ACER

European Union Agency for the Cooperation of Energy Regulators

Cybersecurity benchmarking guide

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

13 June 2025

Cybersecurity benchmarking guide

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

13 June 2025

Find us at:

ACER

E press@acer.europa.eu
Trg republike 3
1000 Ljubljana
Slovenia

www.acer.europa.eu

Table of contents

1. Scope of this guide

ACER[1] has established this cybersecurity benchmarking guide for the national regulatory authorities for the electricity sector[2] (the '**NRAs**'), in cooperation with ENISA[3], pursuant to Article 13(1) of the Commission Delegated Regulation (EU) 2024/1366 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows[4] (the '**NCCS**').

In accordance with Article 13(1) of the NCCS, this guide explains the principles of benchmarking of the implemented cybersecurity controls, taking into account the costs and the effectiveness of the processes, products, services, systems and solutions used to implement such controls.

In preparation of this guide, ACER has taken into account existing benchmarking reports.

1.1. Benchmarking analysis to be carried out by the NRAs

According to Article 13(2) of the NCCS, within 12 months after the establishment of this guide, the NRAs shall assess whether current investments in cybersecurity:

(a) mitigate risks having an impact on cross-border electricity flows;

(b) provide the desired results and engender efficiency gains for the development of the electricity systems; and

(c) are efficient and integrated into the overall procurement of assets and services.

Furthermore, according to Article 13(3) of the NCCS, for the benchmarking analysis, the NRAs shall assess in particular:

(a) the average expenditure related to cybersecurity for mitigating risks having an impact on electricity cross-border flows, especially with respect to the high-impact and critical-impact entities;

(b) in cooperation with the ENTSO-E and the EU DSO entity, the average prices of cybersecurity services, systems and products that contribute to a large extent to the enhancement and maintenance of the cybersecurity risk-management measures in the different system operation regions; and

(c) the existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of the NCCS, identifying possible measures necessary to foster efficiency in spending, particularly where cybersecurity technological investments may be needed.

---

[1] 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).

[2] Designated by each Member State pursuant to Article 57(1) 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 (OJ L 158, 14.6.2019, p. 125–199).

[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). Hereinafter referred to as the '**Cybersecurity Act**'.

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

1.2. Structure of this guide

The main part of this guide, Section 2, consists of ten subsections, each of which explains a different principle of cybersecurity benchmarking, including its significance and possible application in the context of the benchmarking analysis pursuant to Article 13(2) and Article 13(3) of the NCCS. In addition, in Annex 1, this guide includes two templates to assist the NRAs with gathering information from the entities subject to the benchmarking.

Most of the discussed principles are related to measuring or comparing the costs of implementation of cybersecurity controls and the effectiveness of processes, products, services, systems and solutions implementing them. The remaining principles explained in this guide can be considered auxiliary to these general objectives, and cover matters such as understanding the context and potential use of the output of the benchmarking analysis under the NCCS, as well as considerations as to its scope.

This guide does not cover the detail of the administrative process of conducting the benchmarking analysis. For example, the steps or the means of contacting the relevant stakeholders at national level, or detailed methods of data analysis.

Furthermore, this guide does not address the details of cooperation among the NRAs, or the specific format of the final output of the benchmarking analysis to be shared with all NRAs, all competent authorities[5], ACER, ENISA and the European Commission pursuant to Article 13(5) of the NCCS.

Finally, while ACER has established this cybersecurity benchmarking guide with the intention of providing as much assistance to the NRAs as possible, ACER nevertheless stresses its non-binding nature. The NRAs may adopt a different approach to their benchmarking analysis, in whole or in part.

[5] Responsible for carrying out the tasks assigned to them under the NCCS and designated by Member States pursuant to Article 4(1) of the NCCS.

2. Principles of cybersecurity benchmarking

2.1. Benchmark to learn and set targets

From its preparatory stage, when performing a benchmarking analysis, it is advisable to identify and bear in mind the purpose of such benchmarking. Having clarity on the purpose of benchmarking may have the following uses:

- firstly, it will assist with the development of further guiding objectives by the NRAs;
- secondly, where the objectives are already stipulated, as it is the case with Article 13(2) and Article 13(3) of the NCCS, it will assist with their fulfilment.

Thus, the benchmarking exercise should be set up, including the preparation of any questionnaires, and subsequently carried out in a way which ensures that its outputs are aligned with their intended use. This principle also applies to the identification and implementation of any refinements or amendments, which could be identified as necessary during the benchmarking exercise.

Two non-exhaustive examples of how the NRAs could use the outputs of the benchmarking analysis are outlined in this section.

2.1.1. Cost recovery via network tariffs

In general, benchmarking is used as a tool for learning, forecasting and target setting. For example, in the context of network tariff regulation.

On the one hand, the entities under network tariff regulation provide critical services which benefit consumers and businesses. On the other hand, the NRAs have a role in monitoring the costs incurred by these entities so that they are incurred efficiently. Thus, benchmarking analysis can assist with setting objective targets to foster this monitoring process.

In the context of the implementation of the NCCS, the NRAs could, for example, use the output of the benchmarking analysis as a reference point for the Article 11 cost assessment. Pursuant to this provision, TSO and DSO *'*[c]*osts assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms, as determined by the relevant NRA'*[6]. Consequently, the NRAs could refer to the data points generated by the Article 13 benchmarking analysis, and in particular their respective national analyses, to assist them in the assessment of the aforementioned reasonableness, efficiency and proportionality.

To the extent consistent with the requirements of Article 13(2) and Article 13(3) of the NCCS, the NRAs could therefore implement the benchmarking analysis and capture its outputs, so that both their nature and format make them a useful reference for the cost recovery assessment pursuant to Article 11 of the NCCS.

2.1.2. Identifying cost efficiency measures

The second example is explicitly referred to in Article 13(3)(c) of the NCCS: *'identifying possible measures necessary to foster efficiency in spending, particularly where cybersecurity technological investments may be needed'.* To that end, according to the same article, the NRAs shall focus on *'the existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of this Regulation'.*

[6] Article 11(2) of the NCCS.

During the administration of the benchmarking analysis, it could transpire to the NRAs that various cybersecurity services, systems and solutions have comparable functions, yet different costs, depending on how they are implemented. For example, the benchmarking analysis could reveal that certain types of entities would benefit from exploring resource pooling or outsourcing of cybersecurity services, systems and solutions as a means of fostering cost efficiency.

Furthermore, as expressly stipulated by Article 13(3)(c), the benchmarking analysis could identify a need to develop specific types of cybersecurity services, systems and solutions, so that certain types of entities can manage cybersecurity risks to their operations in a more cost efficient manner. Illustrative examples of this could be effective network defences, security solutions for operational technology systems or intrusion prevention systems that would be particularly well-suited for smaller entities.

Overall, the principles listed in this guide have been selected and explained bearing in mind both the requirements of Article 13(2) and Article 13(3) of the NCCS, as well as the potential application of the outputs of the benchmarking analysis in the context of the cost recovery assessment pursuant to Article 11 of the NCCS.

For completeness, the outputs of the benchmarking analysis could also provide input to policy development and implementation by any of its addressees referred to in Article 13(5) of the NCCS. Namely, all NRAs, all competent authorities, ACER, ENISA and the Commission.

2.2. Limit the information requested and the level of complexity to what is required

One of the consequences of the application of the first principle explained in Section 2.1. is limiting the information requested from the entities and the level of complexity of the benchmarking analysis to what is required by such analysis. In this specific context, to what is required by Article 13(2) and Article 13(3) of the NCCS.

The recommendations included in this guide strive to incorporate this principle. For context, two examples are provided in this section. One concerning the evaluation of the costs of cybersecurity and one concerning the evaluation of its effectiveness.

Regarding the former, the information requested should be limited to what is required for the evaluation of costs in the context of Article 13(2)(c), Article 13(3)(a) and Article 13(3)(c) of the NCCS. The NRAs could use the list of cost items discussed in Section 2.5.1 to that end. Based on these cost items, the NRAs could gather the cost summaries from the entities on a per item basis. On the other hand, requesting more detailed costing data, such as salary breakdowns of staff members or detailed breakdowns of hardware maintenance and operational costs may be disproportionate.

Beyond standardised references to mitigations the NRAs may consider requesting in the context of the ‘comparability’ criterion referred to in Article 13(3)(c) (see Section 2.10.2), the NRAs should not request detailed information on entity-specific vulnerabilities that could be useful to the attackers.

