ACER

European Union Agency for the Cooperation of Energy Regulators

Operational reliability performance indicators – submission guidance

Pursuant to the network code for cybersecurity aspects of cross-border electricity flows

27 January 2026

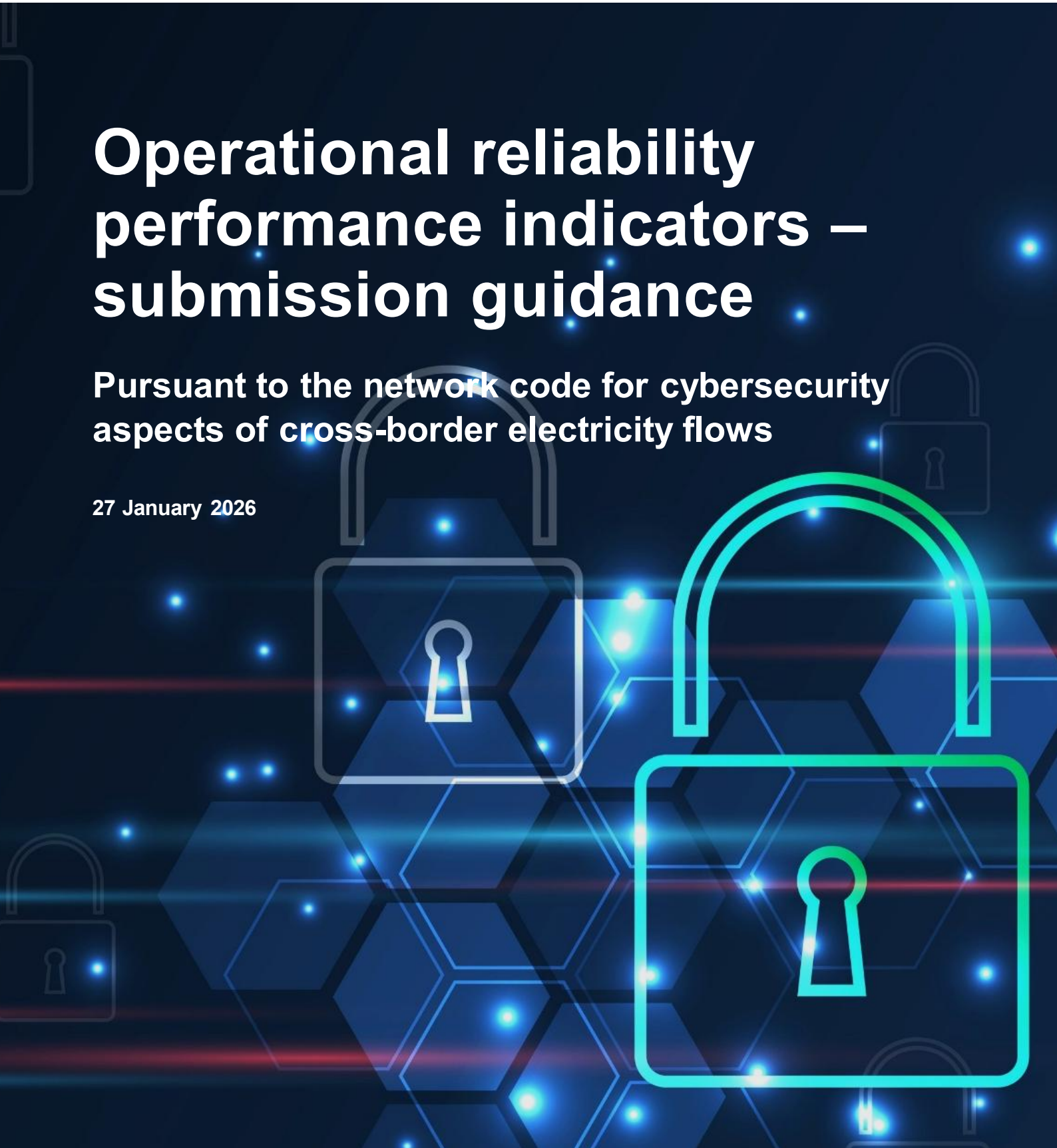

Table of contents

1. Legal basis and structure of this document

Pursuant to Article 12(5) of the Commission Delegated Regulation (EU) 2024/1366 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows[1] (the '**NCCS**'), ACER[2], in cooperation with ENISA[3] and with the support of the ENTSO-E[4] and the EU DSO entity[5], shall issue non-binding performance indicators for the assessment of operational reliability that are related to cybersecurity aspects of cross-border electricity flows ('**performance indicators**').

