Supporting document
for the methodologies for cybersecurity risk assessments

1 Introduction

Under Article 18 of the Network Code for Cybersecurity (NCCS), the European Network of Transmission System Operators for Electricity (ENTSO-E) in cooperation with the EU DSO entity (DSO Entity) has developed a proposal for methodologies for cybersecurity risk assessment. This supporting document has been developed jointly by ENTSO-E and DSO Entity to accompany these methodologies. It provides all interested parties with information about the rationale for the risk assessment methodologies.

1.1 Legal status of this document

This document accompanies the methodology for cybersecurity risk assessments and is provided for information purposes only. Consequently, this document is not legally binding.

2 Risk management methodology

The document contains methodologies for risk assessments at three levels: the Union-wide risk assessment, the risk assessment at member state level, and the regional risk assessment.

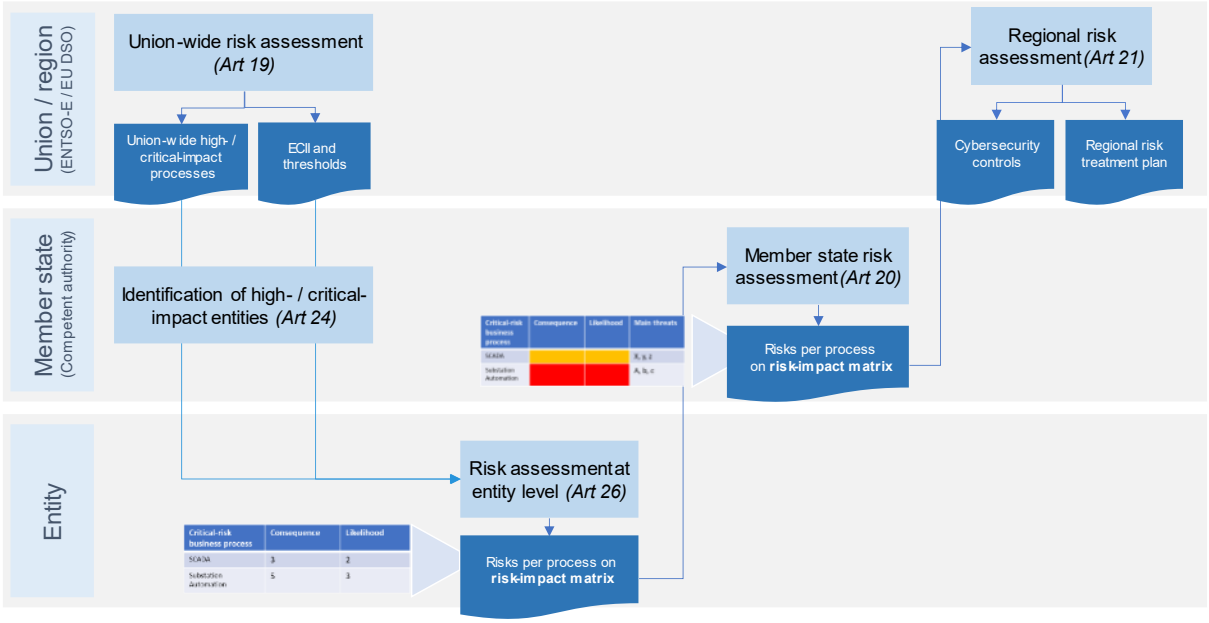


Figure 1: NCCS cybersecurity risk assessment cycle.

No methodology is defined for risk assessments at entity level. Entities may choose their own methodology, as long as it meets the requirements in Article 26 of the NCCS. The document does contain rules to determine the high-impact and critical-impact perimeters during the entity-level risk assessment.

2.1 Title 2: Union-wide cybersecurity risk assessment

Title 2 describes the methodology for the Union-wide cybersecurity risk assessment (see Article 19 of the NCCS). The Union-wide risk assessment is the first step in the risk assessment cycle (see Figure 1). The goal is to identify, analyse, and evaluate the possible **consequences** of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows.

