CYBERSECURITY RISK ASSESSMENT METHODOLOGIES

Proposal of all TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity, for cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level in accordance with Article 18 of the Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code for cybersecurity aspects of cross-border electricity flows

Table of Contents

TSOS, WITH THE ASSISTANCE OF ENTSO FOR ELECTRICITY AND IN COOPERATION WITH THE EU DSO ENTITY, TAKING INTO ACCOUNT THE FOLLOWING:

Whereas

(1) This document provides a methodology for cybersecurity risk assessments (hereafter referred to as "the methodology") in accordance with Article 18, of Commission Regulation (EU) 2024/1366 establishing a network code for cybersecurity aspects of cross-border electricity flows (hereafter referred to as 'NCCS Regulation').

(2) The methodology for cybersecurity risk assessments takes into account the general principles and goals set in the:

a) NCCS Regulation;
b) Directive (EU) 2022/2555 [Directive on measures for a high common level of cybersecurity across the Union; ('NIS 2 Directive')];
c) Regulation (EU) 2019/941 of the European Parliament and of Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/ (hereafter referred to as the 'Risk Preparedness Regulation');
d) as well as Regulation (EU) 2019/943 of the European Parliament and of Council of 5 June 2019 on the Internal Market for Electricity (recast) (hereafter referred to as the 'Electricity Regulation').

(3) 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 in accordance with Article 18 of the NCCS Regulation.

SUBMIT THE FOLLOWING PROPOSAL FOR THE METHODOLOGY FOR CYBERSECURITY RISK ASSESSMENTS TO ALL NCAS

TITLE 1

General provisions

Article 1

Subject matter and scope

(1) This methodology for cybersecurity risk assessments specifies how to perform cybersecurity risk assessments,

a. at Union level in the Union-wide cybersecurity risk assessment;
b. at regional level in the regional cybersecurity risk assessment;
c. at member state level in the member state cybersecurity risk assessment.

(2) At each level, the risk assessments shall only consider consequences to the operational security of the grid. It shall not consider legal, financial, or reputational damage.

(3) The assessments shall only consider consequences of cyber-attacks, that is attempts with malicious intent to gain access to network and information systems. It shall not consider cybersecurity incidents caused by threats with no malicious intent.

Article 2
Definitions

(1) For the purposes of this methodology for cybersecurity risk assessments, the terms used shall have the meaning given to them in Article 3 of the NCCS Regulation, Article 6 of the NIS 2 Directive, Article 2 of the Risk Preparedness Regulation and Article 2 of the Electricity Regulation.

(2) In this methodology for cybersecurity risk assessments, unless the context clearly indicates otherwise:

(a) the singular also includes the plural and vice versa;

(b) the table of contents and headings are inserted for convenience only and do not affect the interpretation of this methodology for cybersecurity risk assessments;

(c) any reference to legislation, regulations, directives, orders, instruments, codes, or any other enactment shall include any modification, extension, or re-enactment of it when in force; and

(d) any reference to an Article without an indication of the document shall mean a reference to this methodology for cybersecurity risk assessments.

TITLE 2
Union-wide cybersecurity risk assessment

Article 3
Objective of the Union-wide risk assessment

(1) The objective of the Union-wide cybersecurity risk assessment 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.

(2) During the Union-wide cybersecurity risk assessment, ENTSO-E in cooperation with the EU DSO entity shall:

(a) identify processes at the electricity sector level that could affect the operational security of the electricity system, pursuant to Article 4 of the present methodology;

(b) assess the possible consequences of a cyber-attack compromising the confidentiality, integrity or availability of the information used in them, pursuant to Article 5 of the present methodology;

(c) identify the Union-wide high-impact and critical-impact processes, pursuant to Article 6 of the present methodology; and

develop the Electricity Cybersecurity Impact Indices (ECII) and high-impact and critical-impact thresholds, pursuant to Article 7 of the present methodology.

Article 4
Identification of electricity sector processes

At the start of the Union-wide cybersecurity risk assessment, ENTSO-E in cooperation with the EU DSO entity shall create a list of potential Union-wide high-impact and critical-impact processes. The list shall contain all processes that may affect the operational security of the electricity system. The processes may involve any of the entities in Article 2(1) of the NCCS Regulation, or a combination of such entities.

Article 5
Analysis of consequences

(1) For every process on the list of potential Union-wide high-impact and critical-impact processes defined pursuant to Article 4 of the present methodology, ENTSO-E in cooperation with the EU DSO entity shall analyse the possible consequences if the confidentiality, integrity, or availability of the information used is compromised by a cyber-attack using the impact metrics in Annex I.