Similarly, when evaluating the effectiveness and efficiency of current cybersecurity investments in the context of Article 13(2), including the risk mitigation they provide, the extent and level of detail of the information requested should be limited to what is required for the purposes of this benchmarking exercise. The benchmarking assessment required by Article 13(2) and Article 13(3) has several aspects, which means that it needs to be designed in a manner fulfilling the requirements encapsulated in these provisions, while keeping the workload manageable for the entities and the NRAs.

Crucially, as the first step, most of the entity-level assessment should be carried out by the entities **internally**, as its outputs will also constitute inputs for subsequent assessment conducted by NRAs. This is the case for the evaluation of both costs and effectiveness of cybersecurity investments. For example, the initial cost calculations against the reference cost items discussed in Section 2.5.1, including the application of any accounting principles and macroeconomic factors, should be performed internally by the entities. The NRAs, on their part, will need to ensure that the entities are uniformly advised on their application.

In conclusion, overall, data points required for the assessment of current cybersecurity investments in the context of Article 13(2) should not be as extensive or as detailed as data points which may be used in the context of evaluating the performance and effectiveness of the cybersecurity management system[7], internal audits[8], cybersecurity management system implementation reviews[9], or verification of the common electricity cybersecurity framework pursuant to Article 31 of the NCCS. Instead, simpler and more general assessment questions could be used, appropriate to what Article 13(2) and Article 13(3) of the NCCS require.

Based on this approach, this guide provides examples of questions which could be used by the NRAs.

2.3. Carry out national analyses following a uniform approach

According to Article 13(3)(a) of the NCCS, the NRAs shall assess *'the average expenditure related to cybersecurity for mitigating risks having an impact on electricity cross-border flows* (…)*'.* Furthermore, according to Article 13(3)(b) of the NCCSs, the NRAs shall assess *'the average prices of cybersecurity services, systems and products* (…) ***in the different system operation regions****'*.

Article 13(3)(a) does not indicate the level at which the NRAs shall assess the average expenditure as explicitly as Article 13(3)(b). Namely, whether such assessment should be carried out at a Member State-level, regional-level, or Union-level. However, given the references to 'the NRAs', instead of 'each NRA', and the singular form reference to '**the** average expenditure', without an affix 'in each Member State', ACER recommends designing and performing the benchmarking analysis in each Member State in a uniform manner. This will allow the NRAs to compare and aggregate their national benchmarking analyses, as well as to calculate the regional and Union-wide averages.

Consequently, all recommendations encapsulated in this guide imply their uniform application by the NRAs.

2.3.1. Recommended costing period: 2022-2024

One of the fundamental aspects the NRAs need to agree upfront is a reasonable and appropriate time period from which cybersecurity costs would be taken into account for calculating the averages. Namely, the annualised CAPEX and the OPEX.

In doing so, the NRAs will need to strike a balance between, among other things, the time period being sufficiently representative in light of various fluctuations, but also reasonable so as to keep the

[7] For example, pursuant to Article 32(1)(j) of the NCCS.

[8] For example, pursuant to Article 32(1)(k) of the NCCS.

[9] For example, pursuant to Article 32(1)(l) of the NCCS.

workload for the entities providing the data (see Section 2.4 below) and the NRAs at a manageable level.

Furthermore, pursuant to Article 13(1) of the NCCS, the NRAs will need to complete the benchmarking analysis within 12 months after the establishment of the benchmarking guide by ACER. The NRAs would therefore be advised to commence gathering the data shortly after ACER establishes this guide.

ACER notes that the above means that the benchmarking analysis would not include the 2025 expenditures, which fall in the first full year after the transposition deadline 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 (the '**NIS 2 Directive'**)[10]. In order to address this, the NRAs could consider refreshing the analysis with additional follow-up data after one or two years.

The time periods applied in existing benchmarking and costing reports vary from one year snapshots to as many as 10 years. In light of the balance referred to above and the fact that the calculations would, in any event, be based on the annual OPEX and annualised CAPEX, three years appear to constitute a reasonable time period for the purposes of the benchmarking analysis pursuant to Article 13(2) and Article 13(3) of the NCCS.

Thus, the NRAs could base their analysis on the costs incurred in years 2022-2024.

2.3.2. Convert all costs to EUR for the purposes of cross-country analysis

In order for the results of Member State-level analyses to be comparable and possible to aggregate, the NRAs should ensure that all the costs are converted to EUR.

To that end, for the CAPEX, the NRAs could request the application of the average currency exchange rate of the local currency to EUR published by the European Central Bank (the '**ECB**') in the year when the CAPEX in question was incurred. This could be the year when the transaction was first recorded in a general ledger.

For the OPEX, the NRAs could request the application of the average currency exchange rate of the local currency to EUR published by the ECB each year when the OPEX in question was recorded in a general ledger.

2.4. Align information sources with benchmarking requirements

In the context of this section, the term 'information sources' should be understood broadly to cover any sources which could provide the information required to carry out the benchmarking analysis pursuant to Article 13(2) and Article 13(3) of the NCCS.

In general, the scope of benchmarking analysis should correspond to its purpose, including the desired outputs. For example, to the extent that the purpose of benchmarking is to provide input to network tariff regulation, the scope of benchmarking would include, at a minimum, the costs recoverable through network tariffs.

[10] OJ L 333, 27.12.2022, p. 80–152.

However, as discussed in Section 2.1, the purpose of the benchmarking analysis referred to in Article 13(2) and Article 13(3) of the NCCS is broader than creating reference points for the cost recovery assessment pursuant to Article 11 of the NCCS.

Firstly, Article 13(3)(a) of the NCCS refers to assessing the average expenditure, *'especially with respect to the high-impact and critical-impact entities'*. Since the high-impact and critical-impact entities will not be identified in time for the benchmarking analysis[11], in the context of Article 13(3)(a), the reference to 'the high-impact and critical-impact entities' could be interpreted as a reference to the candidates for high-impact and critical-impact entities the competent authorities shall identify in their Member States by 13 February 2025 pursuant to Article 48(3) of the NCCS.

The entities providing the benchmarking information in each Member State for the purposes of the analysis encapsulated in Article 13(2) and Article 13(3)(a) of the NCCS could therefore be the ones identified in the national provisional lists of high-impact and critical-impact entities developed by the competent authorities pursuant to Article 48(3) of the NCCS. This would also enable the NRAs to perform the benchmarking analysis by entity type, as listed in Article 2(1) of the NCCS.

Secondly, Article 13(3)(b) of the NCCS refers to 'average prices' of cybersecurity services, systems and products, which could be interpreted as carrying out market research, in cooperation with the ENTSO-E and the EU DSO entity, to obtain the relevant information in the different system operation regions. In other words, in the context of gathering price data on these items, the source of information could be their suppliers.

Thirdly, Article 13(3)(c) of the NCCS refers to *'the existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of this Regulation'*. The NRAs will thus require appropriate information, in particular from the entities, to carry out the comparability assessment required by this article. In determining such information and carrying out the respective analysis, the NRAs could, among other things, refer to the provisional guidance established by the ENTSO-E, in cooperation with the EU DSO entity. Namely:

- the provisional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows to be developed pursuant to Article 48(6) of the NCCS[12]. Specifically, the NRAs could refer to the cybersecurity controls which shall be included in this guidance pursuant to Article 48(7)(b) of the NCCS; and
- the provisional list of Union-wide high-impact and critical-impact processes developed pursuant to Article 48(4) of the NCCS[13].

2.5. Define the cost and price items

Another element of preparation of a benchmarking analysis is defining the data to be collected. This could be executed in two steps: firstly, defining the 'cost items' and, secondly, defining an approach to evaluating their costs, as well as other potential attributes. This section explains the principle of cost

[11] Such identification will take place following the Union-wide risk assessment, pursuant to Article 24(1) of the NCCS, by using the 'Electricity Cybersecurity Impact Index' and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3)(b) of the NCCS.

[12] By 13 June 2025.

[13] https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Network%20codes%20documents/NCCS/Provisional%20list%20of%20Union-wide%20high-impact%20and%20critical-impact%20processes.pdf (hyperlink last verified on 10 June 2025).

item definition in the context of the Article 13 cybersecurity benchmarking, as well as the proposed approach to its application.

Defining cost items upfront ensures that the benchmarking analysis of costs, effectiveness and efficiency is based on common reference points and can thus be meaningful. It is common practice in existing benchmarking studies and analyses, such as those on electricity and gas infrastructure.

