Consultation Questionnaire on the Draft Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

> Fields marked with * are mandatory.

General introduction

The purpose of the non-binding Framework Guideline (FG) is to set high-level principles that should be further elaborated in the Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows.

The role of the FG and of the following network code, is to supplement and further specialise existing cybersecurity and risk preparedness directives and regulations, introducing viable solutions to identified cybersecurity gaps and risks.

The objective of the network code, based on the draft FG principle, should be to solve, mitigate and prevent the potential high impact or materialization of cybersecurity risks, as well as to prevent those cybersecurity attacks or incidents that may impact real time operations (causing cascade effects).

ACER invites all concerned stakeholders to contribute to the public consultation, and therefore to define and shape the final Framework Guideline.

Next steps:

- ACER will analyse the responses received in July 2021 and will deliver a final version of the FG to the European Commission.
- In July 2021, ACER will publish a summary of the consultation, including an evaluation of the responses.
- ACER will publish all responses received and the identity of their respective stakeholders (unless stated otherwise). For this reason, please indicate if your response may be publicly disclosed or not, and if you agree with the data protection policy.

All concerned stakeholders are invited to respond to the public consultation on the proposed Framework Guideline.

The public consultation will run between 30 April 2021 to 29 June 2021 at 23:59 Ljubljana Time.

ACER will only accept responses in electronic format, no other format will be accepted. **In case of technical problems with the submission of your responses please contact DFG-NC-CS@acer.europa.eu.**

ACER will organise a workshop to introduce and explain the content of the proposed Framework Guideline, in May 2021. More information will be circulated via ACER Infoflash closer to the date of the event.

*First Name

███████

* Last Name

███████

* Company/Institution

Europex

* Type of business

Energy exchange association

Address

* Contact email

███████████████

Phone

Country

BE - Belgium

I confirm that I have read the [data protection notice in this link and accepted](#).

◉ Yes
○ No

I authorise the disclosure of my identity together with my response

◉ Yes
○ No (I want my response being completely anonymous)

1. Meeting the general objectives

Question 1 - Does the Framework Guideline contribute to the following objectives?

	Yes	No
To further protect cross-border electricity flows, in particular critical processes, assets and operations from current and future cyber threats?	○	◉

To promote a culture that aims to continuously improve the cybersecurity maturity and not to simply comply with the minimum level	◉	○
To mitigate the impact of cyber incidents or attacks or to promote preparedness and resilience in case of cyber incidents or attacks?	○	◉
To support the functioning of the European society and economy in a crisis situation caused by a cyber-incident or attack, with the potential of cascading effects?	○	◉
To create and promote trust, transparency and coordination in the supply chain of systems and services used in the critical operations, processes and functions of the electricity sector?	○	◉

Please, provide a short explanation justifying your assessment, if needed:

600 character(s) maximum

> Although the Framework Guideline (FG) might have a more specific objective, we fail to see the value added by the proposed requirements to the existing regulatory frameworks of the NIS Directive and its implementation acts as well as the proposed NIS 2 Directive. We therefore believe a stock-taking exercise of the latter is very much needed to ensure the FG is complementing rather than duplicating. If not, duplicative regulatory requirements will take away resources needed to deal with possible threats.

Question 2 - Do you see any gaps concerning the cybersecurity of cross-border electricity flows which the draft FG proposal should address?

- ◉ Yes
- ○ No

If yes, provide details

600 character(s) maximum

> At this stage we are very concerned about a duplication of requirements (see Q1). However, we would also like to raise the importance of ensuring a certain level of secrecy of information. The final network code should, for example, refrain from publishing lists of essential and important services mentioned under point 1.5 of the FG. Published databases, registries and similar documents can pose a risk to the overall security, as attackers would be able to easily detect weak links.

2. Scope, applicability and exemptions.

Question 3 - The draft FG suggests that the Network Code shall apply to public and private electricity undertakings including suppliers, DSOs, TSOs, producers, nominated electricity market operators, electricity market participants (aggregators, demand response and energy storage services), ENTSO-E, EU-DSO, ACER, Regional Coordination Centres and essential service suppliers (as defined in the FG). Does the FG applicability cover all entities that may have an impact on cross-border electricity flows, as a consequence of a cybersecurity incident/attack?

