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

**20 November 2026**



# Table of contents


**1. Legal basis and structure of this document ..... 3**

**2. Three performance indicators ..... 5**

**3. Submission guidance ..... 7**

3.1. Submission once every three years ..... 7

3.2. Information to be submitted ..... 7

3.3. Process for submission ..... 10

3.3.1. Initial user registration ..... 10

3.3.2. Setting up two-factor authentication ..... 12

3.3.3. Accessing the data submission exercise in ACDC ..... 14

3.3.4. Submitting the 2026 performance indicator data ..... 15

**4. Criteria for selecting performance indicators ..... 18**

4.1. Link with electricity impact metrics ..... 18

4.1.1. Link with the processes and supporting assets that affect cross-border electricity flows 18

4.1.2. Alignment with metrics gauging potential impact on these assets and processes ..... 19

4.1.3. Statistical proxy to be applied by provisionally identified candidate entities – reported cyber-attacks ..... 19

4.2. Contextualisation ..... 20

4.2.1. Threats reported by high-impact and critical-impact entities under Cybersecurity Network Code ..... 20

4.2.2. Statistical proxy to be applied by provisionally identified candidate entities – identified threats ..... 20

4.3. Universal applicability ..... 21

4.4. Minimisation of data generation burden for the entities ..... 22

4.5. Minimisation of data sensitivity ..... 22

# 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 statistical 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 by the competent authorities in accordance with Article 48(3) of the NCCS[7] to share the statistical information in accordance with Section 3 of this document.

In order to enable candidates for high-impact and critical-impact entities to submit the required information, ACER separately defines

- performance indicators applicable to candidates for high-impact and critical-impact entities, and
- performance indicators subsequently applicable to entities identified as high-impact and critical-impact entities.

---

[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] Where appropriate, in several parts of this document, the high-impact entities and critical-impact entities identified by the competent authorities in accordance with Article 24 of the NCCS, as well as candidates for high-impact and critical-impact entities identified in accordance with Article 48(3) of the NCCS, are collectively referred to as '**entities**'.

Furthermore, ACER separately specifies

- information to be submitted by candidates for high-impact and critical-impact entities, and
- information to be subsequently submitted by entities identified as high-impact and critical-impact entities.

ACER would like to express its gratitude for the assistance provided in monitoring the performance indicators, which will contribute to the assessment of operational reliability related to cybersecurity of cross-border electricity flows.

For any questions regarding the performance indicators, please contact nccs@acer.europa.eu.

# 2. Three performance indicators

ACER issues the following three performance indicators applicable to **provisionally identified candidates** for high-impact entities and critical-impact entities:

Table 1: Three performance indicators applicable to candidates for high-impact entities and critical-impact entities

| Operational reliability performance indicator | NCCS Article | Categorised into |
|---|---|---|
| **Annual number of cyber-attacks reported as significant incidents under the NIS Directive[8] and the NIS 2 Directive[9]** | See note[10] | Candidates for high-impact entities and critical-impact entities |
| **Annual number of exploited unpatched ('zero day') vulnerabilities** | 38(5) | Candidates for high-impact entities and critical-impact entities |
| **Annual number of identified significant cyber threats** | See note[11] | Threat types listed in the Cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level ('**CRAM**')[12] |

In this context, a '**significant cyber threat**' should be understood as any threat arising from a malicious action that could disrupt one or more business processes of the entity concerned **or** of any other entity and ultimately impair the performance of its key functions, such as electricity generation, transmission or distribution.

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, pp. 1–30). Although the NIS Directive is no longer in force, not all Member States had implemented its successor, the NIS 2 Directive, by the end of 2025. Therefore, for the purposes of the initial data collection for 2026, references to significant incidents reported under the first NIS Directive have been retained.

[9] 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 (OJ L 333, 27.12.2022, pp. 80–152).

[10] Until high-impact entities and critical-impact entities are designated under Article 24 of the NCCS, the cyber-attacks reported as significant incidents under the NIS Directive and the NIS 2 Directive will be used as a statistical proxy for this performance indicator. Pursuant to Article 23(3) of the NIS 2 Directive, an incident shall be considered to be significant if (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; or (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

[11] Until high-impact entities and critical-impact entities are designated pursuant to Article 24 of the NCCS, significant cyber threats that may have a cross-border effect will be used as a statistical proxy for this performance indicator. These threats will be further categorised according to the threat types listed in the Cybersecurity risk assessment methodologies at Union, regional and Member State levels.

[12] On 15 October 2026, the competent authorities provided ENTSO-E and the EU DSO Entity with a position paper reflecting the consensus reached among the competent authorities on the Cybersecurity risk assessment methodologies at Union, regional and Member State levels. These methodologies are now published on the ENTSO-E website: https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Network%20codes%20documents/NCCS/NCCS_amended_Risk_assessment_methodologies.pdf.

For illustrative purposes, such business processes may include system monitoring and control, protection against faults, operational security analysis, outage planning and coordination, procurement of balancing services, load-frequency control, system defence and restoration, system congestion management, intraday or single day-ahead coupling, disconnecting or reducing load of customers through smart metering systems.