(2) When analysing the possible consequences, ENTSO-E in cooperation with the EU DSO entity shall consider:
   (a) intentional compromises through a cyber-attack, possibly affecting multiple entities;
   (b) indirect consequences, including cascading effects;
   (c) controls that would limit the consequences of a cyber-attack, such as backup processes or manual workaround processes; and
   (d) possible changes in the consequences during the next three years because of trends in the electricity sector or other developments.

(3) When analysing the possible consequences of a compromise of availability, ENTSO-E in cooperation with the EU DSO entity shall determine for each process the relevant duration over which an outage should be analysed. They shall select a duration that is long enough so that all relevant consequences have materialized. But they shall also take into account if the outage lasts very long, emergency measure will be taken to resolve the outage or limit the consequences. They shall report the relevant duration used in the analysis in the Union-wide risk assessment report.

Article 6
Identification of Union-wide high-impact and critical-impact processes

(1) For every process on the list of potential Union-wide high-impact and critical-impact processes defined pursuant to Article 4 of the present methodology, ENTSO-E in cooperation with the EU DSO entity shall evaluate if the consequences are above the high-impact and critical-impact thresholds in Annex II.

(2) If one of the impact metrics is above the critical-impact threshold, ENTSO-E in collaboration with the DSO entity shall identify the process as a critical-impact process.

(3) If one of the impact metrics is above the high-impact threshold and the process has not been identified as

critical-impact, ENTSO-E in collaboration with the DSO entity shall identify the process as a high-impact process.

Article 7

Definition of ECII and high-impact and critical-impact thresholds

For each high-impact and critical-impact process identified in Article 6 of the present methodology, ENTSO-E in cooperation with the EU DSO entity shall develop ECII and high-impact and critical-impact thresholds, as follows:

(1) Identify which of the types of entities listed in Article 2 of the NCCS are involved in the process.

(2) For each of the entities involved, determine which of the impact metrics in Annex I are relevant to the entity. The impact metrics relevant to the entity will be a subset of the impact metrics that are relevant to the associated processes. These metrics are considered relevant if their value is above the threshold in Annex II of the present methodology, and if the type of entity involved influences the metric.

(3) Derive for each metric in point (2) an ECII that provides a good estimate of the metric, and that the entity itself can calculate based on the information and knowledge available to them.

(4) Convert the high-impact and critical-impact thresholds for the metrics identified in point (2) into thresholds for the ECII in point (3). In the conversion, a cyber-attack affecting multiple entities shall be considered, so that the threshold for the ECII may be lower than for the impact metric.

Article 8

Union-wide cybersecurity risk assessment report

The Union-wide risk assessment report, created pursuant Article 19 of the NCCS regulation, shall include a list of Union-wide high-impact and critical-impact processes identified according to Article 6 of the present Methodology. For each of these processes, the report shall include:

(1) an assessment of the possible consequences of a cyber-attack compromising the confidentiality, integrity, or availability of information used in the process, as assessed pursuant to Article 5 (1) of the present methodology;

(2) a list of the types of entities involved in the process, determined pursuant to Article 7(1) of the present methodology; and

(3) ECII and high-impact and critical-impact thresholds developed pursuant to Article 7(4) of the present methodology that the competent authorities shall use to identify high-impact and critical-impact entities involved in the Union-wide high-impact and critical-impact processes.

(4) The risk impact matrix pursuant to Article 19 (2)(b) of the NCCS.

TITLE 3

Regional cybersecurity risk assessment and mitigation

Article 9

Objective of the regional cybersecurity risk assessment

(1) The objective 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.

(2) During the regional cybersecurity risk assessment, ENTSO-E in cooperation with the EU DSO entity shall for each of the high-impact and critical-impact processes identified in the Union-wide risk assessment:

(a) aggregate the results from the Member State cybersecurity risk assessments to determine the consequences and likelihood of a compromise of the confidentiality, integrity or availability of the information used, pursuant to Article 10 of the present methodology;

(b) evaluate the risks analysed in point (a) pursuant to Article 11 of the present methodology;

(c) determine the cybersecurity threats that lead to high and critical risks pursuant to Article 12 of the present methodology.

Article 10

Aggregating the Member State risk assessment results

(1) ENTSO-E in cooperation with the EU DSO entity shall aggregate the results from the member state cybersecurity risk assessments. The Member State risk assessment results are reported as the risk of a compromise of the confidentiality, integrity, or availability of each Union-wide high-impact or critical-impact process using the template in Annex V. The risks are reported on the risk impact matrix that will be defined in the Union-wide risk assessment report.

(2) ENTSO-E in cooperation with the EU DSO entity may use quantitative analysis or the judgement of their experts to aggregate the Member State cybersecurity risk assessment results. The aggregation method shall be described in the comprehensive Cross-border cybersecurity risk assessment report. The method shall:

(a) Assess the total risk that a Union-wide process is compromised through any entity in the system operations region.

