in several EU countries and in the case National CSIRT may prefer specialize specific activities.

Paragraph5.b: the target is to receive efficient information to organize effectively the defence of electricity entities

Paragraph 5.d & 5.e.: In a case, that the vendor cannot deliver a patch, but other actionable mitigation measures are known, the information about a 0 day vulnerability and the mitigation measure has to sent out to all electricity entities, that they have the chance to find out if there are effected and in the case they are effected, to implement the mitigation measure as soon as possible.

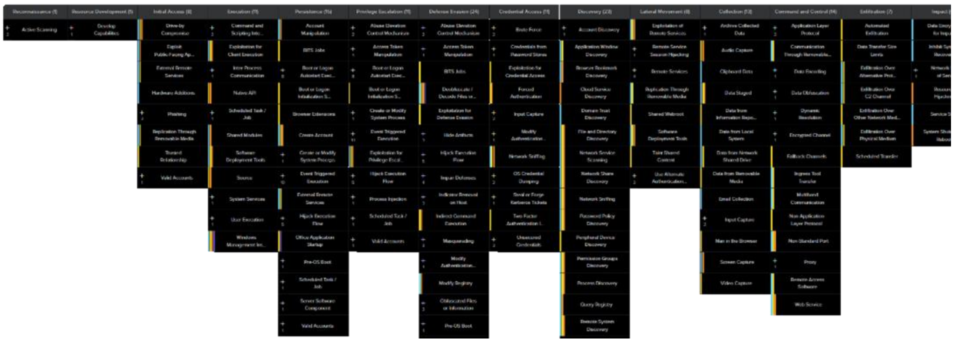
Paragraph 7:

- “The criticality of the asset exposed that will be determined during the asset inventory”: the asset inventory should lead to classify assets according to a methodology ranking assets as it is stated in the ENTSO-E ICS methodology.



Scale 0 Anomaly		Scale 1 Noteworthy incident		Scale 2 Extensive incidents		Scale 3 Wide Area incident or major incident / 1 TSO	
Priority / Short definition (Criterion short code)		Priority - Short definition (Criterion short code)		Priority - Short definition (Criterion short code)		Short definition (Criterion short code)	
#17	Incidents leading to frequency degradation (F0)	#9	Incidents on load (L1)	#2	Incidents on load (L2)	#1	Black out (OB3)
#18	Incidents on Transmission Network elements (T0)	#10	Incidents leading to frequency degradation (F1)	#3	Incidents leading to frequency degradation (F2)		
#19	Incidents on Power Generating Facilities (G0)	#11	Incidents on Transmission Network elements (T1)	#4	Incidents on Transmission Network elements (T2)		
#20	Violation of standards on voltage (OV0)	#12	Incidents on Power Generating Facilities (G1)	#5	Incidents on Power Generating Facilities (G2)		
#21	Lack of reserve	#13	N-1 violation (ON1)	#6	N violation (ON2)		
		#14	Violation of standards on voltage (OV1)	#7	Separation from the grid (RS2)		
		#15	Lack of reserve (OR1)	#8	Loss of tools and facilities (LT2)		
		#16	Loss of tools and facilities (LT1)				