For further information on the processes and assets whose compromise could disrupt one or more key functions of an entity, please refer to the provisional list of Union-wide high-impact and critical-impact processes established by ENTSO-E and the EU DSO Entity.[13]

**Counting 'identified threats' for the purposes of this statistical reporting exercise:**

Where information relating to the same threat is obtained from multiple sources, the entity should correlate the information and count the threat only once.

## Performance indicators applicable to high-impact and critical impact entities designated pursuant to Article 24 of the NCCS

Once the high-impact and critical-impact entities have been designated by the competent authorities in accordance with Article 24 of the NCCS, the following performance indicators will apply:

Table 2: Three performance indicators applicable to high-impact and critical-impact entities

| Operational reliability performance indicator | NCCS Article | Categorised into |
|---|---|---|
| **Annual number of reportable cyber-attacks** | 38(3) | High-impact entities and critical-impact entities<br><br>High-gravity (level 4) and critical-gravity (level 5) cyber-attacks[14] |
| **Annual number of exploited unpatched ('zero day') vulnerabilities** | 38(5) | High-impact entities and critical-impact entities |
| **Annual number of reportable cyber threats that may have a cross-border effect** | 38(6) | Threat types listed in the Cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level |

[13] 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.

[14] 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.

# 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, 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 15 March**.

## 3.2. Information to be submitted

Table 3: General information

| General information type | Sample information |
|---|---|
| **Member State** | France |
| **Type of entity** | Distribution system operator |
| **At submission date, designated as** | Provisional critical-impact entity |

**'At submission date, designated as'**

The data collection tool includes four options:

- provisional high-impact entity (candidate);
- provisional critical-impact entity (candidate);
- high-impact entity; and
- critical-impact entity.

Table 4: Information based on performance indicators applicable to **candidates** for high-impact and critical-impact entities provisionally identified by the Competent Authorities in accordance with Article 48(3) of the NCCS, including sample counts

| Operational reliability performance indicator | Further categorisation | Count |
|---|---|---|
| | | 2026 |
| **Annual number of cyber-attacks reported as significant incidents under the NIS Directive and the NIS 2 Directive** | N/A | 2 |
| | | 0 |
| **Annual number of exploited unpatched ('zero day') vulnerabilities** | N/A | 3 |
| **Annual number of identified significant cyber threats** | Severe and unexpected corruption of the supply chain | 0 |
| | Unavailability of ICT products, ICT services, or ICT processes from the supply chain | 1 |
| | Cyber-attacks initiated through actors in the supply chain | 0 |
| | Leaking of sensitive information through the supply chain, including supply chain tracking | 0 |
| | Introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain | 0 |
| | Attacks through communication networks | 3 |
| | Attacks through removable media | 0 |
| | Unauthorized system access | 0 |
| | Malware intrusion | 2 |
| | Social engineering | 0 |
| | Cyber-attack enabled by unauthorised physical access | 0 |
| | Insider threats | 0 |
| | Other | 0 |

Table 5: Information based on performance indicators applicable to high-impact and critical-impact entities identified by the competent authorities in accordance with Article 24 of the NCCS, including sample counts

| 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 |
| | Cyber-attack enabled by unauthorised physical access | 0 | 0 | 0 |
| | Insider threats | 0 | 0 | 0 |
| | Other | 0 | 0 | 0 |

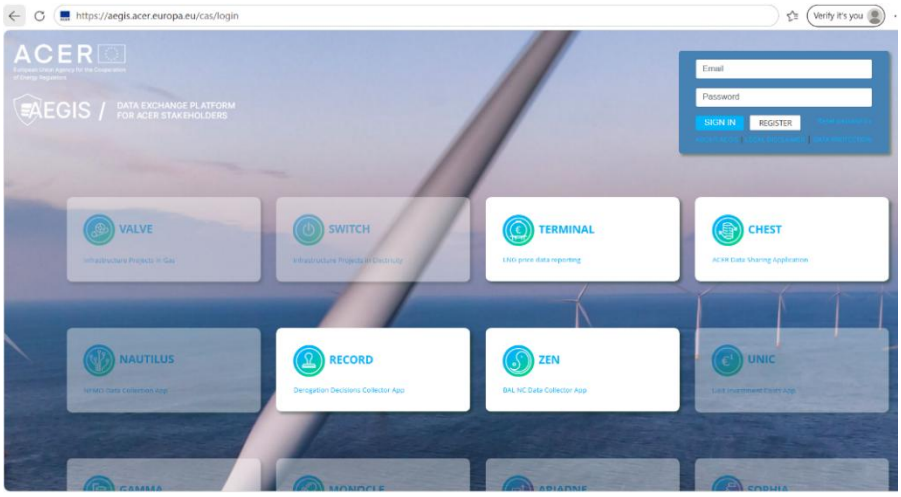
## 3.3. Process for submission

ACER will provide the entities with access to a secure online tool, 'ACDC', hosted on the ACER Electricity and Gas Information System ('AEGIS'), through which they will be requested to submit the information described in Section 3.2.