(b) Consider the cyber-attacks that affect multiple entities in the system operations region.

(c) Assess the risks with the cybersecurity controls that the entities had implemented at the moment they performed the entity-level risk assessment.

(3) When reporting the risk of a compromise of availability, ENTSO-E in cooperation with the EU DSO entity shall report the outage duration that corresponds to the reported risk.

(4) ENTSO-E in cooperation with the EU DSO entity may request additional information from the competent authority for further clarification regarding the results of the Member State cybersecurity risk assessments.

(5) If Member State cybersecurity risk assessment report is not available or not complete, ENTSO-E in cooperation with the EU DSO entity shall not consider the cybersecurity risks for that Member State. In that case, they shall state in the cross-border electricity cybersecurity risk assessment report that risk

information from the Member State is missing.

(6) ENTSO-E in cooperation with the EU DSO entity shall not validate the information received from Member States. In their analysis, ENTSO-E in cooperation with the EU DSO entity shall assume that the information received is correct and up to date.

(7) ENTSO-E in cooperation with the EU DSO entity shall, at the request of ACER in accordance with Article 12 of NCCS Regulation, support ACER for the monitoring of the implementation of the NCCS Regulation, with the following information aggregated per system operations region:

(a) the implementation status of the cybersecurity measures as gathered pursuant Article 15(2) and 15(3);

(b) the current and residual risks per Union-wide high-impact and critical-impact process reported using the risk-impact matrix;

(c) statistics on the cybersecurity cyber-attacks and cyber threats gathered pursuant to Article 17(1).

Article 11
Evaluating the risks

ENTSO-E in cooperation with the EU DSO entity shall evaluate the cybersecurity risks analysed pursuant to Article 10 of the present methodology using the risk impact matrix that will be defined in the Union-wide risk assessment report.

Article 12
Determining cyber threats

ENTSO-E in cooperation with the EU DSO entity shall determine the cyber threats in accordance with Annex III which may lead to the high and critical risks identified in Article 11 of the present methodology. They shall take into account the information on cyber threats provided in the Member State cybersecurity risk assessment reports.

Article 13
Cross-border cybersecurity risk assessment report

ENTSO-E in cooperation with the EU DSO entity shall report the results of the regional cybersecurity risk assessment in the Comprehensive Cross-border electricity cybersecurity risk assessment report pursuant Article 23 of the NCCS Regulation.

TITLE 4
Member state cybersecurity risk assessment

Article 14
Objective of the member state cybersecurity risk assessment

(1) The objective of the member state risk assessment level is to identify and analyse the risks of cyber-attacks affecting the operational security of the electricity system disrupting cross-border electricity

flows. All high-impact and critical-impact entities in the Member State are in the scope of the assessment.

(2) During the member state cybersecurity risk assessment, the competent authority shall:

(a) determine the implementation status of the minimum and advanced cybersecurity controls defined pursuant to Article 15 of the present methodology;

(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 cyber threats gathered pursuant Article 38(3) and (6) of the NCCS Regulation; and

(d) recommend additional cybersecurity controls to mitigate high and critical risks to ENTSO-E in cooperation with the EU DSO entity.

(3) The competent authority may use the outcomes of the risk assessment to mitigate cybersecurity risks at Member State level. The NCCS Regulation does not include requirements for such risk mitigation. Risks are only treated at the level of system operations regions after the regional cybersecurity risk assessment.

Article 15
Determining the implementation status of the cybersecurity measures

(1) The competent authority shall determine the status of the implementation of the minimum and advanced cybersecurity controls for the Member State. For this purpose, it may use verification evidence presented by entities pursuant to Article 31 of the NCCS Regulation or request additional information from the high-impact and critical-impact entities.

(2) The competent authority shall report the implementation status for each minimum and advanced cybersecurity control, by reporting for each control:

(a) the percentage of entities that have implemented the control;
(b) the percentage of entities that have derogations for the control.

(3) The competent authority shall also report the percentage of entities that have implemented the following NCCS measures:

(a) the entity-level risk assessments pursuant to Article 26(4) of the NCCS Regulation;

(b) the entity-level risk treatment plan pursuant to Article 26(5) of the NCCS Regulation;

(c) the cybersecurity management system pursuant to Article 32 of the NCCS Regulation;

(d) the CSOC capabilities pursuant to Article 38(1)(a) of the NCCS Regulation;

(e) the capabilities to handle detected cyber-attacks pursuant to Article 39(1) of the NCCS Regulation;

(f) the entity-level crisis management plan pursuant to Article 41 of the NCCS Regulation;

(g) the entity- or Member-State level cybersecurity exercises pursuant to Article 43 of the NCCS Regulation; and

(h) the participation in regional cybersecurity exercises pursuant to Article 44 of the NCCS Regulation.