The Union-wide risk assessment acts as a business impact assessment performed at EU level. For processes in the European electricity sector the impact of a cyber-attack compromising of confidentiality, integrity, and availability of information is assessed using the criteria in Annex I.

The Union-wide risk assessment results are formalized in a report that contains the following information (see Article 19 (2) and (3) in the NCCS):

- the Union-wide high-impact and critical-impact processes and, for each process:
    - an assessment of the possible consequences of a cyber-attack affecting the considered process according to the impact metrics defined in Annex I of the cybersecurity risk assessment methodology;
    - the ECII and high-impact and critical-impact thresholds that the competent authorities will use to identify high-impact and critical-impact entities;

- a risk impact matrix that entities and the competent authorities will use to assess the cybersecurity risk at Member State level and at entity level.

The Union-wide cybersecurity risk assessment consists of four steps:

(a) identify processes at the electricity sector level that could affect the operational security of the electricity system;

(b) determine the possible consequences of a cyber-attack compromising the confidentiality, integrity or availability of the information used in them;

(c) identify the Union-wide high-impact and critical-impact processes; and

(d) define the Electricity Cybersecurity Impact Indices (ECII) and high-impact and critical-impact thresholds.

The ECII in point (d) will be defined according to the impact metrics in Annex I. Only metrics relevant to the type of entity and process will be selected to derive the ECII. For instance, metrics on voltage and frequency may only be relevant to TSOs and, in particular, only for processes related to voltage and frequency management. Hence, these metrics will only be considered for such entities and processes.

Impact metrics may be simplified when defining the ECII. Some impact metrics in Annex I may be difficult to compute for individual entities; in that case, another metric could be used to provide a good approximation.

The thresholds for the ECII will be based on the high-impact and critical-impact thresholds defined in Annex II of the Risk assessment methodology.

Thresholds for the ECII take into account that a cyber-attack may affect multiple entities, so that they may be lower than for the impact metric (as defined in Annex II). In fact, an attacker may deliberately attack multiple entities and, even though the individual impacts of these attacks may fall below the defined thresholds, the overall impact may still exceed the thresholds.

How many entities an attacker could attack at the same time needs to be determined in the Union-wide risk assessment.

2.2 Title 3: Cybersecurity risk assessment at member state level

Title 3 describes the methodology for the risk assessments at member state level (see Article 20 of the NCCS). The goal of the member state cybersecurity risk assessment is to identify, and analyse, the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows in one member state.

The cybersecurity risk assessment at member state level consists of four steps:

(a) determine the implementation status of the minimum and advanced cybersecurity controls;

(b) aggregate the risk analysis results from the risk assessments at entity level to determine the consequences and likelihood of a compromise of the confidentiality, integrity or availability of the information used in them;

(c) summarize the information on cyber-attacks and threats gathered pursuant Article 38(3) and (6) of the NCCS; and

(d) recommend additional cybersecurity controls to mitigate high and critical risks to ENTSO-E and DSO Entity.

The member state cybersecurity risk assessment results are formalized in the member state cybersecurity risk assessment report.

The information needed to perform the member state level risk assessment is derived from the entity level cybersecurity risk assessments. In particular, all high-impact and critical-impact entities will report to their competent authority the identified risks according to the same risk impact matrix, defined during the Union-wide risk assessment. Competent authorities will also request additional information from entities to be able to determine which controls could be used to mitigate the risk, and what the residual risk is after the controls have been implemented. The additional information is used in the regional risk assessment to determine the minimum and advanced cybersecurity controls.

The competent authority will aggregate the risks (derived from the entity level cybersecurity risk assessments) to assess the overall risk in the member state.

Additional information on cyber-attack and threats is collected though the defined information sharing process (see Articles 37 and Article 38 of the NCCS).

The competent authority will also gather information about the implementation status of the minimum and advanced cybersecurity controls that are required under the NCCS (see Articles 29 and Article 33 of the NCCS). All this information will later be reported by ENTSO-E and DSO Entity in the comprehensive cross-border electricity cybersecurity risk assessment report.