Furthermore, pursuant to Article 12(3) of the NCCS, ACER, in cooperation with ENISA and after consultation of the ENTSO for Electricity and the EU DSO entity, may issue guidance on the relevant information to be communicated to ACER for the monitoring purposes as well as the process and frequency for the collection, based on the performance indicators defined in accordance Article 12(5) of the NCCS ('**submission guidance**').

In Section 2 of this document ACER issues three performance indicators, whereas in Section 4 ACER describes the criteria based on which these performance indicators have been selected.

Section 3 of this document contains submission guidance for the three performance indicators.

ACER encourages all high-impact and critical impact entities identified by the competent authorities[6] in accordance with Article 24 of the NCCS to assist ACER by sharing the information in accordance with the submission guidance provided in Section 3 of this document.

Until the high-impact and critical impact entities are identified, ACER encourages all candidates for high-impact and critical-impact entities identified in accordance with Article 48(3) of the NCCS[7] to share the information in accordance with Section 3 of this document.

ACER will be grateful for the entities' assistance with monitoring the performance indicators, contributing to the assessment of operational reliability related to cybersecurity of cross-border electricity flows.

[1] OJ L, 2024/1366, 24.5.2024.

[2] European Union Agency for the Cooperation of Energy Regulators operating under Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulators (OJ L 158, 14.6.2019, p. 22–53).

[3] European Union Agency for Cybersecurity operating under Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (OJ L 151, 7.6.2019, p. 15–69).

[4] Established pursuant to Article 28 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54.). Hereinafter referred to as '**Regulation 2019/943**'.

[5] Established pursuant to Article 52 of Regulation 2019/943.

[6] Responsible for carrying out the tasks assigned to them under the NCCS and designated by Member States pursuant to Article 4 of the NCCS.

[7] In this document, the high-impact and critical impact entities identified by the competent authorities in accordance with Article 24 of the NCCS and the candidates for high-impact and critical-impact entities identified in accordance with Article 48(3) of the NCCS will be collectively referred to as '**entities**'. However, all references to obligations of the high-impact and critical impact entities stemming from the relevant provisions of the NCCS shall instead be understood as recommendations for the candidates for high-impact and critical-impact entities.

2. Three performance indicators

Based on the criteria described in Section 4 of this document, ACER issues the following three performance indicators:

Table 1: Three performance indicators

Operational reliability performance indicator	NCCS Article	Categorised into
Annual number of reportable cyber-attacks	38(3)	High-impact entities and critical-impact entities High-gravity (level 4) and critical-gravity (level 5) cyber-attacks[8]
Annual number of exploited unpatched ('zero day') vulnerabilities	38(5)	High-impact entities and critical-impact entities
Annual number of reportable cyber threats	38(6)	Threat types listed in the Cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level, pursuant to Article 18(2)(a) of the NCCS

3. Submission guidance

3.1. Submission once every three years

Starting in year 2027, ACER will open a submission window once every three years for all entities to submit the information described in Section 3.2.

In the initial submission taking place in year 2027, to the extent possible, ACER requests the entities to provide information for year 2026. Subsequent submissions, **from year 2030 onwards, will cover the three preceding years**.

Unless ACER communicates otherwise, each year, the aforementioned **submission window will remain open from 15 January until 1 March**.

3.2. Information to be submitted

Table 2: General information

General information type	Sample information
Submitting person	Martin Dubois
Email address of submitting person	Martin.Dubois@nousdistribuons.fr

[8] In accordance with the Cyber-attack classification scale methodology referred to in Article 37(8) of the NCCS. Please refer to Section 4.1.2. of this document.