(4) The competent authority shall separately report the implementation status of the minimum and advanced cybersecurity controls in paragraph 2 of this article and of the security measures in paragraph 3 of this article for the high-impact and the critical-impact entities in the Member State. The competent authorities may use the templates in Annex V(B) to report the implementation status.

Article 16
Aggregating the entity results

(1) The competent authority shall aggregate the results from the cybersecurity risk assessments at entity level. The entity risk assessment results are reported as the risk of a compromise of the confidentiality, integrity, or availability through a cyber-attack of each Union-wide high-impact or critical-impact processes in which the entity is involved. The risks are reported on the risk impact matrix that will be defined in Union-wide risk assessment report.

(2) The competent authority may use quantitative analysis or the judgement of their experts to aggregate the Member State cybersecurity risk assessment results. The aggregation method shall be described in the Member State cybersecurity risk assessment report. The method shall:

(a) Assess the total risk that a Union-wide process is compromised through any entity in the member state.

(b) Consider the cyber-attacks that affect multiple entities in the member state.

(c) Assess the risks with the cybersecurity controls that the entities had implemented at the moment they performed the entity-level risk assessment.

(3) When reporting the risk of a compromise of availability, the competent authority shall report the outage duration that corresponds to the reported risk.

(4) The competent authority shall request for each risks assessed high or critical pursuant to Article 27(2) of the NCCS the following additional information from the high-impact and critical-impact entities:

(a) a list of cyber threats from Annex III that contribute significantly to the risk;

(b) a list of recommended controls selected from European and international standard to mitigate the risk to below high; and

(c) the estimated residual risk after applying the controls in point (b) according to the risk impact matrix.

(5) The competent authority may use the template in Annex IV to collect the results of the risk assessment at entity level from the high- and critical-impact entities.

(6) When entities report the risk of a compromise of availability, the competent authority shall require them to report the outage duration that corresponds to the reported risk.

(7) The competent authority shall analyse the lists of critical ICT service providers received from entities pursuant to Article 27(3) of the NCCS Regulation to assess the cybersecurity risks coming from the

dependency on a single supplier of ICT products, ICT services or ICT processes. They shall analyse the risk both for individual entities and for the whole Member State. If dependency on a single supplier is assessed as a high or critical risk for a Union-wide high-impact or critical-impact process, the competent authority shall report this risk in the Member State cybersecurity risk assessment report.

Article 17
Summarizing the information on cyber-attacks and cyber threats

(1) The competent authority shall provide the following statistics on the cybersecurity cyber-attacks and cyber threats over the last three years to ENTSO-E and EU DSO entity:

(a) Number of cyber-attacks reported pursuant to Article 38(3) of the NCCS Regulation, categorized according to the NCCS cyber-attack classification scale methodology and the cyber threat types defined in Annex III; and

(b) Number of cyber threats reported pursuant to Article 38(6) of the NCCS Regulation, categorized according to the cyber threat types defined in Annex III.

(2) For each of the risks analysed in Article 16 of the present methodology that are classified as high or critical according to the risk impact matrix that will be defined in Union-wide risk assessment report, the competent authority shall provide an analysis of which cyber threats contribute significantly to these risks. The competent authority shall in the analysis at least consider the cyber threats in Annex III. The competent authority may consider additional cyber threats.

Article 18
Recommending cybersecurity controls

1. For each of the risks analysed in Article 16 of the present methodology that are classified as high or critical according to the risk impact matrix that will be defined in Union-wide risk assessment report, the competent authority shall recommend in the Member State cybersecurity risk assessment report cybersecurity controls that would mitigate the risk to below high.
2. The competent authority shall base the recommendation referred in paragraph 1 on the status of the implementation of the cybersecurity controls, the information on cyber-attacks and cyber threats, the risks reported by the entities from the cybersecurity risk assessments at entity level, and on any other information they have from their supervision activities.
3. Whenever possible, the competent authority shall recommend cybersecurity controls from European and international standards that are commonly used in the electricity sector.
4. The competent authority shall report the expected residual likelihood, impact, and risks to the member state if the recommended controls in point (1) have been implemented. The risks are reported on the risk impact matrix that will be defined in Union-wide risk assessment report.

Article 19
Member state cybersecurity risk assessment report

The competent authority shall report the results of the Member State cybersecurity risk assessment to ENTSO-E and the EU DSO entity in the Member State cybersecurity risk assessment report pursuant to Article 20(2) of the NCCS Regulation. The competent authority may report the risks according to the template provided in Annex V(A).