- The severity could be a mix of MITRE ATT&CK framework



Reconnaissance (1)	Resource Development (1)	Initial Access (8)	Execution (11)	Persistence (15)	Privilege Escalation (11)	Defense Evasion (24)	Credential Access (11)	Discovery (22)	Lateral Movement (8)	Collection (13)	Command and Control (14)	Exfiltration (7)	Impact (
Active Scanning	Develop Capabilities	Drive-by Compromise	Command and Scripting Inte...	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Data Encry for Imp
		Exploit Public-Facing Ap...	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Remote Service Session Hijacking	Audio Capture	Communication Through Removable...	Data Transfer Size Limits	Inhibit Sy Recov
		External Remote Services	Inter-Process Communication	Boot or Logon Autostart Exec...	Boot or Logon Autostart Exec...	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Remote Services	Clipboard Data	Data Encoding	Exfiltration Over Alternative Prot...	Network of Ser
		Hardware Additions	Native API	Boot or Logon Initialization S...	Boot or Logon Initialization S...	Deobfuscate / Decode Files or...	Forced Authentication	Cloud Service Discovery	Replication Through Removable Media	Data Staged	Data Obfuscation	Exfiltration Over C2 Channel	Resour Hijack
		Phishing	Scheduled Task / Job	Browser Extensions	Create or Modify System Process	Exploitation for Defense Evasion	Input Capture	Domain Trust Discovery	Shared Webroot	Data from Information Repo...	Dynamic Resolution	Exfiltration Over Other Network Med...	Service S
		Replication Through Removable Media	Shared Modules	Create Account	Event Triggered Execution	Hide Artifacts	Modify Authentication...	File and Directory Discovery	Software Deployment Tools	Data from Local System	Encrypted Channel	Exfiltration Over Physical Medium	System Shu Reboo
		Trusted Relationship	Software Deployment Tools	Create or Modify System Process	Exploitation for Privilege Escal...	Hijack Execution Flow	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Scheduled Transfer	
		Valid Accounts	Source	Event Triggered Execution	Hijack Execution Flow	Impair Defenses	OS Credential Dumping	Network Share Discovery	Use Alternate Authentication...	Data from Removable Media	Ingress Tool Transfer		
			System Services	External Remote Services	Process Injection	Indicator Removal on Host	Steal or Forge Kerberos Tickets	Network Sniffing		Email Collection	Multiband Communication		
			User Execution	Hijack Execution Flow	Scheduled Task / Job	Indirect Command Execution	Two Factor Authentication I...	Password Policy Discovery		Input Capture	Non-Application Layer Protocol		
			Windows Management Ins...	Office Application Startup	Valid Accounts	Masquerading	Unsecured Credentials	Peripheral Device Discovery		Man in the Browser	Non-Standard Port		
				Pre-OS Boot		Modify Authentication...		Permission Groups Discovery		Screen Capture	Proxy		
				Scheduled Task / Job		Modify Registry		Process Discovery		Video Capture	Remote Access Software		
				Server Software Component		Obfuscated Files or Information		Query Registry			Web Service		
				Valid Accounts		Pre-OS Boot		Remote System Discovery					

- The mix of criticality & severity should bring to classification Medium / to foloow / important / high / cirtical

		Critical asset			
		Scale 0 Anomaly	**Scale 1** Noteworthy Incident	**Scale 2** Etensive incidents	**Scale 3** Wide are 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

Paragraph 8: At the moment, even the national CSIRTs have no european wide tool in place to exchange information. The EU CSIRT Network plan to implement such information sharing tool. It should be examined whether this tool can also be used for the purposes of the European energy sector.

Article 38: Data collection, sanitisation and dissemination

Paragraph 1.a.iii: Actions includes sending alerts inside the electricity entity for example to the operational teams in order to implement mitigations (e.g. patches, necessary firewall configurations and other necessary configurations).

Paragraph 1.b: Over the time we expect, that Artifical Intelligence or Machine Learning will be able to support the cyber security monitoring and incident response procedures by not replacing but supporting the human CSOC analysts. Therefore, there is a possibility to implement such solutions in the future, but that is not mandatory due to the fact, that these solutions are still under development and we have to use stable market solutions.

Paragraph 1.d: Single Point of Contact shall not be person-dependent but may be based at least on functional email-address, backup email address and a phone number. Single Point of Contact was left out of SOC capabilities because we think that each entities should have the choice where to place the SPoC (inside the SOC or not).

Paragraph 2: this article should avoid double reporting by sending the same information and in addition some more information.

Article 39: Detection of incidents and handling of incident related information

Examples of involvement in incident management are provided in Figure 4. Incident X illustrates a smaller incident that is handled locally by an electricity undertaking and its MSSP without the involvement of any other entities on the network.