According to the risks, threats, and implementation status of the minimum and advanced cybersecurity controls, the competent authorities will also recommend additional controls aimed at mitigating the identified risks. They will then estimate the residual risk if these controls are implemented. ENTSO-E and DSO Entity will use the recommended controls to determine additional minimum and advanced cybersecurity controls.

2.3 Title 4: Regional cybersecurity risk assessment

Title 4 describes the methodology for the regional cybersecurity risk assessment (see Article 21 of the NCCS). The regional cybersecurity risk assessment is the last step in the risk assessment cycle (see Figure 1). While the Union-wide risk assessment only considers consequences, the goal of the regional risk assessment is to identify, analyse, and evaluate the **risks** of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows.

The regional risk assessment is the basis for several other documents:

- The regional risk mitigation plans (Article 22 of the NCCS)
- The comprehensive cross-border electricity cybersecurity risk assessment report (Article 23 of the NCCS)
- Updates of the minimum and advanced cybersecurity controls (Article 29 of the NCCS), including the controls in the supply chain (Article 33 of the NCCS)
- Cybersecurity procurement recommendations (Article 35 of the NCCS).

The regional cybersecurity risk assessment consists of five steps:

(a) aggregate the risk analysis derived from the member state risk cybersecurity assessments to determine the consequences and likelihood of a compromise of the confidentiality, integrity or availability of the information used in them;

(b) evaluate the risks analysed in (a);

(c) determine the cybersecurity threats that lead to high and critical risks.

The information needed to perform the regional cybersecurity risk assessment is derived from the member state cybersecurity risk assessment results. In particular, all member states will report to ENTSO-E and DSO Entity the identified risks according to the same risk impact matrix, defined during the Union-wide risk assessment.

ENTSO-E in cooperation with DSO Entity will aggregate the aforementioned risks (derived from the member state cybersecurity risk assessments) to assess the overall risk in the system operation regions.

ENTSO-E and DSO Entity will not validate the risk information received from member states or collect missing information from the member states. For the correctness and completeness of the risk information, they completely rely on the competent authorities, assuming that the received information is correct and up to date.

3 Annex I: Impact metrics

Annex I of the Cybersecurity risk assessment methodology defines the impact metrics. The NCCS in Article 18(3)(a) states that risk impact matrix will measure the consequences of cyber-attacks based on the following criteria:

(i) loss of load;
(ii) reduction of power generation;
(iii) reduction of capacity in the frequency containment reserve;
(iv) loss of capacity for restoration of an electric grid to operation without relying on the external transmission network to recover after a total or partial shutdown (also called 'black start');
(v) the expected duration of an electricity outage affecting customers in combination with the scale of the outage in customer numbers;

All the above criteria have been included as impact metrics in Annex I of the Cybersecurity risk assessment methodology. The related definitions are based on the ENTSO-E Incident Classification Scale. The metric (v) was defined in terms of the System Average Interruption Duration Index (SAIDI), as this is a common reliability metric for the electricity system.

Furthermore, the NCCS allows the risk impact metrics to include any other quantitative or qualitative criteria that could reasonably act as an indicator of the effect of a cyber-attack on cross-border electricity flows. Three additional impact metrics have been added under this provision:

(vi) Incidents leading to frequency degradation
(vii) Violation of standards on voltage
(viii) Reduction of capacity in the other frequency reserves

These metrics were taken from the ENTSO-E Incident Classification Scale. Metrics for impact on frequency and voltage were added, as these factors were not considered in the NCCS list, and potential cybersecurity incidents affecting some TSOs' processes may lead to such impacts. Reduction of the capacity in other frequency reserves was added because such reserves are important for TSOs to respond to incidents, and it was considered insufficient to only include the frequency containment reserves.