Entity	NousDistribuons
Member State	France
Type of entity	Distribution system operator
At submission date, designated as	High-impact entity
Years covered	2027-2029
Date of submission	30 January 2030

At submission date, designated as: the data collection tool will include four options. Namely, candidate for a high-impact entity, candidate for a critical-impact entity, high-impact entity and critical-impact entity.

Table 3: Information based on performance indicators with sample count

Operational reliability performance indicator	Further categorisation	Count		
		2027	2028	2029
Annual number of reportable cyber-attacks	High gravity	2	1	0
	Critical gravity	0	0	0
Annual number of exploited unpatched ('zero day') vulnerabilities	N/A	3	1	0
Annual number of reportable cyber threats	Severe and unexpected corruption of the supply chain	0	0	0
	Unavailability of ICT products, ICT services, or ICT processes from the supply chain	1	0	0
	Cyber-attacks initiated through actors in the supply chain	0	0	0
	Leaking of sensitive information through the supply chain, including supply chain tracking	0	1	0
	Introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain	0	0	1
	Attacks through communication networks	3	1	2
	Attacks through removable media	0	0	0
	Unauthorized system access	0	1	0

	Malware intrusion	2	0	2
	Social engineering	0	0	0
	Physical attack	0	0	0
	Insider threats	0	0	0

3.3. Process for submission

ACER will provide the entities registration and access to a secure online tool through which the entities will be requested to provide the information described in Section 3.2.

Prior to the first data submission window (see Section 3.1), ACER will update this process guidance with more detailed instructions to assist the entities with providing the information described in Section 3.2.

4. Criteria for selecting the performance indicators

In issuing the performance indicators listed in Section 2, ACER specifically considered the following five criteria:

4.1. Link with electricity impact metrics

Since the performance indicators are to serve the assessment of operational reliability of cross-border electricity flows, they should be:

- linked to the processes and supporting assets that affect the cross-border electricity flows; and
- aligned with the metrics developed under the NCCS to gauge potential impact on these assets and processes.

4.1.1. Link with the processes and supporting assets that affect cross-border electricity flows

Pursuant to Article 19(2)(a) of the NCCS, a Union-wide cybersecurity risk assessment report drawn up by the ENTSO-E, in cooperation with the EU DSO entity, shall include Union-wide high-impact and critical-impact processes[9]. These processes will be identified following a Union-wide risk assessment carried out pursuant to Article 19(1) of the NCCS evaluating possible consequences of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows.

[9] A non-binding provisional list of Union-wide high-impact and critical-impact processes the ENTSO-E and the EU DSO entity developed in accordance with Article 48(4) of the NCCS can be found on the ENTSO-E website: https://www.entsoe.eu/network_codes/nccs/. In developing this provisional list, the TSOs and DSOs estimated the impact on cross-border electricity flows should a process be compromised by taking into account how much electrical load or generation the process controls.

Pursuant to Article 19(3)(b) of the NCCS, with respect to the Union-wide high-impact and critical-impact processes, the Union-wide cybersecurity risk assessment report shall also include a classification scale that ranks possible consequences of cyber-attacks to business processes involved in cross-border electricity flows, referred to as the 'electricity cybersecurity impact index' (the '**ECII**'). In addition, the Union-wide cybersecurity risk assessment report shall include high-impact and critical-impact thresholds[10].

Pursuant to Article 26(4)(c) of the NCCS, each entity shall, in the context of entity level risk management, classify assets according to the possible consequences when cybersecurity is compromised and determine the high-impact and critical-impact perimeter. This asset classification shall use the ECII and include the following three steps:

- classification of processes as high-impact or critical-impact if their ECII is above the high-impact or critical-impact threshold;
- determination of high-impact and critical-impact assets supporting these high-impact and critical-impact processes; and
- definition of the high-impact and critical-impact perimeters containing the high-impact and critical-impact assets.