### 3.3.1. Initial user registration

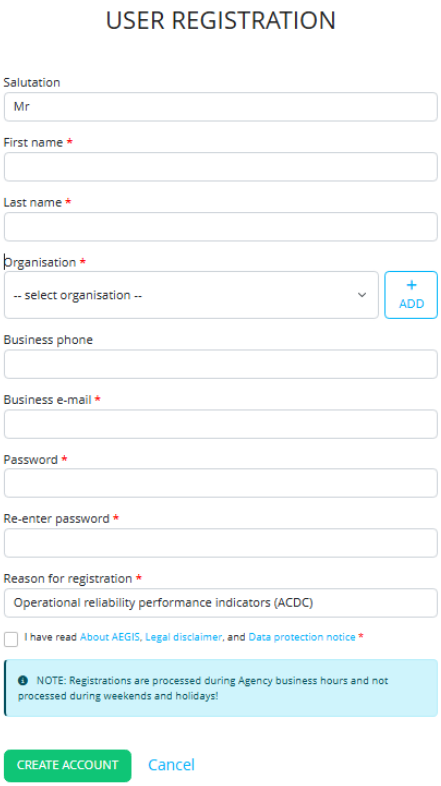
Users with no access to AEGIS system can self-register following provided URL: https://aegis.acer.europa.eu/.

Figure 1: AEGIS login screen




Please click the '**REGISTER**' button to open the user registration form:

Figure 2: AEGIS user registration form



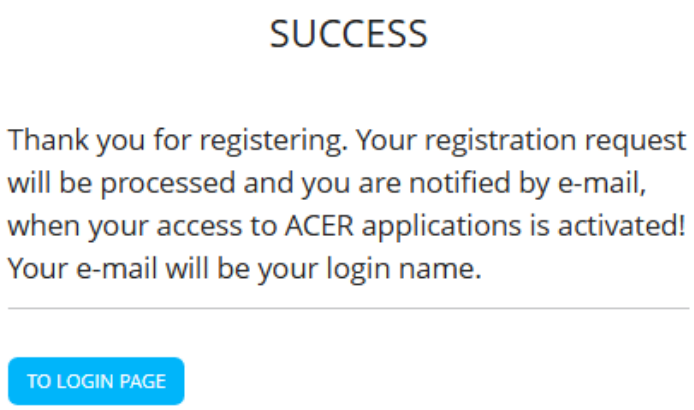
Please fill in required data and accept AEGIS legal disclaimer and data protection notice.

**IMPORTANT:**

- If you cannot find your organisation in the 'Organisation' drop-down box, please press the '+' sign and add it manually.
- Please ensure that you select '**Reason for registration'** as '**Operational reliability performance indicators (ACDC)**'.
- Please ensure that the email domain can be associated with the organisation you enter. Generic email addresses, such as Gmail or Hotmail, cannot be approved.

Next, click the '**CREATE ACCOUNT**' button to initiate the self-registration process. The system will then notify you that your registration request has been successfully submitted.

Figure 3: Successful initiation of AEGIS user registration process




Please note that the average processing time for submitted user registration requests is one business day.

Once the registration request has been processed, you will receive an email notification informing you of the access approval decision.

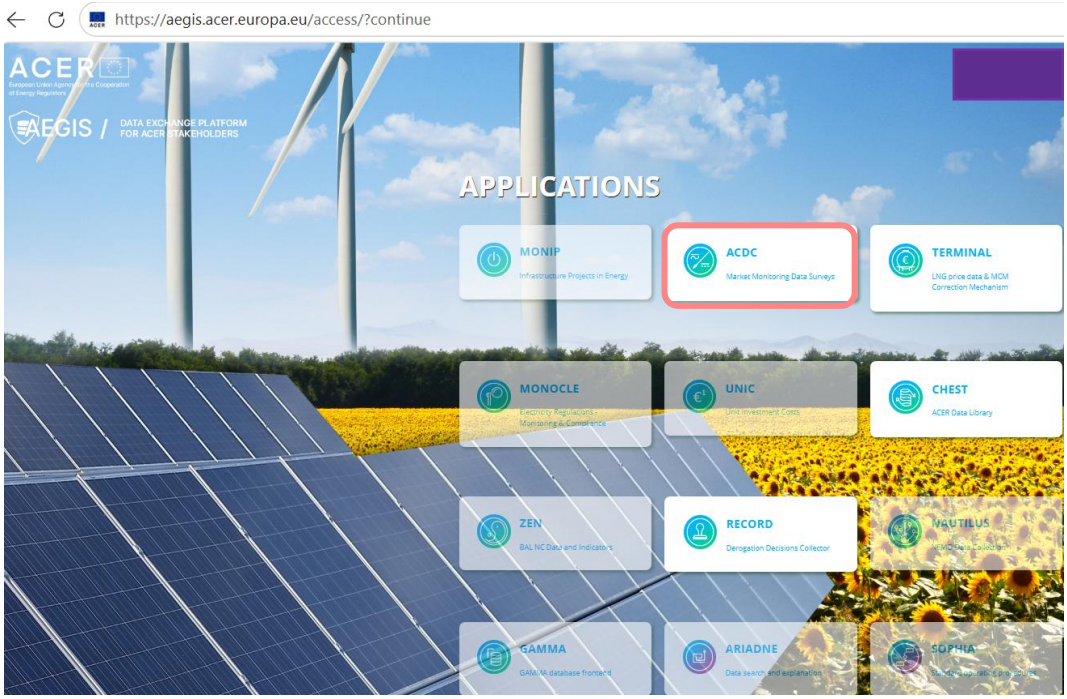
If the registration request is approved, you will be able to proceed to log in to AEGIS using the following URL: https://aegis.acer.europa.eu/.