TITLE 5
Final provisions

Article 20
Implementation timeline

(1) This methodology shall be implemented according to the timelines given in the NCCS regulation.

(2) The implementation of this methodology includes the following deliverables:

a. the Union-wide cybersecurity risk assessment report pursuant Article 19 of the NCCS Regulation;

b. the Comprehensive cross-border cybersecurity risk assessment report pursuant Article 23 of the NCCS Regulation;

c. the regional cybersecurity risk mitigation plans pursuant Article 22 of the NCCS Regulation; and

d. the Member State cybersecurity risk assessment reports pursuant Article 20 of the NCCS Regulation.

Article 21
Language

The reference language for this cybersecurity risk assessment methodology Proposal shall be English. For the avoidance of doubt, where TSOs and DSOs need to translate this cybersecurity risk assessment methodology Proposal into their national language(s), in the event of inconsistencies between the English version published by TSOs and DSOs in accordance with Article 5(10) of the NCCS Regulation and any version in another language, the relevant TSOs shall, in accordance with national legislation, provide the relevant national competent authorities for the NCCS Regulation with an updated translation of the cybersecurity risk assessment methodology Proposal.

Annex I: Impact metrics

The following impact metrics are used to measure the consequences of a compromise of confidentiality, integrity or availability of information:

Impact metric	Description
Loss of load	The reduction caused by the cyber-attack in the total load of the affected TSOs. The total load means a load equal to generation and any imports deducting any exports and power used for energy storage as defined in Article 2(27) of Regulation (EU) 543/2013.
Reduction of power generation	The reduction in the total aggregated generation output of the TSOs involved in the process caused by the cyber-attack. The aggregated generation output per market time unit and per production type is defined according for Article 16(1)(b) of Regulation (EU) 543/2013. For the impact metric, the aggregated output over all production types is considered.
Frequency degradation	Deviation from the standard frequency in combination with the duration of the deviation.
Violation of standards on voltage	Operations of a node of the transmission system in steady state outside of the voltage ranges defined in Article 27 of SO GL within time range (which are different for each synchronous area) specified in Article 16 of Regulation (EU) 2016/631 (RfG).
Reduction of capacity in the primary frequency reserve	A reduction in the reserve capacity for the Frequency Containment Reserves (FCR), as defined in the System Operations Guideline (Regulation (EU) 2017/1485). The reduction of reserve capacity is calculated using the minimum reporting time which is determined by each TSO's scheduling resolutions of power generating facilities. These resolutions may vary between 5 and 30 minutes across different TSOs and the reduction in reserve capacity is related to the pre-fault levels.
Reduction of capacity in the other frequency reserves	A reduction in the reserve capacity for the Frequency Restoration Reserves (FRR), both automatic and manual, and the replacement reserves (RR), as defined in the System Operations Guideline (Regulation (EU) 2017/1485). The reduction of reserve capacity is calculated using the minimum reporting time which is determined by each TSO's scheduling resolutions of power generating facilities. These resolutions may vary between 5 and 30 minutes across different TSOs and the reduction in reserve capacity is related to the pre-fault levels.
Loss of capacity for a black start	The loss of availability any tools, means and facilities as defined in Article 24 of Regulation (EU) 2017/1485 that are needed for a black start. This includes the tools, means and facilities needed to communicate with and operate the power sources in the TSO's control area necessary to re-

	energise its system with bottom-up re-energisation strategy having black start capability, and the substations which are essential for its restoration plan procedures as identified under Article 23(4) of Regulation (EU) 2017/2196. TSOs have redundant power sources in their control area to perform a black start. The capacity for a black start is only to be lost if not enough power sources can be operated to perform a black start.
The expected duration of outage affecting customers in combination with the scale of the outage in customer numbers	The sum of all customer interruption durations for the interruptions caused by the cyber-attack.

Annex II: High-impact and critical-impact thresholds

The tables below give the thresholds for determining when the impact of a cybersecurity risk should be considered high-impact or critical-impact for the Union-wide cybersecurity risk assessment, the cybersecurity regional risk assessment, and the member state cybersecurity risk assessment.

Note that different thresholds may be used for the ECII, pursuant to Article 7; ECII thresholds are determined during the Union-wide risk assessment.

Union-wide cybersecurity risk assessment

The table below gives the thresholds for determining when the impact of a cybersecurity risk should be considered high-impact or critical-impact for the Union-wide cybersecurity risk assessment.

Table 1: High-impact and critical-impact thresholds for the Unionwide cybersecurity risk assessment.