Incident Y illustrates a larger incident impacting two electricity undertakings. Here, the national CSIRT is involved to support the SOCs of the affected undertakings. In this case the incident shall be handled by personnel from the affected electricity undertakings with support and coordination from the national CSIRT. The affected undertakings SOCs or MSSP can establish a virtual ad hoc CSIRT if it seems helpful and resources are available

Incident Z illustrates an incident with cross-border effects, in which, an electricity undertaking in state A and one or more undertaking(s) in state C, are affected. In case of incident Y, the affected undertakings can establish a coordination ad hoc team. The overall coordination of the incident with cross-border effect is managed by Joint Cyber Unit. The SOCs of the involved electricity undertakings shall, upon request, be supported by national CSIRTs or by the the Joint Cyber Unit. In cases of cross-border incidents, overall coordinating national CSIRT shall keep the relevant Regional Coordination Centre updated with summaries of the situation on a regular basis. The CSIRTs network shall be informed by this coordination national CSIRT of ongoing developments and changes at regular intervals. The Joint Cyber Unit dealing with cross-border incidents should also be able to count on the support of ENISA and other EU resources.

The Regional Coordination Centres, ENTSO-E and the EU-DSO Entity, shall handle incidents at their respective level (EU Level). In cases of larger incidents, and under the condition that they will become members of the CERT-EU, they will be able to receive support through the CERT EU and from the Joint Cyber Unit.

The electricity undertaking has to follow the reporting guidelines developed by the NIS coordination group pursuant to Article 14(3) of the NIS Directive, including the circumstances for reporting incidents and the format and procedure for such reporting. The CSIRTs Network shall be consulted when defining criteria to identify Reportable Cyber Security Incidents.

Joint Cyber Unit will report large-scale incidents[1] (incidents with cross boarder effect) arising from cyber-attacks to Europol's European Cybercrime Centre as soon as there is a reasonable certainty that the disruption is the result of a cyber-attack.