2.5.1. Cost item reference list – two alternative approaches

Similarly to the information sources, cost item definition must be aligned with the requirements of Article 13 of the NCCS. In this respect:

- Article 13(1), second sentence, refers to *'benchmarking of the **implemented** cybersecurity controls'* and *'the costs of implementing the controls and* (…) ***processes, products, services, systems and solutions** used to implement such controls'*;
- Article 13(2) refers to benchmarking ***'current investments** in cybersecurity'*, and Article 13(2)(a) refers to mitigating *'risks having an impact on cross-border electricity flows'* as an assessment criterion;
- Article 13(3)(a) refers to 'expenditure'; and
- Article 13(3)(c) refers to *'the **existence and level of comparability** of costs and functions of cybersecurity services, systems and solutions'* and *'identifying possible measures necessary to foster **efficiency in spending**'*.

What follows from the above is that the first aspect of the benchmarking analysis under Article 13 of the NCCS could be understood as the existing processes, products, services, systems and solutions mitigating risks having an impact on cross-border electricity flows and the respective cybersecurity costs incurred by the entities (see Section 2.4).

This guide proposes two alternative approaches to the definition of a cost item reference list for the purposes of such benchmarking analysis.

Section 2.6 of this guide provides general descriptions of different types of cybersecurity expenditures and how they could be taken into account for the CAPEX and OPEX calculations.

2.5.1.1. Cost item definition based on general ledger data and relation to assets involved in the provisional Union-wide high-impact and critical impact processes

The first approach to defining a reference list of cybersecurity cost items could be based on how the entities subject to the benchmarking analysis record cybersecurity expenditures in their general ledgers.

Nevertheless, bearing in mind the requirements of Article 13(2)(a) and Article 13(3)(a) of the NCCS, such cybersecurity cost items for collecting information based on general ledger data would need to pertain to implementing cybersecurity controls mitigating risks having an impact on electricity cross-border flows. In order to draw such a link during the definition of the cost items, where feasible, each cost item should relate to one or more 'supporting assets involved' in the provisional Union-wide high-impact and critical-impact processes, as defined in the provisional list developed by the ENTSO-E, in cooperation with the EU DSO entity, pursuant to Article 48(4) of the NCCS.

Such references should only be made where the cost item in question implements controls mitigating one or more cybersecurity risks to these assets.

Where linking a reference cost item to at least one of the supporting assets from the list of the provisional Union-wide high-impact and critical-impact processes is not feasible or appropriate, yet such a cost item relates to implementing a control or controls that mitigate risks having an impact on cross-border electricity flows, such a cost item could be placed in 'other' cost category.

This first approach would assume the ENTSO-E and the EU DSO entity defining the cost items upfront so that they are most aligned with how the entities record cybersecurity expenditures in their general ledgers.

2.5.1.2. Cost item definition based on assets involved in the provisional Union-wide high-impact and critical impact processes

The second approach, constituting an alternative to the first approach, would assess the costs and effectiveness of implementation of cybersecurity controls against each type of asset supporting the provisional Union-wide high-impact and critical-impact processes these controls protect, **as relevant to each benchmarked entity type**:

- '**supporting assets involved**' listed in the last row of each table describing the respective provisional Union-wide high-impact and critical-impact processes, also referred to as the 'primary assets' for the purposes of this guide; and
- '**generic supporting assets**' listed on page 6 of the provisional Union-wide high-impact and critical-impact processes document, which further break down to
    - telecommunications networks used for communication between control centres or with substations, field devices, or other remote locations;
    - the IT and OT infrastructure underlying the processes' primary applications, such as servers, databases, virtualisation platforms, and cloud platforms; and
    - systems used to maintain the process's primary IT and OT systems through all stages of the lifecycle, as further explained in that document.

For the purposes of the Article 13 NCCS benchmarking analysis, the costs of implementation of cybersecurity controls to protect these generic supporting assets could be apportioned in the following manner:

- if any given generic asset can be linked to one specific primary asset ('supporting asset involved' referred to above) supporting one or more Union-wide high-impact and critical-impact processes, then the costs of implementation of cybersecurity controls to protect this generic asset would be apportioned to the protection of that specific primary asset;
- all costs associated with generic supporting assets that cannot be apportioned in the manner described above would instead be apportioned to a single 'generic supporting assets' category.

Consequently, for each benchmarked entity, the costs and effectiveness of implementation of cybersecurity controls would be assessed asset-by-asset. This assessment would be carried out for each one of the supporting assets involved relevant for the benchmarked entity, such as the TSO substation automation systems, and finally for the single 'generic supporting assets' category, in accordance with the approach proposed above.

Whilst processes, products, services, systems and solutions may implement more than one cybersecurity control and protect more than one type of asset, in line with accounting principles, the costs of their implementation shall not be counted more than once. Therefore, when apportioning the costs across the various assets, the entities shall apportion any specific cost to only one of the supporting assets involved, or otherwise add it to the 'generic supporting assets' category.

In Annex 1, this guide offers a template to assist with such asset-based assessment (Table 1).

2.5.2. Price item reference list

Article 13(3)(b) of the NCCS refers to *'**prices** of cybersecurity services, systems and products that **contribute to a large extent** to the enhancement and maintenance of the cybersecurity risk-management measures'*. Furthermore, Article 13(3)(c) of the NCCS refers to 'solutions', which could be included in the aforementioned 'products'.

The wording of Article 13(3)(b) of the NCCS indicates that this reference list should be based on what can be found in the market of cybersecurity products and services. This is corroborated by the reference to 'prices' instead of 'costs' in that same article, which could be seen as a reference to market prices, excluding other costs related to acquisition, operation and maintenance and any adjustments based on accounting practices.

Consequently, the assessment required by Article 13(3)(b) of the NCCS could be based on market surveys.

However, without a common reference list of such 'price items', market surveys by NRAs will not lead to comparable prices. To that end, the ENTSO-E and the EU DSO entity could prepare a reference list of these price items based on how cybersecurity products and services that are subject to procurement could be categorised comparably within the different system operation regions. Indeed, Article 13(3)(b) of the NCCS requires that the assessment referred to in this provision is carried out *'in cooperation with the ENTSO for Electricity and the EU DSO entity'.*

Article 13(3)(b) of the NCCS also requires that these products and services contribute to the *'enhancement and maintenance of the cybersecurity risk-management measures'*. In order to draw such a link, to be eligible for inclusion in the reference list, every price item should implement one or more cybersecurity controls to protect either one or more (primary) 'supporting assets involved' or, alternatively, one or more 'generic supporting assets' outlined in Section 2.5.1.2.

Some hardware and software may have both cybersecurity-specific and additional network or system operation applications. The criterion of 'contributing to a large extent' encapsuled in Article 13(3)(b) of the NCCS is broader to include price items which may not be only aimed at implementing cybersecurity controls.

Such price items could thus include hardware and software used by the 'generic supporting assets', including the IT and OT systems and infrastructure. Examples of this could be firewalls which may also have network routing and additional connectivity functions, or automation tools, which to a large extent contribute to responding to cyber-attacks.

2.6. Apply general accounting concepts to the cost items

This section concerns the cost items described in Section 2.5.1.

In addition to defining the cost items upfront, general accounting concepts and approaches should be applied to these cost items consistently. This will contribute to reporting the costs by the entities in a consistent manner.

This section will, therefore, propose the application of general accounting concepts to the cost items described in Section 2.5.1, as well as the investments' time threshold applicable to the benchmarking analysis pursuant to Article 13 of the NCCS.

CAPEX and OPEX in the context of cybersecurity benchmarking

In the context of cybersecurity benchmarking under Article 13 of the NCCS:

- the costs that generate cybersecurity-specific assets, including cybersecurity-specific upgrades to existing assets defined in the provisional list of Union-wide high-impact and critical-impact process list, with a useful life longer than one fiscal year should constitute capital expenditure (CAPEX). They are annualised for accounting purposes;
- whereas the costs creating cybersecurity-specific assets with a useful life of up to one fiscal year, as well as the costs that do not create any assets but are instead related to the ongoing cybersecurity operations, should constitute operational expenditure (OPEX). Such costs are often recorded annually.

Taking into due account any partial years, the NRAs could subsequently add the average annualised CAPEX to the average annual OPEX over the time period agreed for the purposes of the benchmarking analysis.

For the purposes of the calculations, the entities should use individual useful life of each relevant cybersecurity asset.