4.1.2. Alignment with metrics gauging potential impact on these assets and processes

Pursuant to Article 37(8) of the NCCS, transmission system operators ('**TSOs**') shall develop a cyber-attack classification scale methodology to classify the gravity of cyber-attacks according to five levels, the two highest levels being 'high' and 'critical'.

Pursuant to Article 38(3) and (4) of the NCCS, the entities shall report cyber-attacks to their computer security incident response teams ('**CSIRTs**')[11] and their competent authorities when they assess the cyber-attack affecting them as either 'high' or 'critical' gravity.

Pursuant to Article 37(8)(a) of the NCCS, one of the two parameters on which the cyber-attack classification scale methodology shall be based is the potential impact **considering the assets and perimeters exposed**, determined in accordance with Article 26(4)(c) of the NCCS and described in Section 4.1.1.

What follows from the above is that the entities will be required to report cyber-attacks affecting them to their CSIRTs and their competent authorities if these cyber-attacks

- have at least high gravity; and
- impact the assets which support either high-impact or critical-impact processes affecting the cross-border electricity flows.

In other words, the impact of a cyber-attack will need to have at least potential operational consequences for that cyber-attack to be reportable. As a result, the performance indicators selected will assess operational reliability, and they will be related to cybersecurity aspects of cross-border electricity flows.

[10] A non-binding provisional Electricity Cybersecurity Impact Index the ENTSO-E and the EU DSO entity developed in accordance with Article 48(2) of the NCCS ('**provisional ECII**') can be found on the ENTSO-E website: https://www.entsoe.eu/network_codes/nccs/. This provisional ECII includes high-impact and critical-impact thresholds.

[11] A team responsible for risk and incident handling in accordance with Article 10 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union ('**Directive 2022/2555**').

Furthermore, since cyber-attacks will not only be reportable pursuant to the NCCS when there has been an actual operational impact on cross-border electricity flows, but also when the assets supporting these flows have been compromised, the reportable cyber-attacks and the resulting performance indicators will be capable of generating a meaningful amount of datapoints.

4.2. Contextualisation

To the extent possible, performance needs to be measured in its context. Specifically, only gathering data on cyber-attacks affecting the entities and the resulting asset compromise would not demonstrate how the entities perform in the context of a changing threat landscape, including any occurrences of unpatched and actively exploited vulnerabilities[12].

For example, a substantial increase in the overall threat level in any given period accompanied by little to no increase in cyber-attacks impacting the assets which support the processes affecting the cross-border electricity flows would provide an indication that cybersecurity risk management measures implemented by the entities are effective.

Similarly, there may be a substantial increase in actively exploited unpatched vulnerabilities reported in any given period accompanied by little to no increase in cyber-attacks of 'high' or 'critical' gravity. This could provide an indication that, despite a substantial increase in exploited 'zero-day vulnerabilities', the countermeasures the entities had in place, such as network and system segregation, nevertheless reduced their impact.

Pursuant to Article 38(6) of the NCCS, the entities shall provide to their respective CSIRTs any information related to a reportable cyber threat that may have a cross-border effect. Such information shall be considered 'reportable' if:

- it provides relevant information for another entity to prevent, detect, respond or mitigate the impact of the risk;
- the identified techniques, tactics and procedures used in the context of an attack lead to information useful to contextualise and correlate the attack; or
- a cyber threat may be further assessed and contextualised with additional information provided by service providers or third parties not subject to the NCCS.

Furthermore, pursuant to Article 38(5) of the NCCS, the entities may notify relevant information related to unpatched actively exploited vulnerabilities to a CSIRT.

4.3. Universal applicability

Depending on the Union-wide high-impact and critical-impact processes identified pursuant to Article 19(2)(a) of the NCCS, the ECII and the high-impact and critical-impact thresholds established pursuant to Article 19(3)(b), the following entities could potentially be identified as 'high-impact' or 'critical-impact' entities, depending on the degree of impact of possible cyber-attacks on their operations of cross-border flows of electricity:

(a) electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity[13]. Namely, undertakings carrying out at least one of the following functions:

[12] Commonly referred to as 'zero-day vulnerabilities'. See Section 2, Table 1.