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

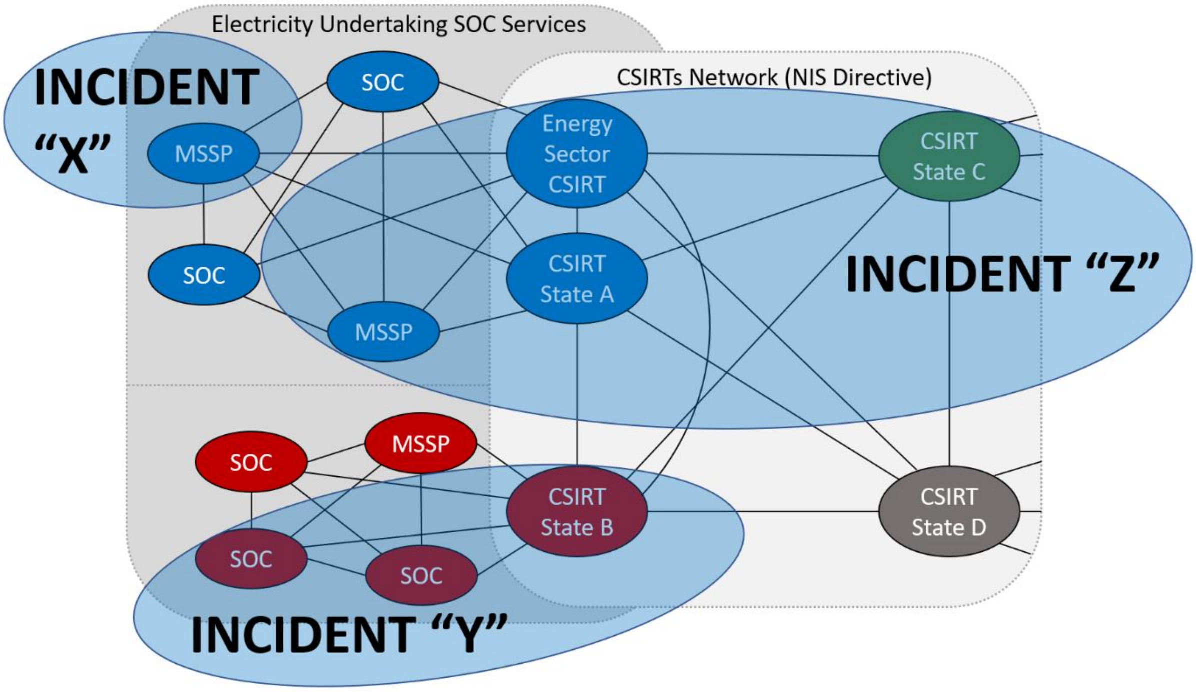


Figure 4: Examples of involvement of response environments for incident handling on electricity undertaking (X), national (Y) and regional (Z) level. Involvement shall follow the principle of proximity.

Paragraph 2: Cross border cybersecurity incidents shall be dealt in accordance with the principle of proximity, which implies that an incident shall be handled as closely as possible, both geographically and organisationally.

Article 40: Crisis management

Paragraph 1: As the cybersecurity root cause could not be easy to find in a first step, we believe, any cross border electricity crisis should lead to an investigation to be sure that there is any cybersecurity root cause.

Paragraph 2: The ad'hoc coordination Group should be organized alongside crisis management group as a supporting group. But according to the crisis, it could be completely in the crisis management group.

Article 42: ECEWC

An early warning system can be desribed as a solution for threat information gathering, processing and notification of threat information. It is about systematically providing the right information to the right people at the right time – connecting the dots across relevant actors.

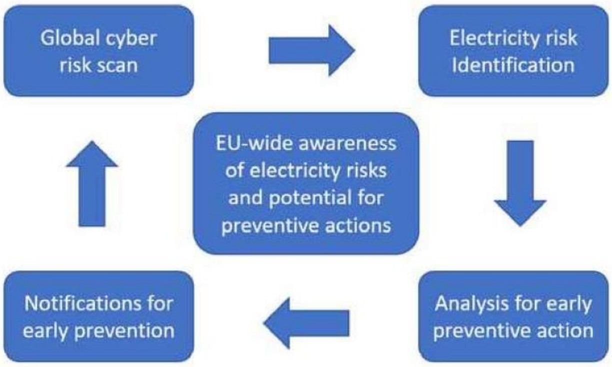

Global cyber risk scan
Electricity risk Identification
EU-wide awareness of electricity risks and potential for preventive actions
Notifications for early prevention
Analysis for early preventive action

Figure 1 : Illustration of steps of a ECEWC for the EU 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.

Paragraph 2 (b) : The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information.

13 ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

The overall target is that each critical-risk entity shall have at least two cybersecurity exercises within every 3 years: one internal or national and one regional or cross regional.

Article 43 : Regional or cross regional cybersecurity exercises

Paragraph 1: “system operation region”: definition is given in Art 36 Reg 2019/943 and here: https://documents.acer.europa.eu/Official_documents/Acts_of_the_Agency/Annexes%20to%20the%20DECISION%20OF%20THE%20AGENCY%20FOR%20THE%20C9/ACER%20Decision%2010-2020%20on%20SOR%20-%20Annex%20I.pdf

Paragraph 2: “ENTSO-E shall designate”: we believe some regional exercises should include only national CSIRTs w/o Critical Entities. Consequently, we don’t want ENTSO-E to be forced to include critical entities. This is the reason why we suggest letting ENTSO-E designate the participants.

14 FINAL PROVISIONS

The NCCS will enter into force 20 days after its publication. 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.