The remainder of this section outlines what could be in scope of these two cost categories, as well as how certain accounting methods could be uniformly applied.

2.6.1. CAPEX

Cybersecurity hardware – these purchases with a useful life of more than one year should include hardware costs and associated installation fees. For calculating entity-wide costs for the purposes of Article 13(3)(a) of the NCCS, this should constitute the sum of all hardware and associated installation costs.

Cybersecurity software – software licensed or developed internally to have a useful life of more than one year. In cases of internal development, referred to as ‘customised software development’, salaries of development staff, including benefits, should be proportionately capitalised based on the number of hours worked on all stages of software development.

The same approach should be followed for outsourced development. If an entity has contracted a third-party to carry out development work on a specific piece of cybersecurity software, then the applicable CAPEX should be based on the contracted price of that software.

For calculating entity-wide costs for the purposes of Article 13(2)(b) and Article 13(3)(a) of the NCCS, this should constitute the sum of all software purchase and development costs.

Straight line CAPEX depreciation and amortisation

As noted above, CAPEX is annualised. This section outlines the key factors to take into account in carrying out this annualisation:

Depreciation – if a hardware cost is categorised as CAPEX, it should be depreciated over its useful life.

Depreciation represents the decrease in value of an asset over its lifespan and is commonly applied in accounting. While two most commonly used depreciation methods are ‘straight line’ and ‘accelerated’ depreciation, almost all NRAs apply the former approach in the context of electricity and

gas regulatory practices[14]. The straight line depreciation approach could therefore also be applied in the context of cybersecurity benchmarking pursuant to Article 13 of the NCCS.

For example, a hardware component which costs 10.000 EUR and has a useful life of 10 years would consequently amount to annual CAPEX of 1.000 EUR.

Furthermore, hardware upgrades should be taken into account when calculating their depreciation if they extend the asset life, increase its cost or alter its residual (salvage) value.

Amortisation – similarly, if software cost is categorised as CAPEX, it should be amortised over its useful life.

While there are several approaches to amortisation of intangible assets (in this case, primarily software), straight-line amortisation could be used as it is the most common and arguably the simplest method.

For example, a piece of software which costs 10.000 EUR and has a useful life of five years would consequently amount to annual amortised CAPEX of 2.000 EUR.

Similarly to how hardware upgrades may affect their depreciation calculations, software upgrades may influence their amortisation calculations if they extend the asset life, increase its cost or, much less commonly for software, alter its residual value.

The entities should appropriately deduct any residual asset value from the cost calculation.

2.6.2. OPEX

As discussed at the beginning of this section, OPEX is often recorded annually.

Cybersecurity OPEX can be categorised in four ways: hardware-related, software-related, staff salaries and contractor fees.

These categories are provided primarily for descriptive purposes. As such, they can overlap. For example, hardware maintenance by entity staff members would be categorised as both ‘cybersecurity hardware OPEX’ and ‘internal cybersecurity personnel OPEX’. However, the entities should not count the related costs more than once.

Cybersecurity hardware OPEX includes repairs, servicing and maintenance of existing cybersecurity hardware. Hardware OPEX may also include other operational costs, such as energy, to the extent that they can be appropriately attributed to specific cybersecurity hardware.

Cybersecurity software OPEX includes licences for up to one year, including any initial subscription fees, if applicable. This cost category may include potential support or maintenance fees.

Internal cybersecurity personnel OPEX includes salaries of cybersecurity personnel, as well as any benefits. If cybersecurity tasks constitute less than 100% of staff member’s time, because the staff member in question also has other non-cybersecurity-specific tasks, then a proportion of staff member’s salary should be appropriately attributed.

Cybersecurity contractor OPEX includes contractor fees for cybersecurity operations, such as vulnerability management, penetration testing, network threat detection or compliance management.

[14] Focusing on aspects such as calculation of a rate of return, determination of the regulatory asset base and depreciation of assets in the different regulatory systems.

However, it does not include contractor fees working on CAPEX projects, such as developing software with a useful life of more than one fiscal year.

2.7. Apply macroeconomic factors based on benchmarking requirements

NRAs should request the entities to apply macroeconomic factors following the requirements of the benchmarking analysis, on the one hand, and being mindful of any additional complexity they may involve, on the other hand.

In addition to converting all costs to EUR for the purposes of cross-country analysis recommended in Section 2.3.2, two other aspects are worth highlighting: inflation adjustments and inclusion of taxes.

2.7.1. Ensure a uniform inflation adjustment methodology

Inflation adjustments are particularly important when carrying out multi-year cost calculations. While in the present case the analysis could be limited to as few as three years (2022-2024), such a time period already warrants inflation adjustments, especially in light of the inflation figures registered during those years.

Firstly, for inflation-adjusted comparative benchmarking, the most commonly used base year tends to be the latest one. In the present case, this would be 2024.

Secondly, in the absence of a more suitable price index, general inflation in the form of the 'harmonised index of consumer prices' (the '**HCIP**') published by Eurostat for each Member State of the European Union[15] could be adopted for the purposes of the benchmarking analysis. It is a straightforward approach which has been applied in some existing benchmarking reports.

The NRAs could, nevertheless, agree on a more nuanced approach. One potential alternative for cybersecurity benchmarking could include selecting a subset of the 'services producer price index'[16] (for example, relating to computer programming and consultancy – information services) and identifying an appropriate index or indices reflecting hardware costs. While certain price indices have a more limited historical reach, this issue is less pertinent in the event of selecting the proposed benchmarking time period.

Thirdly, all costs incurred before the base year would now be adjusted to the base year separately for each cost item using the same agreed methodology:

- for CAPEX, this would mean taking the year when the expenditure was actually incurred (for example, based on the first general ledger entry – see Section 2.3.2) and adjusting it to the base year; and
- for OPEX, this would mean adjusting each relevant year to the base year. In other words, an OPEX item from year 2022 would need to include the inflation registered in years 2022-2024,

[15] https://ec.europa.eu/eurostat/databrowser/view/prc_hicp_aind/default/table?lang=en (hyperlink last verified on 10 June 2025).

[16] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Services_producer_price_index_overview#Information_and_communications (hyperlink last verified on 10 June 2025).

whereas an OPEX item from year 2023 would need to include the inflation registered in years 2023-2024.

2.7.2. Consider taxes

The issue of taxes is one of the aspects the NRAs should take into consideration in their assessment of the existence and level of comparability of costs of cybersecurity services, systems and solutions prescribed by Article 13(3)(c).

Taxes are factors extrinsic to the operations of the entities. That is to say, in general, they are factors beyond their control. Therefore, ordinarily, cost benchmarking analyses do not include taxes, whether direct or indirect, in order to increase the level of comparability. For example, with regards to the efficiency of spending. This is especially the case when the analysis involves multiple Member States.

Since Article 13(2) of the NCCS includes assessing whether current investments in cybersecurity are 'efficient', specifically in point (c) of this article, to the extent possible, the entities should exclude all taxes from the reported costs. Nevertheless, certain types of taxes, such as payroll taxes, may be unavoidable in the process of calculating the OPEX.

One aspect of the costing assessment which could potentially include taxes is Article 13(3)(a) of the NCCS, which refers to 'expenditure'. This term could be interpreted as including taxes so as to calculate the total amount an entity spent over a period of time, without normalising it in a manner akin to Article 13(2) of the NCCS.

2.8. Simplify the assessment of the effectiveness of investments

This principle constitutes an elaboration of the principle 'Limit the information requested and the level of complexity to what is required' discussed in Section 2.2, albeit in a non-costing context. The NRAs could apply this principle in benchmarking the aspects of cybersecurity investments referred to in Article 13(2) of the NCCS.

As noted in Section 2.2, when evaluating the effectiveness and efficiency of current cybersecurity investments in the context of Article 13(2) of the NCCS, including the risk mitigation they provide, the extent and level of detail of the information requested should be limited to what is required for the purposes of this benchmarking exercise.

This is especially the case since the benchmarking assessment required by Article 13(2) of the NCCS has several aspects, which means that it needs to be designed to fulfil the requirements encapsulated in these provisions, while keeping the workload manageable for the entities and the NRAs. Questions appropriate for benchmarking purposes thus need to be of a different character than those used in the context of operational performance evaluations, internal audits or cybersecurity management system implementation reviews.

For example, while quantitative performance indicators could furnish objective and empirical data on the effectiveness of cybersecurity investments, they may be too detailed for investment benchmarking purposes, and they may go beyond what most entities would be able to furnish within the timeframes of the benchmarking analysis foreseen by Article 13(2) of the NCCS.