[13] OJ L 158, 14.6.2019, p. 125–199.

generation, transmission, distribution, aggregation, demand response, energy storage, supply or purchase of electricity, and who is responsible for the commercial, technical or maintenance tasks related to those functions;

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

(c) organised market places or 'organised markets' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014 of 17 December 2014 on data reporting [14] implementing Article 8(2) and Article 8(6) of Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency [15] that arrange transactions on products relevant to cross-border electricity flows;

(d) critical ICT service providers as referred to in Article 3(9) of the NCCS;

(e) ENTSO-E;

(f) EU DSO entity;

(g) balancing responsible parties as defined in Article 2(14) of Regulation 2019/943;

(h) operators of recharging points as defined in Annex I to Directive 2022/2555;

(i) regional coordination centres ('RCCs') as established pursuant to Article 35 of Regulation 2019/943;

(j) managed security service providers ('MSSP') as defined in Article 6(40) of Directive 2022/2555;

(k) any other entity or third party to whom responsibilities have been delegated or assigned pursuant to the NCCS.

The performance indicators should be designed in a manner that could make them applicable to as many entities as practicable. Thus, for example, while the operational security indicators listed in Article 15(3) and (4) of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation [16] could provide operational datapoints for the TSOs and potentially larger distribution system operators ('**DSOs**'), it is unclear how they could apply to other entities.

On the other hand, since the cyber-attack classification scale methodology developed under the NCCS will be applicable to all entities, so too will the performance indicator based on them (see Section 4.1.2).

4.4. Minimisation of data generation burden for the entities

If possible, the performance indicators should be based on data already generated by the entities.

Firstly, the entities will already have information sharing obligations under the NCCS, such as those referred to in Section 4.1 and Section 4.2 of this document. Secondly, given the non-binding nature of

[14] OJ L 363, 18.12.2014, p. 121–142.

[15] OJ L 326, 8.12.2011, p. 1–16.

[16] OJ L 220, 25.8.2017, p. 1–120.

the performance indicators, minimisation of data generation burden for the entities will be a key success factor.

Furthermore, the information collected based on the performance indicators, as well as the frequency of its collection, should be aligned with other reference points relevant to this assessment.

As noted in Section 4.2, these other reference points will constitute the implementation status of cybersecurity risk management measures by the entities. Since the entities will be required to report to their respective competent authorities information on the implementation status of cybersecurity controls every three years[17], ACER will also collect this information in cooperation with each competent authority[18] every three years. These cybersecurity controls will constitute a key part of the overall cybersecurity risk management measures ACER will monitor and correlate with the performance indicators.

Thus, considering the specific purpose of collecting the information based on the performance indicators, doing so every year does not appear necessary. Instead, the entities could specify the year in which an event occurred, as depicted in Table 3 (Section 3.2), so as to more accurately correlate the information collected with the implementation status of the cybersecurity risk management measures, as well as with itself. For example, by comparing the number of threat reports in any given year with the number of reportable cyber-attacks.

4.5. Minimisation of data sensitivity

Pursuant to Article 47(8) of the NCCS: *'Information that is confidential pursuant to Union and national rules shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Regulation. The information exchanged shall be limited to that which is necessary and proportionate to the purpose of that exchange.* (…)'

The performance indicators should thus be designed in a manner that minimises their utility to threat actors. For example, they should not contain any information relating to risk assessments, high-impact or critical-impact processes, or assets.

Therefore, the performance indicators should be limited to statistical information.

[17] Pursuant to Article 27(1) of the NCCS. Furthermore, pursuant to Article 12(2) of the NCCS, ACER shall publish a report at least every three years to, among other things, review the implementation status of the applicable cybersecurity risk management measures referred to in Article 12(2)(a) of the NCCS.

[18] Pursuant to Article 17(1) of the NCCS, ACER is required to monitor the implementation of cybersecurity risk management measures pursuant to Article 12(2)(a) of the NCCS in cooperation with each competent authority.