Impact metric	High-impact threshold	Critical-impact threshold
Loss of load	250 MW	3,000 MW
Reduction of power generation	250 MW	3,000 MW
Frequency degradation	>50 mHz for > 15 min OR >100 mHz for >5 min.	>200 mHz for >30 sec
Violation of standards on voltage	<0,85 pu, for >30 seconds OR <= 0,90 pu for >60 min. OR	Same as high-impact but with consequences on at least one neighbouring TSO

	>1,05 pu for >60 min. OR >1,10 pu, for >30 seconds	
	No consequences on neighbouring TSO	
Reduction of capacity in the primary frequency reserve	More than 20 % reduction, with a duration of more than 30 minutes	Reserve capacity unavailable more than 30 minutes
Reduction of capacity in the other frequency reserves	More than 20 % reduction, with a duration of more than 30 minutes	Reserve capacity unavailable more than 30 minutes
Loss of capacity for a black start	Loss of any tools, means and facilities needed for a black start with consequences for neighbouring TSOs for more than 30 minutes OR The unplanned evacuation to the back up control room	Loss of all tools, means and facilities needed for a black start within a TSOs control area, for more than 30 minutes
The expected duration of outage affecting customers in combination with the scale of the outage in customer numbers	50,000,000 customer outage minutes	100,000,000 customer outage minutes

Regional cybersecurity risk assessment

The table below gives the thresholds for determining when the impact of a cybersecurity risk should be considered high-impact or critical-impact for regional cybersecurity risk assessment.

Table 2: Thresholds for the loss of load and reduction of power generation impact metrics for the regional cybersecurity risk assessment.

	Central Europe	SEE	SWE	Nordic	Baltic
High-impact threshold	250 MW	250 MW	250 MW	500 MW	500 MW
Critical-impact threshold	3,000 MW	3,000 MW	3,000 MW	3,000 MW	900 MW

Table 3: Thresholds for frequency degradation impact metric for different system operation regions.

	Central Europe SEE SWE	Nordic	Baltic
High-impact threshold	>50 mHz for > 15 min OR >100 mHz for >5 min.	>100 mHz for > 15 min OR >250 mHz for >5 min.	>50 mHz for > 15 min OR >200 mHz for >10 min.
Critical-impact threshold	>200 mHz for >30 sec	>500 mHz for >1 min OR >1 Hz	>400 mHz for >1 min

Table 4: Thresholds for the voltage impact metric at the connection point between >110 kV and ≤300 kV for different system operation regions. (Here pu stand for per-unit.)

	Central Europe SEE SWE	Nordic	Baltic
High-impact threshold	<0,85 pu, for >30 seconds OR <= 0,90 pu for >60 min. OR >1,118 pu for >60 min. OR >1,15 pu, for >30 seconds	<0,90 pu, for >30 seconds OR >1,05 pu for >60 min. OR >1,10 pu, for >30 seconds	<0,85 pu, for >30 seconds OR <= 90 pu for >30 min. OR >1,118 pu for >20 min. OR >1,15 pu, for >30 seconds
		No consequences on neighbouring TSO	
Critical-impact threshold		Same as high-impact but with consequences on at least one neighbouring TSO.	

Table 5: Thresholds for the voltage impact metric at the connection point above 300 kV for different synchronous areas.

	Central Europe SEE SWE	Nordic	Baltic
High-impact threshold	<0,85 pu, for >30 seconds OR <= 0,90 pu for >60 min. OR >1,05 pu for >60 min. OR >1,10 pu, for >30 seconds	<0,90 pu, for >30 seconds OR >1,05 pu for >60 min. OR >1,10 pu, for >30 seconds	<0,88 pu, for >30 seconds OR <= 90 pu for >30 min. OR >1,097 pu for >20 min. OR >1,15 pu, for >30 seconds
		No consequences on neighbouring TSO	
Critical-impact threshold		Same as high-impact but with consequences on at least one neighbouring TSO.	

Table 6: Thresholds for the reduction of capacity in the primary frequency reserve impact metric for different system operation regions.

	Central Europe SEE SWE	Nordic	Baltic
High-impact threshold	More than 20 % reduction, with a duration of more than 30 minutes		
Critical-impact threshold	Reserve capacity unavailable more than 30 minutes		

Table 7: Thresholds for the reduction of capacity in the other frequency reserves impact metric for different system operation regions.

	Central Europe SEE SWE	Nordic	Baltic
High-impact threshold	More than 20 % reduction, with a duration of more than 30 minutes		

Critical-impact threshold	Reserve capacity unavailable more than 30 minutes

Table 8: Thresholds for the loss of capacity for a black start impact metric for different system operation regions.

	Central Europe SEE SWE	Nordic	Baltic
High-impact threshold	Loss of any tools, means and facilities needed for a black start with consequences for neighbouring TSOs for more than 30 minutes OR The unplanned evacuation to the back up control room		
Critical-impact threshold	Loss of all tools, means and facilities needed for a black start for more than 30 minutes.		