Likewise, self-assessment questionnaires akin to 'cybersecurity maturity' self-evaluation tools[17] may be disproportionate for the benchmarking analysis pursuant to Article 13(2) of the NCCS. The

[17] Such as the Cybersecurity Capability Maturity Model (C2M2) provided by the United States Department of Energy to help with optimising cybersecurity investments (https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2),

assessment of the effectiveness of the function played by processes, products, services, systems and solutions used to implement cybersecurity controls referred to in Article 13(1) of the NCCS should be simpler.

Thus, while the key aspects of the assessment pursuant to Article 13(2) of the NCCS could yield several 'levels' to indicate the perceived performance of the processes, products, services, systems and solutions used to implement cybersecurity controls, the individual assessment criteria (questions) should not go into numbers or level seen in most existing cybersecurity evaluation methods and tools. Instead, these assessment criteria should be designed to accommodate inclusion of the following elements in the analysis:

- the cost items discussed in Section 2.5.1 of this guide;
- the costs of these items reported by the entities. For example, based on the approach proposed in Section 2.6 and Section 2.7; and
- the effectiveness criteria against which the cost items and their respective costs could be assessed within the timeline stipulated in Article 13(2) of the NCCS. These criteria are discussed in Section 2.9.

Regardless of the format adopted by the NRAs to fulfil the requirements of the benchmarking analysis in accordance with Article 13(2) and Article 13(3) of the NCCS, the overall recommendation for structuring the assessment criteria and the resulting assessment forms is simplicity. This approach is particularly desirable in light of a multi-faceted and time-bound exercise, such as the one at hand.

2.9. Evaluate the effectiveness of investments based on benchmarking objectives

Section 2.8 discussed the overall approach, structuring and the level of abstraction that could be adopted in the context of the benchmarking analysis prescribed by Article 13 of the NCCS. This section will discuss the assessment objectives stipulated by Article 13(2) of the NCCS, with some examples of how the NRAs could approach them.

Pursuant to Article 13(2) of the NCCS, the NRAs shall assess whether current investments in cybersecurity:

(a) mitigate risks having an impact on cross-border electricity flows;

(b) provide the desired results and engender efficiency gains for the development of electricity systems; and

(c) are efficient and integrated into the overall procurement of assets and services.

The assessment proposals for Article 13(2)(a) and (c) of the NCCS provided in this section rely on the approach to defining cost items based on the assets involved in the provisional Union-wide high-impact and critical impact processes discussed in Section 2.5.1.2 of this guide. This guide also refers to these proposals as the '**asset-based assessment**'.

ENISA's cybersecurity maturity self-assessment tool for small and medium-sized businesses (https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/), or ENISA's Computer Security Incident Response Teams Maturity Framework (https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework). Hyperlinks last verified on 10 June 2025.

Annex 1 of this guide includes a template (Table 1) to assist with gathering information from the entities to perform such an asset-based assessment. This template integrates all the proposals discussed in this section to fulfil the assessment objectives encapsulated in Article 13(2)(a) and (c) of the NCCS.

Should the reference cost items be instead defined in accordance with Section 2.5.1.1 of this guide, the NRAs would need to design an appropriate template to that end and carry out the assessment described in this section based on these cost items. In all cases, however, the link between the relevant cost items and the 'supporting assets' from the Union-wide high-impact and critical-impact processes document should be maintained so as to enable an asset-based assessment of risk mitigation pursuant to Article 13(2)(a) of the NCCS.

The assessment proposals for Article 13(2)(b) of the NCCS are independent of any approach to defining cost items, as they are based on evaluating the fulfilment of the objectives encapsulated in this article at entity-level. This guide also refers to these proposals as the '**entity-based assessment**'.

Annex 1 of this guide also includes a template (Table 2) to assist with gathering information from the entities to perform such an entity-based assessment. This template integrates all the proposals discussed in this section to fulfil the assessment objectives encapsulated in Article 13(2)(b) of the NCCS.

2.9.1. Mitigating risks having an impact on cross-border electricity flows

Under the NCCS, a fundamental purpose of cybersecurity investments is to mitigate risks having an impact on cross-border electricity flows. Specifically, risks to the assets involved in the provisional Union-wide high-impact and critical impact processes.

Although Article 13(2)(a) of the NCCS does not require the NRAs to assess the **extent** to which current investments in cybersecurity mitigate risks having an impact on cross-border electricity flows, but rather **whether** they do so, each cost item identified by an entity in accordance with Section 2.5.1 of this guide could nevertheless be assessed through at least a semi-quantitative question or questions with several possible answers. As discussed in Section 2.8 of this guide, this could result in several risk mitigation levels reportedly achieved by the cost item in question, which would enrich any subsequent comparative analysis.

Considering that such a question or questions would be applicable to each cost item relevant to the entity, such as each asset type supporting the provisional Union-wide high-impact or critical-impact processes carried out by that entity, this question or questions should be phrased appropriately to ensure their general relevance and to keep the workload manageable. For example:

What is the percentage of residual cybersecurity risks within your risk tolerance levels?			
>85%	>50%	>25%	<=25%

'Residual risk' is the risk that remains after risk mitigation[18], whereas 'Risk tolerance' is an entity's readiness to bear the residual risk[19]. While the specific level of risk tolerance is dependent on each

[18] Or 'risk treatment', using the terminology of the ISO/IEC 27000:2018, cl. 3.72.

[19] ISO 31073:2022, cl. 3.3.28.

entity's context[20], the residual risk should not exceed an entity's risk tolerance level. If it does, the entity's existing cybersecurity controls, and the processes, products, services, systems or solutions used to implement them, are not operating effectively enough to manage the identified risk[21].

Thus, in addition to fulfilling the criteria discussed in the prior sections of this guide, the question above would:

- reflect a key criterion of risk management;
- be applicable to any type of asset and any type of entity;
- produce meaningful results notwithstanding any differences in the entities' context; and
- produce comparable results that could also be used as an input to the benchmarking analysis stipulated in Article 13(2)(c) of the NCCS and discussed in Section 2.9.3 of this guide.

2.9.2. Providing the desired results and engendering efficiency gains for the development of the electricity systems

Assessing whether current investments in cybersecurity *'provide the desired results and engender efficiency gains for the development of the electricity systems'*, as stipulated by Article 13(2)(b) of the NCCS, leaves the NRAs a degree of interpretative freedom. The NRAs could approach this aspect of the benchmarking analysis is by:

- identifying, at an appropriate level of abstraction, the 'desired results' that investments in cybersecurity could provide;
- relating these results to the development of the electricity systems; and
- evaluating efficiency gains engendered by cybersecurity investments.

This section discusses each of these three elements of the Article 13(2)(b) assessment and how they could be integrated. Table 2 in Annex 1 of this guide provides an illustrative demonstration of how such a combined assessment could be presented in a tabular format.

2.9.2.1. Providing the 'desired results'

As discussed in Section 2.9.1, a fundamental purpose of cybersecurity investments under the NCCS is to mitigate risks having an impact on cross-border electricity flows. This fundamental purpose of cybersecurity investments could also be reflected in the assessment of the 'desired results' referred to in Article 13(2)(b). In this case, however, instead of carrying out this assessment individually for each asset type, it could be carried out at an entity level. Thus, similarly to the assessment carried out in the context of Article 13(2)(a) of the NCCS (Section 2.9.1), the NRAs could enquire about the percentage of residual cybersecurity risks within each entity's risk tolerance levels.

The NRAs could also identify certain more specific indicators of the achievement of the 'desired results' of cybersecurity investments. Similarly to the degree of risk mitigation, such indicators should reflect key outcomes that investments in cybersecurity could bring.

[20] Internal or external environment in which the entity operates. For example, entity's internal context includes its policies, corporate objectives, ICT and OT systems in place, information flows, and contractual relationships.

[21] See for example, ISO/IEC 27005:2022, cl. 8.3 on determining all controls that are necessary to implement the information security risk treatment options, guidance preceding 'example 1'.

One such outcome could be the existence of cybersecurity operation centre capabilities referred to in Article 38(1)(a) of the NCCS, which is a key risk management measure each high-impact and critical impact entity will need to implement under the NCCS. Analogously to Article 38(1)(b) of the NCCS, this criterion should be considered fulfilled if the benchmarked entity procures all or parts of these capabilities through managed security service providers ('**MSSPs**').