4 Annex II: High-impact and critical-impact thresholds

Annex II defines the thresholds for classifying impact as high or critical. The Cybersecurity risk assessment methodology must include criteria to evaluate the impact of cybersecurity risks as high or critical (NCCS Article 18(2)(b)). These criteria are the impact metrics defined in Annex I of the Cybersecurity risk assessment methodology.

Most impact metrics are based on the ENTSO-E incident classification scale (ICS). For those metrics, the thresholds are also taken from the ICS. The high-impact threshold is taken to be the L1 thresholds in the ICS. The critical-impact threshold is taken to be the L2 threshold.

There are two exceptions:

1. For the “loss of load” and “reduction of power generation” impact metrics, the thresholds from the provisional ECII and thresholds have been used. In this way, the classification of entities based on the ECII is consistent with the classification of risk according to the impact metrics. Using different thresholds might result, for example, in high-impact entities not having any associated high-impact risks or in high-impact entities actually having critical impact risks associated.

2. For the “expected duration of outage affecting customers in combination with the scale of the outage in customer numbers impact metric”, the thresholds been derived by looking at expected values for the SAID for European distribution system operators. The *Distribution System Operator Observatory 2022*, conducted by the JRC, shows that SAIDIs are typically between 0 and 150 minutes depending on the type of operator. Most values are around 50 minutes. Hence, an increase of 25 minutes would significantly affect the SAIDI of most operators, while an increase in 50 minutes would in many cases double it.

Separate thresholds are defined for the risk assessments at member state, regional, and Union-wide level.

- For the **Union-wide risk assessment**, the ENTSO-E ICS thresholds from the continental Europe synchronous area are used, as this is the largest synchronous area. For the thresholds for loss of load and reduction of power generation**,** the thresholds used in the regional risk assessments for the central Europe system operation region are used. The central Europe region is used, because it is the largest region, and it is connected to all other regions. South Eastern Europe and South Western Europe are in the same synchronous area, and the Nordic and Baltic regions are connected through interconnectors.

- For the **regional risk assessments**, the thresholds from the ENTSO-E ICS are taken from the synchronous area in which the system operation region is located. For the central Europe system operation region, the thresholds of the Continental Europe synchronous area are used, because all member states in the region except Ireland are in this synchronous area. For the thresholds for loss of load and reduction of power generation, the minimum of ECII threshold over all countries in the region is taken. The reason to take the minimum is that in the Union-wide risk assessment we need to determine if a compromise of a process can cause a high-impact incident in one of the member states. If a process controls more than the minimum high-impact threshold over the member states in the region, it could potentially cause a high-

impact incident in the country with the lowest threshold. For the central Europe region, Ireland is excluded when this minimum is taken, as otherwise the critical-impact threshold would be unrealistically low.

- For the **member state risk assessments**, each member state uses the thresholds from the system operation region it is in. Only for the thresholds for loss of load and reduction of power generation, the ECII thresholds for the member state are used.

5 Annex III: List of cyber threats

The NCCS requires the cybersecurity risk assessment methodologies to include a list of cyber threats to be considered (Article 18(2)(a)). This list is defined in Annex II of the Cybersecurity risk assessment methodology.

The threat list includes the five supply chain threats listed in the NCCS ((Article 18(2)(a))):

(i) a severe and unexpected corruption of the supply chain;

(ii) the unavailability of ICT products, ICT services, or ICT processes from the supply chain;

(iii) cyber-attacks initiated through actors in the supply chain;

(iv) leaking of sensitive information through the supply chain, including supply chain tracking;

(v) the introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain.

The following additional threats have been considered in the methodology, according to Annex C of the ISO/IEC 27005:2011:

(vi) attacks through communication networks;

(vii) attacks through removable media;

(viii) unauthorized system access;

(ix) malware intrusion;

(x) social engineering;

(xi) cyber-attack enabled by unauthorized physical access;

(xii) insider threats.

As the NCCS is only concerned with cyber-attacks, only threats of deliberate origin (type “D” in ISO/IEC 27005:2011 Annex C) have been considered, such as threats related to information compromise, unauthorised actions and function compromise. Physical damage, natural events, loss of essential services, and disturbance due to radiation are not included in the threat list.