### 3.3.2. Setting up two-factor authentication

Log in to the AEGIS system using your username (business email address) and the password you created during the registration process.

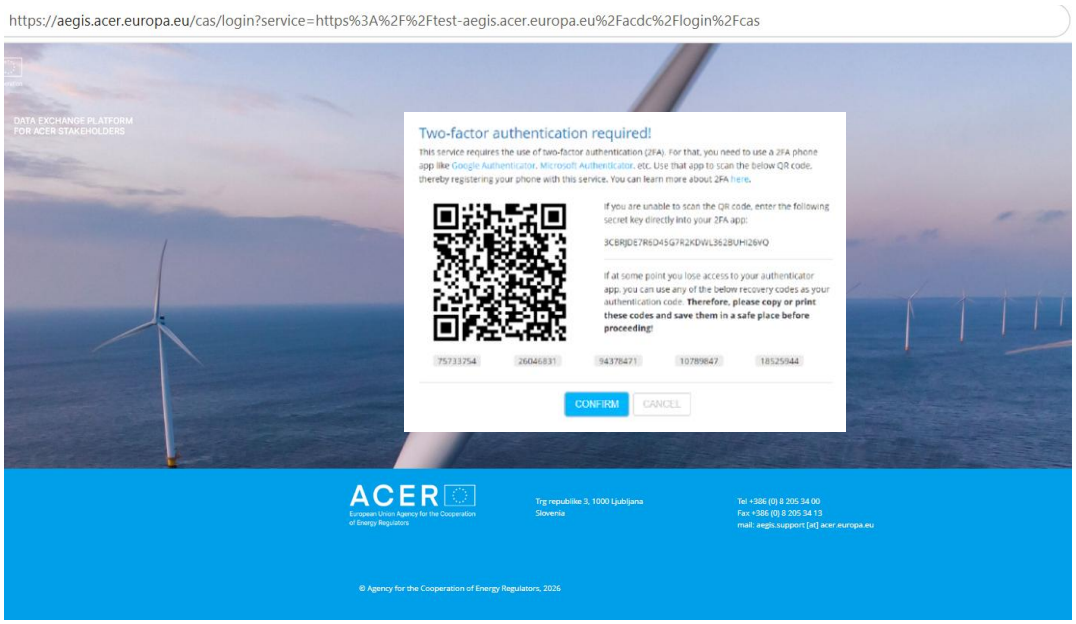
Once you have signed in to AEGIS, select the **ACDC** application.

Figure 4: Selecting the ACDC application




The first time you access the **ACDC** application, the system will prompt you to complete the user registration process by setting up two-factor authentication.

Figure 5: Authenticator initialisation window



Detailed instructions on how to set up two-factor authentication are available in the user manual at the following link:

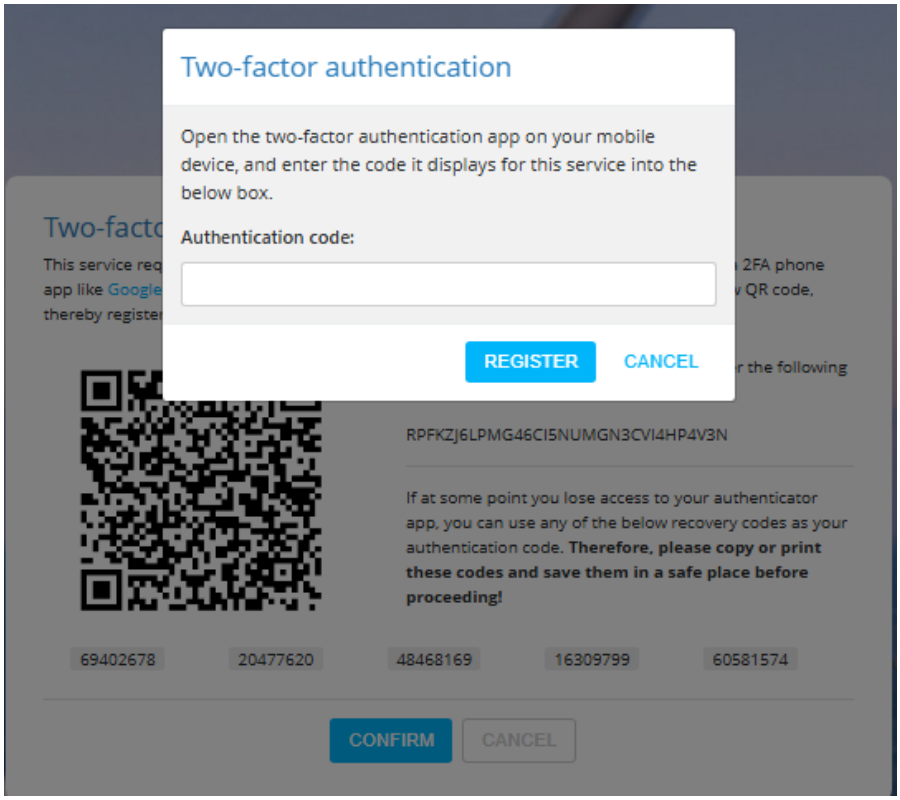
https://aegis.acer.europa.eu/docs/terminal/terminal-2fa-users-manual.pdf

Two-factor authentication can be configured using an authenticator application, such as Google Authenticator or Microsoft Authenticator. When using Microsoft Authenticator, please ensure that you configure the application by manually entering the 32-character secret key (see Appendix A of the Two-Factor Authentication (2FA) User Manual).