Another outcome that the NRAs could view as a reflection of desired results of cybersecurity investments could be a successful completion of either a security audit or an inspection carried out by either a qualified party independent from the entity inspected or audited, or by the competent authority designated or established pursuant to Article 8(1) of the NIS 2 Directive ('**CS-NCA**').

Table 2 in Annex 1 of this guide includes these three elements in columns J, K and L.

2.9.2.2. Representation of the development of the electricity systems

The development of the electricity systems referred to in the latter part of Article 13(2)(b) of the NCCS could be represented as a specific simplified metric for the purposes of this benchmarking analysis and linked to the assessment of the desired results discussed in Section 2.9.2.1. Such a linkage could include an element of relativity or otherwise normalisation of cybersecurity costs (discussed in Section 2.9.2.3 below) and the desired results, on the one hand, and the scale of each entity's electricity systems developed and operated while supported by investments in cybersecurity, on the other hand.

In this context, while it may be challenging to gauge the development of electricity systems by reference to the amount of hardware making up these systems and networks, one could employ appropriate metrics that could serve as a representation of their size, simplified for the NCCS benchmarking context. Such a metric could be, for example, the amount of power controlled by the key business processes, measured in megawatts (MW).

As noted in Section 2.4 of this guide, by the time this benchmarking analysis commences, the competent authorities will have identified candidates for high-impact and critical-impact entities in their Member State pursuant to Article 48(3) of the NCCS. To that end, pursuant to Article 48(2) of the NCCS, the ENTSO-E and the EU DSO entity have developed a recommended provisional electricity cybersecurity impact index ('**ECII**')[22].

For each entity type, Table 1 of the ECII contains metrics related to the key business process or processes of that entity. These metrics reflect the amount of power these processes control. For example, for the DSOs, it is the maximum DSO load over the previous year.

The NRAs could thus request that the entities report the ECII values that determined their provisional identification in the context of Article 48(3) of the NCCS, as well as the values from the years 2022 and 2023. Such values could be used as a simplified indicator of the development of electricity systems in the context of the benchmarking analysis pursuant to Article 13(2)(b) of the NCCS.

Table 2 in Annex 1 of this guide includes this element in column I.

2.9.2.3. Evaluating efficiency gains engendered by cybersecurity investments

'Efficiency' is ordinarily understood as achieving one or more set objectives in the shortest time or with the least expenditure. In the context of the analysis prescribed by Article 13(2)(b) of the NCCS, the NRAs could focus on the latter element: comparing the degree to which current investments in cybersecurity provide the desired results for the development of the electricity systems with the

[22] https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Network%20codes%20documents/NCCS/Provisional%20ECII.pdf (hyperlink last verified on 10 June 2025).

expenditure of implementing cybersecurity controls reported by the entities based on the methodologies proposed in Section 2.6 and Section 2.7.

In the context of the Article 13(2)(b) analysis, the same entity-wide expenditure as the one reported in the context of Article 13(3)(a) should be used. This single figure would be derived from adding the reported cybersecurity CAPEX to the reported cybersecurity OPEX, as seen in Annex 1, Table 2, columns M and N.

Beyond assessing whether cybersecurity investments *'engender efficiency gains for the development of the electricity systems'*, as stipulated in Article 13(2)(b) of the NCCS, NRAs could assess the extent to which they do so by combining the values in a single equation. For example, by way of multiplying the ECII value (see Section 2.9.2.2) by values appropriately representing the desired results, and dividing the result of this multiplication by the total cybersecurity expenditure.

The explanation accompanying Table 2 in Annex 1 provides an illustrative example of such an equation.

Historical values for the years 2022 and 2023 could be used as comparative periods for both the ECII and the total expenditure to see whether and to what extent efficiency **gains** for the development of the electricity systems are indeed being engendered.

Without an appropriate categorisation, the outcome of the abovementioned calculation, further explained in Annex 1, can only be used to track the evolution of each entity's individual performance over the years with regards to engendering efficiency gains for the development of the electricity systems.

In order to compare the results of the Article 13(2)(b) analysis between the entities of the same type, at a minimum, such entities would need be categorised based on their ECII and total cybersecurity expenditure.

2.9.3. Efficiency of investments in cybersecurity

Similarly to Section 2.9.2.3 above, NRAs could also interpret the term 'efficiency' in the context of the analysis prescribed by Article 13(2)(c) of the NCCS as achieving set objectives with the least costs of cybersecurity investments reported by the entities based on the methodologies proposed in Section 2.6 and Section 2.7. In this case, however, the assessment could be carried out at the level of each asset type, comparing the outcome of the risk mitigation assessment described in Section 2.9.1 with the total expenditure recorded for each asset type.

To this end, the NRAs could evaluate the ratio between

- the output of the Article 13(2)(a) assessment proposed in Section 2.9.1 of this guide. Namely, the effectiveness of mitigating risks having an impact on cross-border electricity flows recorded in column C of Table 1 proposed in Annex 1 of this guide. This output should be multiplied by the relevant ECII value to reflect the increased risk impact; and
- the average of the total annual implementation costs (CAPEX and OPEX) for the years 2022-2024, whereas such total costs would be established by aggregating the values in columns E and F of Table 1 proposed in Annex 1 of this guide.

The NRAs could compare these asset type-specific values among the entities of the same type and with similar ECII and cybersecurity expenditure values, following the logic discussed in Section 2.9.2.3.

Furthermore, should the NRAs repeat this assessment in the future, the ratios evaluated in this manner could be tracked over the years, to examine inflation-adjusted fluctuations in the efficiency of investments in cybersecurity with respect to each asset type.

2.9.4. Integrating investments in cybersecurity into the overall procurement of assets and services

The second part of the Article 13(2)(c) NCCS benchmarking analysis should aim at assessing the extent to which cybersecurity is taken into account in the development and implementation of procurement policies. In other words, when procurement policies are created and agreed within the entity and when the entity carries out any procurement-related activities.

An approach similar to that proposed in Section 2.9.1 of this guide, relating to the Article 13(2)(a) assessment, could also be followed here. Namely, given that the selected question or questions would be applicable to each asset type relevant to an entity, they should be phrased appropriately to ensure their general relevance and to keep the workload manageable. For example:

To what degree are cybersecurity investments integrated into the overall procurement of assets and services?			
>85%	>50%	>25%	<=25%

Such a general question should be accompanied by appropriate guidance on how to assess the degree of integration of cybersecurity investments into the overall procurement of assets and services. This guidance should be based on predefined objectives or criteria that would apply uniformly to all relevant assets and entities, so as to render the assessment results comparable.

In this regard, Recital 21 of the NCCS provides that its provisions *'should ensure that the relevant security objectives in Article 51 of Regulation (EU) 2019/881* [the Cybersecurity Act] *are met by the ICT products, ICT services and ICT processes to be procured'.*

Article 51 of the Cybersecurity Act establishes the following security objectives of European cybersecurity certification schemes, which could also be referred to in the context of the assessment discussed in this section:

(a) 'to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;

(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;

(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;

(d) to identify and document known dependencies and vulnerabilities;

(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;

(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;

(i) that ICT products, ICT services and ICT processes are secure by default and by design;

(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates'.

When carrying out the assessment discussed in this section, procurement of critical ICT services should be given particular emphasis. Providers of these services are defined in Article 3(9) of the NCCS, with the following examples provided on p. 6 of the document listing the provisional Union-wide high-impact and critical-impact processes:

- suppliers of SCADA systems;
- parties with remote access to high- or critical-impact assets;
- hosting providers or cloud providers hosting high-impact or critical-impact applications; and
- software as a service providers for high-impact or critical-impact applications.

2.10. Explore different angles of comparability of costs and functions

This final principle, dedicated to Article 13(3)(c) of the NCCS, offers advice with regards to the assessment of the existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of the NCCS.

2.10.1. Establish basic comparability as a common assessment reference

In terms of fostering the assessment of comparability of costs, this guide recommends adopting a uniform approach to:

- applying elementary accounting methodologies to the cost items, such as depreciation and amortisation (Section 2.6);
- the costing period (Section 2.3.1);
- inflation adjustment (Section 2.7.1);
- taxes (Section 2.7.2); and
- currency, including applying the same conversion method (Section 2.3.2).

Section 2.7 omits certain macroeconomic cost factors whose application may not be suitable or proportionate given the specific objectives encapsulated in Article 13(2) and Article 13(3) of the NCCS. Nevertheless, the NRAs may choose to take them into account if they wish to compare the expenditures between the Member States, such as those calculated pursuant to Article 13(3)(a) of the NCCS, and analyse further macroeconomic factors influencing these expenditures. An example of this are median wages in the Member States.