Table 9: Thresholds for the expected duration of outage affecting customers in combination with the scale of the outage in customer numbers impact metric for different synchronous areas.

	Central Europe SEE SWE	Nordic	Baltic
High-impact threshold	50,000,000 customer outage minutes		
Critical-impact threshold	100,000,000 customer outage minutes		

Member state cybersecurity risk assessment

The thresholds for the member state cybersecurity risk assessment are the same as for the regional cybersecurity risk assessment. Member states use the thresholds of their system operation region. The only exception is for the loss of load and reduction of power generation impact metrics. For those metrics, member states use the thresholds in Table 10.

Table 10: Thresholds for the loss of load and reduction of power generation impact metrics for the member state cybersecurity risk assessment.

Member state	High-impact threshold	Critical-impact threshold
Austria	500 MW	3,000 MW
Belgium	1,500 MW	3,000 MW
Bulgaria	250 MW	3,000 MW
Croatia	250 MW	3,000 MW
Cyprus	250 MW	800 MW

Czech Republic	500 MW	3,000 MW
Denmark	1,000 MW	3,000 MW
Estonia	500 MW	900 MW
Finland	500 MW	3,000 MW
France	1,500 MW	3,000 MW
Germany	1,500 MW	3,000 MW
Greece	500 MW	3,000 MW
Hungary	500 MW	3,000 MW
Ireland	500 MW	800 MW
Italy	1,500 MW	3,000 MW
Latvia	500 MW	900 MW
Lithuania	500 MW	900 MW
Luxembourg	1,500 MW	3,000 MW
Malta	250 MW	500 MW
Netherlands	1,500 MW	3,000 MW
Poland	1,000 MW	3,000 MW
Portugal	250 MW	3,000 MW
Romania	1,000 MW	3,000 MW
Slovakia	500 MW	3,000 MW
Slovenia	1,000 MW	3,000 MW
Spain	1,000 MW	3,000 MW
Sweden	1,500 MW	3,000 MW

Annex III: List of cyber threats

The table below gives a list of cyber threats that shall be considered during the regional cybersecurity risk assessment.

Cyber threat	**Description**
Severe and unexpected corruption of the supply chain	The supply chain of a high-impact and critical-impact entity is severely and unexpectedly corrupted through a cyber-attack.

The unavailability of ICT products, ICT services, or ICT processes from the supply chain	Because of a cyber-attack, products, services, or processes in the supply chain are not available. This includes for instance network services not being available.
Cyber-attacks initiated through actors in the supply chain	Cyber-attacks are initiated through actors in the supply chain of a high-impact or critical-impact entity. This includes the abuse of remote access rights of service providers, malware infections of laptops used by contractors, and failures in separating resources (memory, storage, routing) between different tenants of shared (cloud) infrastructure.
Leaking of sensitive information through the supply chain, including supply chain tracking	The confidentiality of high-impact or critical-impact information assets is compromised through service providers or other actors in the supply chain that have access to the assets.
The introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain	Weaknesses or backdoors are deliberately inserted into ICT products, ICT services, or ICT processes used in the high-impact or critical-impact perimeters through actors in the supply chain. This includes the inclusion of software backdoors by developers, in third party software, or in open-source software, and the inclusion of hardware backdoors during design and production.
Attacks through communication networks	The confidentiality, integrity or availability of high-impact or critical-impact assets are compromised when they are sent over a communication network. This includes eavesdropping, manipulation of data in transit, man-in-the-middle attacks, DDoS attacks, or failure in telecommunication equipment due to cyber-attacks. When analysing this threat, entities should in particular analyse the risks of disrupting communication for systems with real-time requirements.
Attacks through removable media	The confidentiality, integrity or availability of high-impact or critical-impact assets are compromised when they are stored on removable media. This includes theft of media, and retrieval of recycled or discarded media. When analysing this cyber threat, entities should in particular analyse the cyber threat of removable media to legacy system.
Unauthorized system access	Threat actors gain unauthorized access to network and information systems within the high-impact or critical-impact perimeter. This includes unauthorized remote access with compromised credentials or by exploiting software vulnerabilities. When analysing this cyber threat, entities should in particular analyse the risks of unauthorized access to legacy systems.
Malware intrusion	Malware is introduced into the high-impact or critical-impact perimeter. This includes worms, viruses, remote

	access toolkits, wipers, and ransomware. Both targeted and untargeted malware should be considered. When analysing this cyber threat, entities should in particular analyse the cyber threat of malware being introduced into legacy systems.
Social engineering	Social engineering attacks are performed on staff or contractors involved in the high-impact and critical-impact processes to compromise the information used in them. This includes phishing and spear-phishing.
Physical attacks	Attackers physically attack assets in the high-impact or critical-impact perimeter to compromise the confidentiality, integrity or availability of the high-impact or critical-impact information assets. This includes breaking in on locations with high-impact or critical-impact information assets, or physically tampering or destroying hardware components that process high-impact or critical-impact information assets.
Insider threats	Employees at the high-impact or critical-impact entities intentionally compromise the confidentiality, integrity or availability of the high-impact or critical-impact assets.