**Before closing the authenticator initialisation window, make sure to save your recovery codes in a safe place. These codes will allow you to access the system if you lose access to your authenticator application.**

After scanning the QR code using Google Authenticator or manually entering the secret key into Microsoft Authenticator, you will be prompted to enter an authentication code twice. The first entry is required to confirm and complete the authenticator set-up.

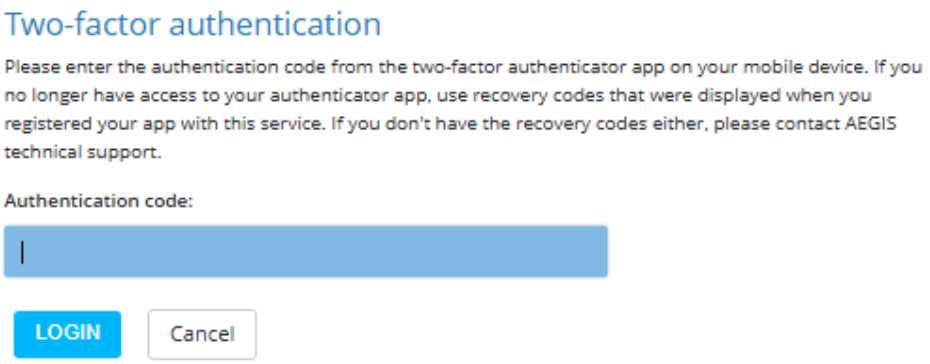
Figure 6: Approving the authenticator setup




The second entry is required to authenticate your access to the ACDC application.

Please wait for the authentication code to refresh before entering the new code in the two-factor authentication box displayed by ACDC.

Figure 7: Entering the authentication code to access the ACDC application

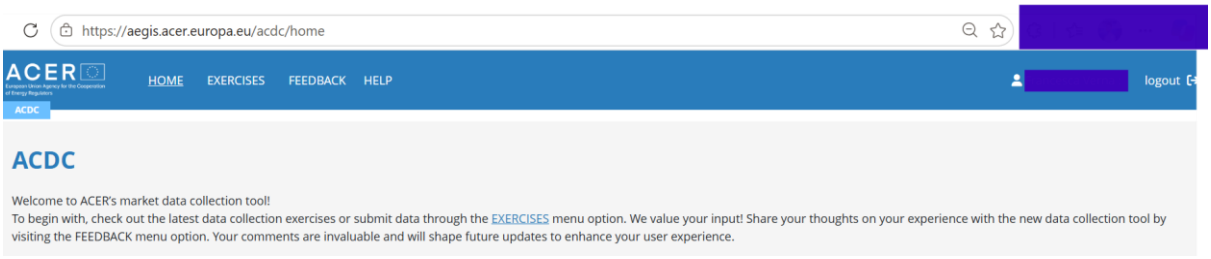



Once you have completed the two-factor authentication set-up, you will be prompted to enter an authentication code each time you access the ACDC application.

### 3.3.3. Accessing the data submission exercise in ACDC

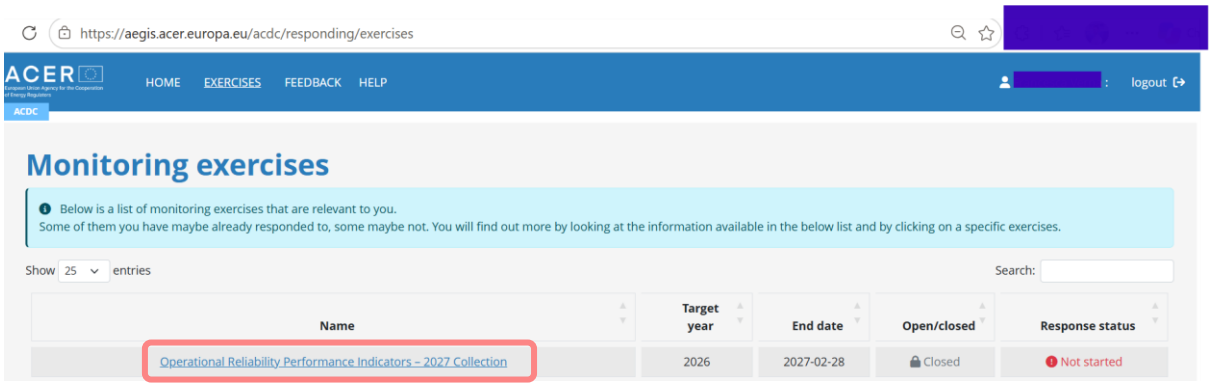
Once you have successfully authenticated using your account credentials and two-factor authentication, you will be presented with the ACDC landing page.

Figure 8: ACDC landing page




Please select the '**EXERCISES**' option in the ACDC application toolbar to view the list of exercises assigned to you. From the list, select '**Operational Reliability Performance Indicators – 2027 Collection**'.