On the other hand, the recommendations for defining the reference cost items in accordance with Section 2.5.1 serve to create a common basis for the assessment of costs and effectiveness of cybersecurity investments in accordance with Article 13(2) and Article 13(3)(a) of the NCCS. The extent to which these recommendations foster the assessment of comparability of functions of cybersecurity services, systems and solutions, however, is much more limited. For example, the cost item reference list approach proposed in Section 2.5.1.2 would only indicate the assets protected by

cybersecurity services, systems and solutions. It would not provide further information or categorisation of the cybersecurity services, systems and solutions in question.

Similarly, defining a reference list of cybersecurity cost items based on the relevant general ledger data of the entities, as discussed in Section 2.5.1.1 of this guide, would align this reference list with existing accounting practices of the entities, but not with specific functions of such cybersecurity services, systems and solutions.

As a result, relying on such lists alone would not be sufficient for establishing comparability of functions.

2.10.2. Enhance the assessment of comparability of functions

To address the requirement encapsulated in Article 13(3)(c) of the NCCS, the NRAs need to introduce a further assessment, specifically from the angle of function. This section proposes three criteria to that end.

2.10.2.1. Implementation of cybersecurity controls

Since Article 13(3)(c) of the NCCS refers to *'cybersecurity services, systems and solutions suitable for the implementation of this Regulation'*, and Article 13(1) of the NCCS refers to *'benchmarking of the implemented cybersecurity controls (…), taking into consideration (…) the effectiveness of the function played by processes, products, services, systems and solutions used to implement such controls',* the NRAs could commence the functional assessment by identifying cybersecurity controls 'suitable' for the implementation of the NCCS. In other words, suitability of processes, products, services, systems and solutions to implement cybersecurity controls could constitute the starting point for establishing comparability of functions within the meaning of Article 13(3)(c) of the NCCS.

However, the legally-binding cybersecurity controls under the NCCS, referred to as the 'minimum and advanced cybersecurity controls'[23], will not be adopted in time for the benchmarking analysis. Therefore, the NRAs may instead need to refer to cybersecurity controls and respective services, systems and solutions implementing these controls that **could** be suitable for the implementation of the NCCS.

Pursuant to Article 48(7)(b) of the NCCS, the provisional list of European and international standards and controls the ENTSO-E and the EU DSO entity are to adopt by 13 June 2025[24] shall include *'cybersecurity controls equivalent to the controls that are expected to be part of the* [abovementioned] *minimum and advanced cybersecurity controls'*.

Therefore, the NRAs could refer to this provisional list of cybersecurity controls as an initial broad indicator of functions. Consequently, implementation of the same controls from this list could be considered an initial general indicator of comparability of functions of cybersecurity services, systems and solutions.

2.10.2.2. Types of technologies and activities that mitigate cybersecurity risks

While suitability of processes, products, services, systems and solutions to implement cybersecurity controls could constitute the starting point for establishing comparability of functions within the

[23] Developed pursuant to Article 29 of the NCCS.

[24] Provisional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows prepared pursuant to Article 48(6) of the NCCS, taking into account the information provided by the competent authorities pursuant to Article 48(5) of the NCCS.

meaning of Article 13(3)(c) of the NCCS, in order to facilitate identification of possible measures necessary to foster efficiency in spending, particularly where cybersecurity technological investments may be needed, NRAs could take further steps, such as the ones described in this and the following section.

In taking these further steps, the NRAs should cooperate with the CS-NCAs and the computer security incident response teams designated or established pursuant to Article 10(1) of the NIS 2 Directive. To that end, taking into consideration Article 5 of the NCCS, the NRAs shall first request the competent authorities for assistance.

As discussed in Section 2.9.1 of this guide, a fundamental goal of cybersecurity investments is to mitigate cybersecurity risks. Thus, an example of a resource that could be considered for more specific comparisons of functions of cybersecurity services, systems and solutions is the publicly-available MITRE ATT&CK® knowledge base[25]. Specifically, its lists of enterprise[26] and industrial control system ('**ICS**') mitigations[27].

These lists contain types of technologies[28] and activities[29], the latter of which could be provided as a service, and both of which are used to mitigate cybersecurity risks. The NRAs could thus further categorise cybersecurity services, systems and solutions in accordance with these different technologies and activities.

Fragment of the MITRE ATT&CK® ICS Mitigations presented for illustrative purposes:

Figure 1: Extract from the MITRE ATT&CK® ICS Mitigations

ID	Name	Description
M0801	Access Management	Access Management technologies can be used to enforce authorization polices and decisions, especially when existing field devices do not provided sufficient capabilities to support user identification and authentication. These technologies typically utilize an in-line network device or gateway system to prevent access to unauthenticated users, while also integrating with an authentication service to first verify user credentials.
M0936	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M0915	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use security identifier (SID) Filtering, etc.
M0949	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software. Within industrial control environments, antivirus/antimalware installations should be limited to assets that are not involved in critical or real-time operations. To minimize the impact to system availability, all products should first be validated within a representative test environment before deployment to production systems.
M0913	Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.
M0948	Application Isolation and Sandboxing	Restrict the execution of code to a virtual environment on or in-transit to an endpoint system.
M0947	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Perform periodic integrity checks of the device to validate the correctness of the firmware, software, programs, and configurations. Integrity checks, which typically include cryptographic hashes or digital signatures, should be compared to those obtained at known valid states, especially after events like device reboots, program downloads, or program restarts.

[25] https://attack.mitre.org/ (hyperlink last verified on 10 June 2025).

[26] https://attack.mitre.org/mitigations/enterprise/ (hyperlink last verified on 10 June 2025).

[27] https://attack.mitre.org/mitigations/ics/ (hyperlink last verified on 10 June 2025).

[28] Such as antimalware or account management.

[29] Such as technical audit or user training.

The technologies and activities listed in the 'Name' column in Figure 1 are further described by referring to specific cyber-attack techniques or vectors[30] they address, provided in column 'Name' in Figure 2 presented below, as well as descriptions of how these cybersecurity technologies and activities can address these techniques, provided in column 'Use':

Figure 2: Extract from the MITRE ATT&CK® Enterprise Mitigations – Antivirus/Antimalware

Domain	ID	Name	Use
Enterprise	T1027	Obfuscated Files or Information	Anti-virus can be used to automatically detect and quarantine suspicious files. Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10+ to analyze commands after being processed/interpreted. [4]
	.002	Software Packing	Employ heuristic-based malware detection. Ensure updated virus definitions and create custom signatures for observed malware.
	.009	Embedded Payloads	Anti-virus can be used to automatically detect and quarantine suspicious files.
	.010	Command Obfuscation	Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10+ to analyze commands after being processed/interpreted.
	.012	LNK Icon Smuggling	Use signatures or heuristics to detect malicious LNK and subsequently downloaded files.
	.013	Encrypted/Encoded File	Anti-virus can be used to automatically detect and quarantine suspicious files, including those with high entropy measurements or with otherwise potentially malicious signs of obfuscation.
	.014	Polymorphic Code	Anti-virus can be used to automatically detect and quarantine suspicious files. Employment of advanced anti-malware techniques that make use of technologies like machine learning and behavior-based mechanisms to conduct signature-less malware detection will also be more effective than traditional indicator-based detection methods.
Enterprise	T1566	Phishing	Anti-virus can automatically quarantine suspicious files.
	.001	Spearphishing Attachment	Anti-virus can also automatically quarantine suspicious files.
	.003	Spearphishing via Service	Anti-virus can also automatically quarantine suspicious files.

The NRAs could consult these descriptions to understand the functions of various cybersecurity services, systems and solutions in more detail. Consequently, this would allow the NRAs to assess the existence and level of comparability of these services, systems and solutions in more detail than at cybersecurity control implementation-level.

2.10.2.3. Degree of assurance

Finally, notwithstanding addressing similar threats or vulnerabilities, or providing similar mitigations, cybersecurity services, systems and solutions can provide a different degree of assurance to an entity. In this context, 'assurance' could be understood in two ways.

Firstly, it could be understood as the existence of objective evidence pointing to the quality of the service, system or solution in question.

For example, many cybersecurity services, systems and solutions, such as chips and smartcards, can be certified by accredited bodies against European and international standards. Furthermore, they can be subject to independent standard-based third-party audits and conformity assessments. Lastly, systems, solutions and parts thereof can bear declarations of conformity from their manufacturers.