Annex IV: Entity reporting template

The table below provides a template for high- and critical-impact entities to report the results of cybersecurity risk assessment at entity level according to Article 27 of the NCCS. Not all information in the template is required by the NCCS. Competent authorities may have to request additional information according to Article 16 of this methodology.

Process Art 27 NCCS	**Property compromised** Art 27 NCCS	**Current risk** Art 27 NCCS				**Cyber threats causing risk** Art 16(4)	**Recommended controls to mitigate the risk** Art 16(4)	**Residual risk after recommended controls** Art 16(4)		
		Likeli-hood	**Impact**	**Risk**	**Duration analysed** Art 16(3)			**Likeli-hood**	**Impact**	**Risk**
<Process 1>	Confidentiality									
	Integrity									
	Availability									
<Process 2>	Confidentiality									
	Integrity									
	Availability									

Remarks:

- Risks must be reported for all processes on the list of Union-wide high- and critical-impact processes (see NCCS Article 27).
- The current and residual risks are reported on the risk-impact matrix that will be provided in the Union-wide risk assessment report (see NCCS Article 27 and Article 16(4)).
- The cyber threats are selected from Annex III (see Article 16(4)). All relevant threats should be listed. When a threat affects several processes, it should be listed at each process.
- The controls should be selected from European and international standards (see Article 16(4)).

- Besides the information in the template, competent authorities should separately report a list of critical ICT service providers for their critical-impact processes according to Article 27(3) of the NCCS.

Annex V: Member state reporting template

A. Reporting template for member state cyber security risk assessment

The table below provides a template for competent authorities to report the results of the member state cybersecurity risk assessment according to Article 22.

Process Art 16(1)	**Property compromised** Art 16(1)	**Current risk** Art 16(1)				**Cyber threats causing risk** Art 17(2)	**Recommended controls to mitigate the risk** Art 18(1)	**Residual risk after recommended controls** Art 18(4)		
		Likeli-hood	**Impact**	**Risk**	**Duration analysed** Art 16(3)			**Likeli-hood**	**Impact**	**Risk**
<Process 1>	Confidentiality									
	Integrity									
	Availability									
<Process 2>	Confidentiality									
	Integrity									
	Availability									

Remarks:

- Risks must be reported for all processes on the list of Union-wide high- and critical-impact processes (see Article 16(1)).
- The current and residual risks are reported on the risk-impact matrix that will be provided in the Union-wide risk assessment report (Article 16(1) and 18(4)).
- The cyber threats are selected from Annex III (Article 17(2)). All relevant threats should be listed. When a threat affects several processes, it should be listed at each process.

- The controls should be selected from European and international standards (Article 18(3)).
- Use of the reporting template by competent authorities is voluntary. They may report the risk assessment results also in another format.

B. Reporting template for the implementation of controls

The table below provides a template for competent authorities to separately report the percentage of entities that have implemented the NCCS minimum and advanced cybersecurity controls according to article 15(2) and the NCCS measures according to Article 15(3).

Note that according to Article 20(4), competent authorities should not report the implementation status of controls if the information can be linked to specific entities or assets.

NCCS Minimum cybersecurity controls	**Percentage of entities that have implemented the control**	**Percentage of entities with derogations for the control**
<Control 1>		
…		
…		
<Control n>		

NCCS Advanced cybersecurity controls	**Percentage of entities that have implemented the control**	**Percentage of entities with derogations for the control**
<Control 1>		
…		
…		
<Control n>		

NCCS Measure	Percentage of entities that have implemented the control	Percentage of entities with derogations for the control
Entity-level risk assessment *Art 26(4)*		
Entity-level risk treatment plan *Art 26(5)*		
Cybersecurity management system *Art 32*		
CSOC capabilities *Art 38(1)*		
Capabilities to handle detected cyber-attacks *Art 39(a)*		
Entity-level crisis management plan *Art 41(6)*		
Participation in Entity/Member State level cybersecurity exercises *Art 43*		
Participation in (cross)regional cybersecurity exercises *Art 44*		

Remarks:

- Implementation status of minimum and advanced cybersecurity controls and implementation status of NCCS measures must be reported for separately.
- Use of the reporting template by competent authorities is voluntary. They may report the risk assessment results also in another format.