Figure 9: ACDC monitoring exercise list



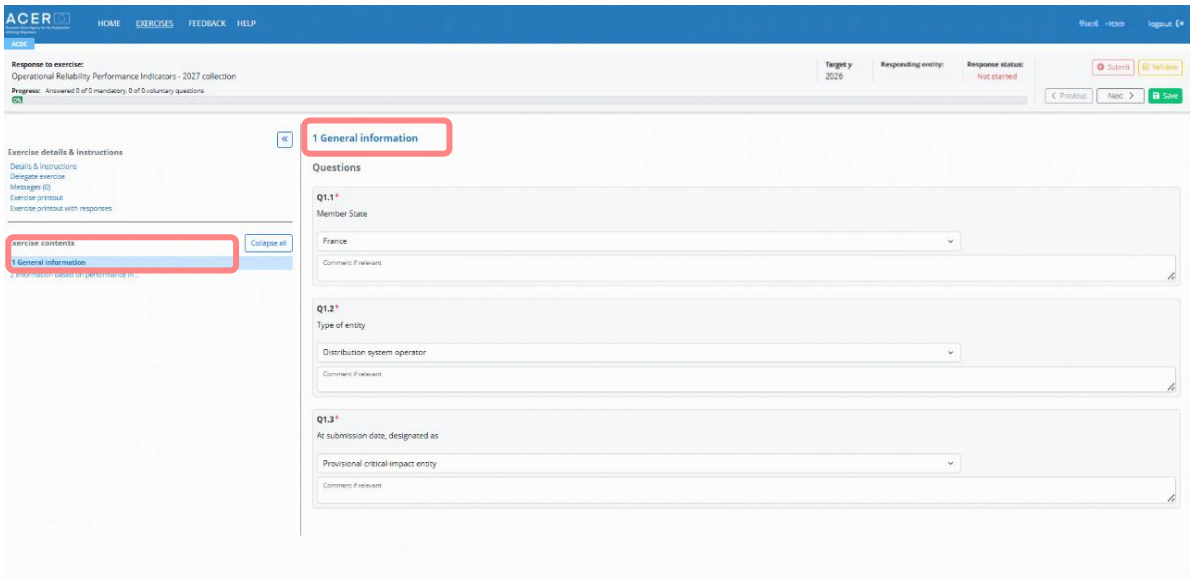
### 3.3.4. Submitting the 2026 performance indicator data

The data collection tool requests you to submit the information described in Section 3.2.

When you open the exercise, you will be taken to the exercise details page. To access the questions, use the '**Exercise contents**' menu on the left-hand side and select '**1. General information**' to get started.

This section requests the general information described in Table 3 of this guidance document.

Figure 10: Exercise menu – general information




Once completed, click the '**Save'** button before advancing to exercise content **'2 Information based on performance indicators'** in the same menu. This section requests the submission of information based on the performance indicators applicable to candidates for high-impact and critical-impact entities (provisional entities), as described in Table 4:

Figure 11: Information based on performance indicators – Questions 2.1 and 2.2

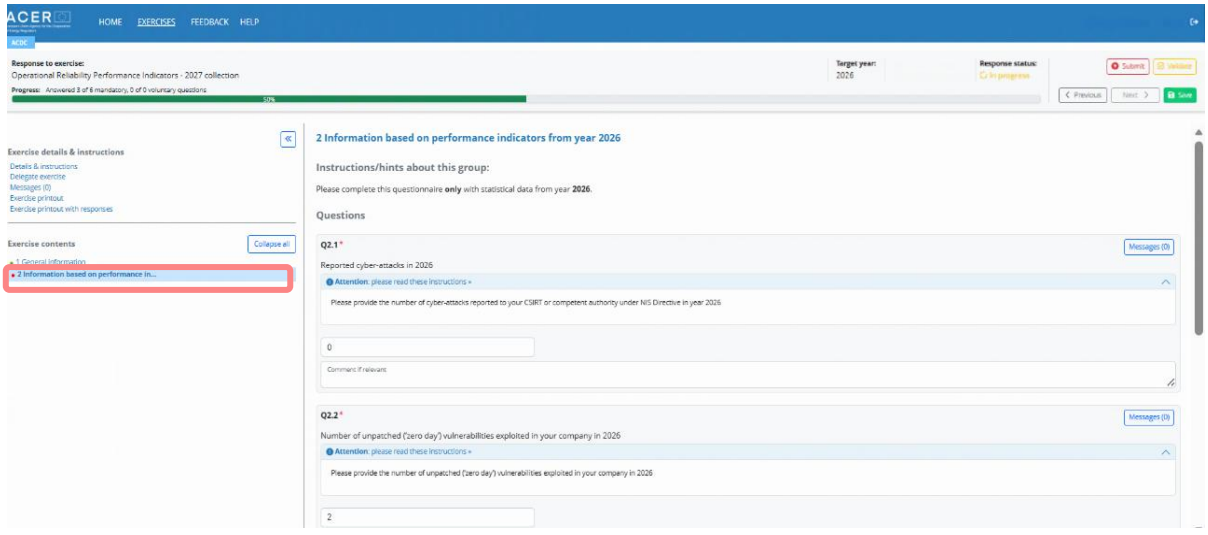
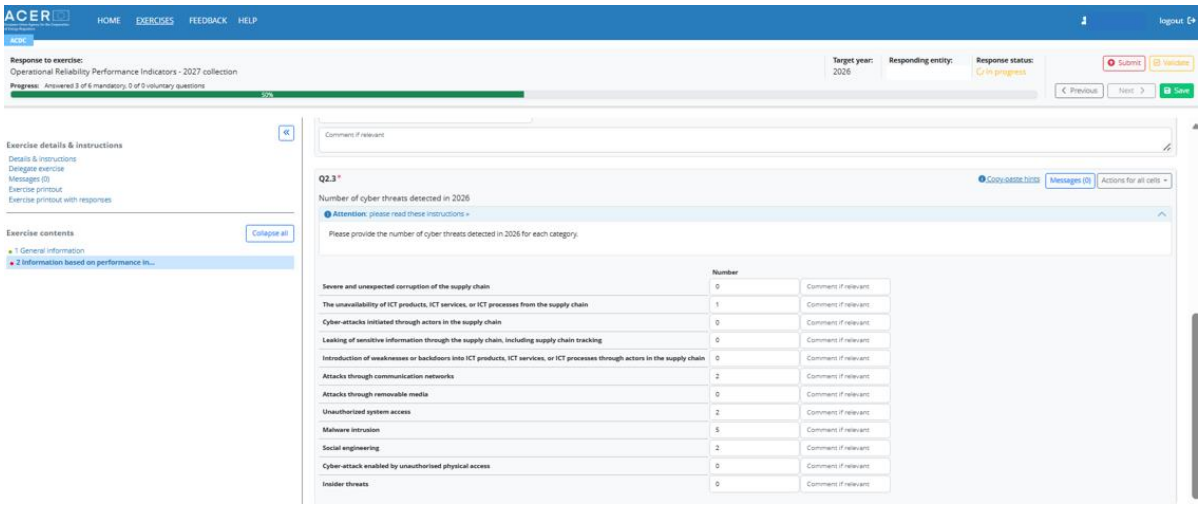
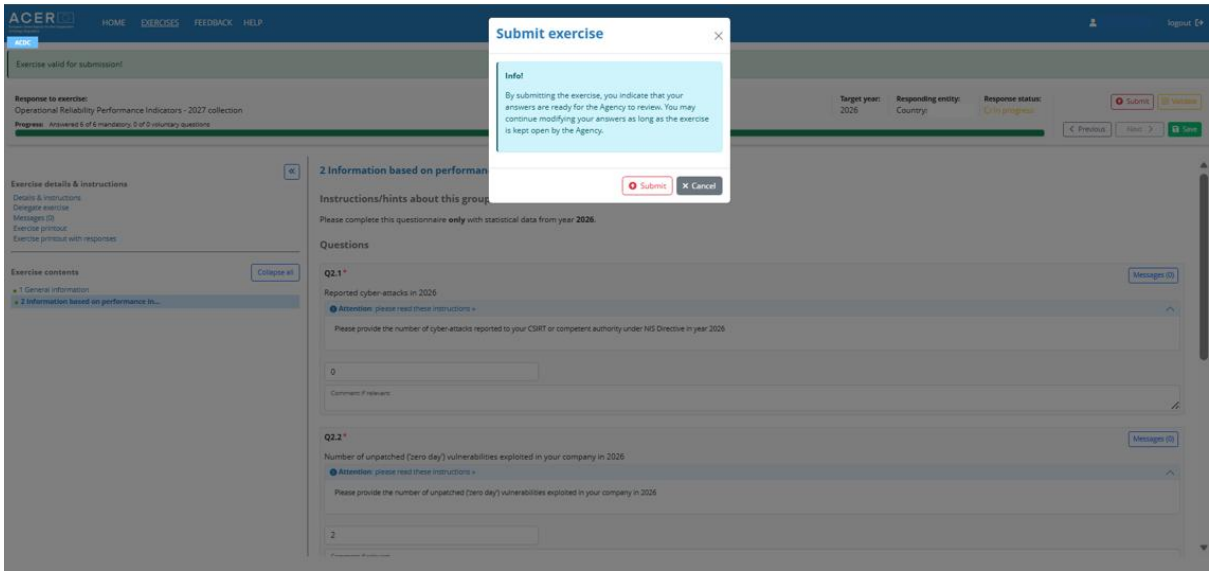