Secondly, a system or solution could conform to the requirements of a specific standard and could thus be certified against it, but the standard itself could recognise more than one 'assurance level'. This is the case with the existing national Common Criteria-based cybersecurity certification schemes[31] which envisage seven 'Evaluation Assurance Levels'.

[30] Such as abusing commands and scripts in programming languages. For example, in Python.

[31] Common Criteria is an international standard for information security evaluation published, for instance, as the ISO/IEC 15408 for information security, cybersecurity and privacy protection — evaluation criteria for IT security.

Though the EU Common Criteria certification scheme (the '**EUCC**') for cybersecurity systems pursuant to Commission Regulation 2024/482 of 31 January 2024[32] has only been in application since 27 February 2025, for completeness, ACER notes that it also allows identifying *'ICT products that have specific and similar security functionality that mitigates attacks where the characteristics are common to a given assurance level'*[33]. The EUCC provides for certificates at two assurance levels: 'substantial' or 'high'.

Thus, in addition to categorising cybersecurity services, systems and solutions for comparative purposes based on the mitigation types provided, NRAs could also consider whether they have been certified pursuant to the relevant certification schemes, as well as any assurance level offered by the product in question.

[32] Commission Implementing Regulation 2024/482 of 31 January 2024 laying down rules for the application of Regulation 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (OJ L, 2024/482, 7.2.2024).

[33] Recital 4, first sentence.

Annex 1: Benchmarking assessment templates

Table 1: Asset-based assessment

A	B	C				D				E			F		
Asset type supporting provisional Union-wide process(es)	**Provisional Union-wide process(es) supported by these assets** Art 48(4) NCCS	**Residual cybersecurity risks to the asset within tolerance levels** by end of 2024 For Art 13(2)(a) and (c) NCCS				**Integrating cybersecurity investments into overall procurement of assets and services** by end of 2024 For Art 13(2)(c) NCCS				**Cybersecurity CAPEX per asset (EUR)** For Art 13(2)(c) NCCS			**Cybersecurity OPEX per asset (EUR)** For Art 13(2)(c) NCCS		
		>85%	>50%	>25%	<=25%	>85%	>50%	>25%	<=25%	2022	2023	2024	2022	2023	2024
Asset 1	*Process 1, Process 2*														
Asset 2	*Process 3*														
…															

The primary function of Table 1 is facilitation of the assessment referred to in Article 13(2)(a) and Article 13(2)(c) of the NCCS

In each of the columns C-F, references are made to the relevant provisions of the NCCS under assessment. For example, the assessment proposed in column C could be used '*For Art 13(2)(a) and (c) NCCS*', meaning that this assessment would be relevant to the assessment referred to in Article 13(2)(a) and (c) of the NCCS.

Certain assessments referred to in Article 13(2) of the NCCS could require more than one input, which implies more than one prior assessment. For example, the assessment of 'efficiency' referred to in Article 13(2)(c) of the NCCS could require a prior assessment of risk mitigation pursuant to Article 13(2)(a) of the NCCS, as proposed in column C, and the assessment of costs proposed in columns E and F.

For clarity, Article 13(2)(c) of the NCCS is also referred to in column D, as it includes the assessment of integrating cybersecurity investments into overall procurement of assets and services.

Table 2: Entity-based assessment

G	H	I			J				K		L		M			N		
Entity From Art 3(1), Table 1 of Provisional ECII doc	**Provisional Union-wide process(es) of the entity** Art 48(4) NCCS	**ECII MW value per entity Art 3(1), Table 1 of Provisional ECII doc** For Art 13(2)(b) NCCS			**Residual cybersecurity risks within tolerance levels entity-wide** by end of 2024 For Art 13(2)(b) NCCS				**Audited or inspected cybersecurity management system in 2024** For Art 13(2)(b) NCCS		**CSOC capabilities** by end of 2024 For Art 13(2)(b) NCCS		**Cybersecurity CAPEX (EUR)** For Art 13(2)(b) NCCS and Art 13(3)(a) NCCS			**Cybersecurity OPEX (EUR)** For Art 13(2)(b) NCCS and Art 13(3)(a) NCCS		
		2022	2023	2024	>85%	>50%	>25%	<=25%	Yes	No	Yes	No	2022	2023	2024	2022	2023	2024
Entity name	*Process*																	

The primary function of Table 2 is facilitation of the assessment referred to in Article 13(2)(b) and Article 13(3)(a) of the NCCS

This approach complements the asset-based assessment proposed in Table 1 of this annex by evaluating the costs and effectiveness of implementation of cybersecurity controls for each benchmarked entity (**column G** in Table 2). In other words, this assessment would be carried out at entity-level.

Columns M and N could facilitate the assessment referred to in Article 13(3)(a) of the NCCS by way of establishing total annual expenditures of each entity resulting from the aggregation of the CAPEX and OPEX values encapsulated in these two columns. The average expenditure could thus be calculated for each type of benchmarked entity.

Columns I-N could facilitate the assessment referred to in Article 13(2)(b) of the NCCS, using the average value of the years 2022-2024, in the following manner:

Column J: While reducing cybersecurity risks to individual assets so that the residual risks are within risk tolerance levels could be employed in the context of the assessment referred to in Article 13(2)(a) of the NCCS, as discussed in Section 2.9.2.1 of this guide, a similar entity-wide assessment could be used to gauge whether cybersecurity investments provide the 'desired results' in the context of Article 13(2)(b) of the NCCS.

Assessing whether cybersecurity investments *'engender efficiency gains for the development of the electricity systems'*, as further required by Article 13(2)(b) of the NCCS, could involve the following inputs:

Column I would provide the entity's average ECII value of the years 2022-2024, which would offer a simplified representation of the development of the electricity systems that could be used specifically for the purposes of this benchmarking analysis. This value could be based on the methodology recommended in the provisional ECII document developed by the ENTSO-E in cooperation with the EU DSO entity.

Column K refers to either a security audit or an inspection carried out in 2024 by a qualified party independent from the entity inspected or audited, or by the CS-NCA.

Column L refers to the CSOC capabilities described in Article 38(1)(a) of the NCCS. In line with Article 38(1)(b) of the NCCS, this criterion would be fulfilled if the entity procured all or parts of these capabilities through MSSPs.

Beyond assessing **whether** cybersecurity investments *'engender efficiency gains for the development of the electricity systems'*, as required by Article 13(2)(b) of the NCCS, NRAs could assess the **extent** to which they do so by combining the values gathered in columns I-N in a single equation, such as the following, provided to illustrate this concept:

$(I*(J*K*L)/(M+N))*1000$, whereas

Column J could, for example, provide any of the following four values: 0.85, 0.5, 0.25 or 0.125. Value 0.125 would be selected if column J yields a response '<=25%'.

Columns K and L could each provide an increased coefficient, such as 1.2, if the answers in their respective columns are 'yes'. Otherwise, either one of them, or both, could be removed from the equation altogether.

The total cost represented by columns M+N could be calculated as an average value of the years 2022-2024.

Thus, a hypothetical entity with the following characteristics:

Column	Value
I	1200 MW
J	0.85%
K	No
L	1.2
M+N	1900000 EUR

would yield the following result rounded to three decimal places: (1200*(0.85*1.2)/1900000)*1000 = 0.644.

Based on the premise that achieving the same results with lower spending translates to higher efficiency, the same hypothetical entity spending 1500000 EUR would yield a higher result of 0.816.

Similarly, if such a hypothetical entity increased its ECII value, such as capacity, to 1300 MW, whilst maintaining cybersecurity expenditure at the original level, this could be said to constitute greater efficiency gains for the development of the electricity systems of 0.751 (rounded), compared to the original result of 0.644.

The purpose of the approach and example presented above is solely to demonstrate a possibility of expressing the output of assessments consisting of several components, such as the one referred to in Article 13(2)(b) of the NCCS, in a single figure.

Such an approach could be used to track the evolution of any specific entity's performance in the context of Article 13(2)(b). For example, by tracking changes in the ECII and cybersecurity expenditures over the 2022-2024 period.

Due to the differences in cost structures between the entities, normalising factors would need to be introduced to foster comparability of the assessment results. In order to compare the results of the Article 13(2)(b) analysis between the entities of the same type, at a minimum, such entities would need be categorised based on their ECII and total cybersecurity expenditure.

Annex 2: Lists of figures and tables

List of figures

List of tables