The defined threat list was kept short by aggregating similar threats, to facilitate its use by the entities. The threat list may be extended at a later stage to include significant threats resulting from the regional risk assessment.

6 Annex IV: Entity reporting template

Annex IV contains a template for entities to report the results of the cybersecurity risk assessment at entity level. Entities will be required to fill in one table with the risk information per Union-wide high- or critical-impact process. The template includes references to the relevant articles in the NCCS and the methodology.

7 Annex V: Member state reporting template

Annex V contains a template for competent authorities to report the results of the member state cybersecurity risk assessment. Competent authorities will be required to fill in one table with the risk information per Union-wide high- or critical-impact process. The template includes references to the relevant articles in the NCCS and the methodology.

8 Mapping to the NCCS requirements

The table below shows how the methodology fulfils all the requirements defined in Article 18 of the NCCS related to the cyber risk assessment methodologies.

Requirement from NCCS Article 18	Methodology section	Notes
(1) By [OP: please insert the date = within nine months after the entry into force of this Regulation], the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and following a consultation with the NIS Cooperation Group, shall submit a proposal for the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level.	*Not applicable*	
(2) The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall include:	*Not applicable*	
(a) a list of cyber threats to be considered, including at least the following supply chain threats: (i) a severe and unexpected corruption of the supply chain; (ii) the unavailability of ICT products, ICT services, or ICT processes from the supply chain; (iii) cyber-attacks initiated through actors in the supply chain; (iv) leaking of sensitive information through the supply chain, including supply chain tracking; (v) the introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain	Annex II	
(b) the criteria to evaluate the impact of cybersecurity risks as high or critical, using defined thresholds for consequences and likelihood;	Annex I	Thresholds for likelihoods are not included, as the goal is to evaluate the impact. Such thresholds will be included in the risk impact matrix in the Union-wide risk assessment report.
(c) an approach to analyse the cybersecurity risks coming from legacy systems, the cascading effects of cyber-attacks and the real-time nature of systems operating the grid;	Article 6(2) Annex II	The risk to legacy systems is analysed as part of the threats of attacks through removable media, unauthorized system

		access, and malware intrusion in Annex II. Cascading effects are analysed as part of the analysis of consequence in the Union-wide risk assessment in Article 6(2). The risks to the real-time nature of systems operating the gris is analysed as part of the threat of attacks through communication networks in Annex II.
(d) an approach to analyse the cybersecurity risks coming from the dependency on a single supplier of ICT products, ICT services or ICT processes.	Article 20(3)	
(3) The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall assess cybersecurity risks using the same risk impact matrix. The risk impact matrix shall: (a) measure the consequences of cyber-attacks based on the following criteria: (i) loss of load; (ii) reduction of power generation; (iii) loss of capacity in the primary frequency reserve; (iv) loss of capacity for restoration of an electric grid to operation without relying on the external transmission network to recover after a total or partial shutdown (also called 'black start'); (v) the expected duration of an electricity outage affecting customers in combination with the scale of the outage in customer numbers; and (vi) any other quantitative or qualitative criteria that could reasonably act as an indicator of the effect of a cyber-attack on cross-border electricity flows. (b) measure the likelihood of an incident as the frequency of cyber-attacks per year.	Article 6 Article 12 Article 19	The risk impact matrix itself will be defined in the Union-wide risk assessment report
(4) The cybersecurity risk assessment methodologies at Union level shall describe how the ECII values for high-impact and critical-impact thresholds will be defined. The ECII shall enable entities to estimate with the help of the criteria referred to in paragraph 2 point (b), the impact of the risks on their business process during the business impact assessments they perform pursuant to Article 26(4) point (c)(i).	Article 8	

(5) The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the Electricity Coordination Group on the proposals for the cybersecurity risk assessment methodologies that are developed pursuant to paragraph 1.	*Not applicable*	