Figure 13: Information based on performance indicators – Question Q2.3



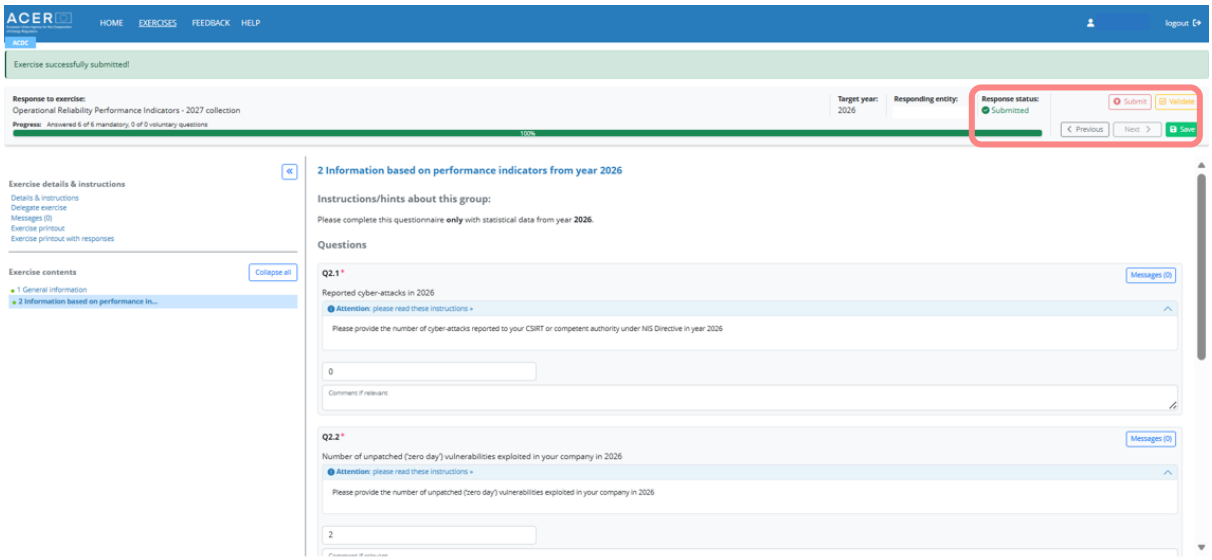

Please review the exercise data you have entered. Once you have completed your review, you can submit the exercise by clicking the red ‘SUBMIT’ button and confirming your submission in the pop-up window.

Figure 14: Exercise submission



After exercise submission, the response status will change to ‘Submitted’, and the bar immediately below the blue menu will turn green.

Figure 15: Exercise status - ‘Submitted’




*Please note that some functionalities of the tool, such as the ‘Delegate exercise’ and ‘Messages’, are not relevant for this exercise.*

Should you have any questions regarding the submission process, please contact nccs@acer.europa.eu.

ACER will be grateful for your assistance in monitoring the performance indicators, which will contribute to the assessment of operational reliability related to cybersecurity of cross-border electricity flows.

# 4. Criteria for selecting 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. 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.

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[15].

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.

[15] 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.

### 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**')[16] 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.

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.

### 4.1.3. Statistical proxy to be applied by provisionally identified candidate entities – reported cyber-attacks

Until high-impact entities and critical-impact entities are designated pursuant to Article 24 of the NCCS, cyber-attacks reported as significant incidents under the NIS Directive and the NIS 2 Directive shall be used as a statistical proxy for this performance indicator.

Pursuant to Article 23(3) of the NIS 2 Directive, an incident shall be considered significant if:

- it has caused, or is capable of causing, severe operational disruption of the services provided by the entity concerned or financial loss to that entity; or
- it has affected, or is capable of affecting, other natural or legal persons by causing considerable material or non-material damage.

For the purposes of this statistical proxy, **only significant incidents involving cyber-attacks are taken into account**.

[16] A team responsible for risk and incident handling in accordance with Article 10 of NIS 2 Directive.

## 4.2. Contextualisation

### 4.2.1. Threats reported by high-impact and critical-impact entities under Cybersecurity Network Code

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[17].

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.

### 4.2.2. Statistical proxy to be applied by provisionally identified candidate entities – identified threats

Until high-impact entities and critical-impact entities are designated pursuant to Article 24 of the NCCS, identified significant cyber threats with potential cross-border effects will be used as a statistical proxy for the reportable threats referred to in Article 38(6) of the NCCS.

In this context, a 'significant cyber threat' should be understood as any threat arising from a malicious action that could disrupt one or more business processes of the entity concerned or of any other entity and ultimately impair the performance of its key functions, such as electricity generation, transmission or distribution.

For further details, please refer to the explanatory note below Table 1 in Section 2.

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

## 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[18]. Namely, undertakings carrying out at least one of the following functions: 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[19] 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[20] 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[21] could provide operational datapoints for the TSOs and potentially larger distribution system operators ('**DSOs**'), it is unclear how they could apply to other entities.

[18] OJ L 158, 14.6.2019, p. 125–199.

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

[20] OJ L 326, 8.12.2011, p. 1–16.

[21] OJ L 220, 25.8.2017, p. 1–120.

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). The same rationale applies to cyberattacks reported as significant incidents pursuant to the NIS Directive or the NIS 2 Directive (see Section 4.1.3).

## 4.4. Minimisation of data generation burden for the entities

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

Given the non-binding nature of the performance indicators, minimising the additional data-generation burden on entities will be a key success factor. In this context, entities have already been subject to information-sharing obligations under the NIS Directive and the NIS 2 Directive, which will be further complemented by obligations under the NCCS, including those referred to in Sections 4.1 and 4.2 of this document.

Where the information concerned is not yet subject to reporting obligations, such as information relating to the identification of cyber threats, entities could nevertheless be expected to have relevant statistical data available in the ordinary course of their cybersecurity operations.

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[22], ACER will also collect this information in cooperation with each competent authority[23] 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 5 (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 other performance indicators. 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.

---

[22] 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.

[23] 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.

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