Article 49 Transitional provisions

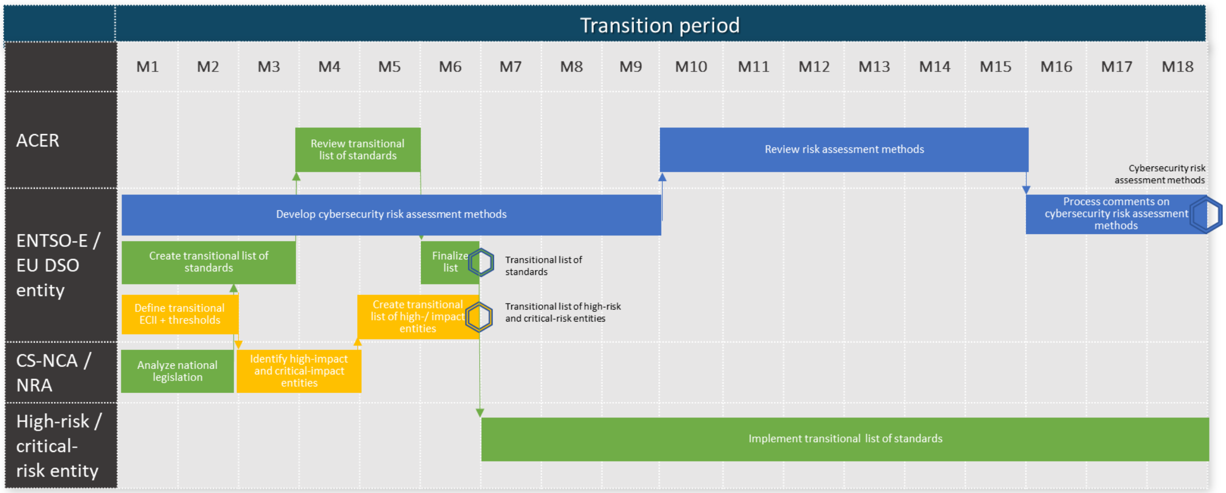
14.1 TRANSITION PHASE

There is no formal transition phase for the harmonized security requirement sets and verification schemes. The cybersecurity risk working group will start developing the requirements sets and schemes when the network code goes 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. Critical-impact entities are expected to arrange their own verification of the requirements.

14.2 TRANSITION PERIOD

A transitional period of 18 months is foreseen between when the network code goes into force and the first risk assessment cycle (see Figure 8). The goal of the transition period is to create all methodologies and information needed to start the risk assessments.



Transition period
M1
M2
M3
M4
M5
M6
M7
M8
M9
M10
M11
M12
M13
M14
M15
M16
M17
M18
ACER
ENTSO-E / EU DSO entity
CS-NCA / NRA
High-risk / critical-risk entity
Review transitional list of standards
Review risk assessment methods
Cybersecurity risk assessment methods
Develop cybersecurity risk assessment methods
Process comments on cybersecurity risk assessment methods
Create transitional list of standards
Finalize list
Transitional list of standards
Define transitional ECII + thresholds
Create transitional list of high-/ impact entities
Transitional list of high-risk and critical-risk entities
Analyze national legislation
Identify high-impact and critical-impact entities
Implement transitional list of standards

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

During the transition period, ENTSO-E and EU DSO entity together with he working groups will create three deliverables:

- The methodologies for the Union-wide cybersecurity risk assessment, the member state risk analysis, and the regional risk assessment.

- 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.
- A transitional list of high-impact and critical-impact entities. 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.

National legislation is included in the transitional list of standards if it is supplied by the CS-NCA to EN.

To compile the transitional list of high-impact and critical-impact entities, ENTSO-E and the EU-DSO entity need help from the CS-NCA. ENTSO-E and the EU DSO entity will provide the CS-NCA with a transitional set of ECII and thresholds. 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 entities then compile the lists into a Union-wide list.

The methodologies for the Union-wide cybersecurity risk assessment, the member state risk analysis, and the regional risk assessment. ACER will provide an opinion on these methodologies.

Article 50 Entry into force

The NCCS will enter into force 20 days after its publication. 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.

15 ANNEXE A basic cybersecurity hygiene requirements

To achieve a minimum level of security the “Review of Cyber Hygiene practices” from the European Union Cybersecurity Agency (ENISA) from September 2017 provide basic cybersecurity hygiene requirements.

All entities including micro and small entities shall at least implement the basic cybersecurity requirements specified in the Annex A.