- ○ Yes
- ◉ No

Please, explain who is missing and why

600 character(s) maximum

> We recommend limiting the applicability for NEMOs to where it directly concerns cross-border electricity flows. Our understanding is that trading venues & clearing houses are not defined as essential service providers (please note these entities have extensive coverage via financial regulatory oversight).
>
> To avoid substantial overlap with the upcoming NIS 2 Directive we believe the FG should either
> a) Exclude entities which will be covered by NIS 2, or
> b) Allow for partial overlap regarding entities covered, but not duplicating requirements covered by existing frameworks (less preferable)

3. Classifications of applicable entities and transitional measures

Question 4 - The proposed FG prescribes a process to differentiate electricity undertakings based on their level of criticality/risk, and setting different obligations depending on their criticality/risk level. This will imply a transition period until the full system is established and will require the establishment of a proper governance to duly manage the entire risk assessment process. Do you think that the proposed transition is the most appropriate?

- ○ Yes
- ⦿ No

Would you suggest another transition approach and why?

600 character(s) maximum

> We believe a transitional phase is not needed as the NIS 2 Directive will soon be implemented. A transition assessment by the institutions named under 1.6 of the FG bears a risk of arbitrariness as the methodology is not comprehensively developed. As a result, entities might be considered essential within this transition period and incur unnecessary costs to comply, but ultimately be deemed non-essential in the established methodology. As the adoption of such FG takes time - for both law maker and law subject – sufficient time should be given for the transition. Please also see Q1 and Q3.

Question 5 – The FG proposes that all small and micro-businesses, with the exception of those that, despite their size, are defined as important/essential electricity undertakings, shall be exempted from the obligations set in the NC (excluding the general requirements for cyber hygiene). Do you think this approach is consistent with the general idea to uplift and harmonise the cybersecurity level within the ecosystem in order to efficiently protect cross-border electricity flows?

- ○ Yes
- ⦿ No

Please, explain why:

600 character(s) maximum

> While we agree in principle with this approach, we find that additional clarity is needed on when a small or micro-business will be defined as important/essential and which authority will be responsible for this definition.

4. Cybersecurity security governance

Question 6 - Do you find that the proposed FG succeeds in establishing a sound governance for the overall process of ensuring the cybersecurity of cross-border electricity flows?

○ Yes
◉ No

What is missing and where do you think ACER should put more attention to?

600 character(s) maximum

> We support the lean governance structure proposed. It is essential to ensure that existing agencies with competences on Information Security agree on cooperation & on a single energy specific contact point for energy specific incidents (SPOC), which is to be informed in case of a CS incident. We support the idea, as under current regulation, power exchanges are often already required to report to multiple institutions with differing standards. There is significant potential to reduce efforts to report and self-assess. In particular, a SPOC could reduce these efforts & avoid double-reporting.

Question 7 – The proposed FG describes the process and governance to determine the conditions to classify and distinguish electricity undertakings with different risk profiles for cross-border electricity flows. Is the decision on setting up the conditions assigned to the right decision group or should that decision be taken at a higher strategic level in respect to what is proposed in the draft, having in mind that this decision will be extremely sensitive?

○ Yes, the decision is taken by the right decision group.
○ No, the decision shall be taken at a higher strategic level.

Please, explain shortly by whom and your reasoning:

600 character(s) maximum

> Rather than setting up a new process to determine the conditions to classify and distinguish entities, we believe existing lists can be used, such as those under NIS2 and relevant national legislation (BSI-KritisV for example). Not having a consistent and clear definition of essential and important electricity undertakings could lead to unnecessary complexity.

Question 8 – Please, tell us which aspects of the proposed governance may better be developed further.

Per each line covering the governance aspects of each chapter, please select all statements that can fit.

	Roles are defined	Responsibilities are assigned	Authorities are defined	Accountability is clear	High level decisional processes are defined
General Governance	☐	☐	☐	☐	☐
Cross Border Risk Management	☐	☐	☐	☐	☐
Common Electricity Cybersecurity Level	☐	☐	☐	☐	☐
Essential information flows, Incident and Crisis Management	☐	☐	☐	☐	☐
Other aspects	☐	☐	☐	☐	☐

Please, add comments in case you may suggest changes to the attribution of roles, responsibilities, authorities, and to the envisaged processes, where described.

600 character(s) maximum

> More precise definitions are needed to be able to evaluate the points mentioned above. However, as a general remark, we suggest that NEMOs have a specific role in governance of the NC.

5. Cross border risk management

Question 9 – The draft FG proposes a high-level methodology for cross border risk assessment presented in chapter 3 and based on three consecutive levels. Is this high-level methodology adequate for assessing and managing risks of cross-border electricity flows?

- ○ Yes
- ◉ No

Would you suggest any alternative way to proceed?

600 character(s) maximum

> Identification scenarios having the potential to escalate should be identified commonly. To ensure harmonisation and efficiency, Member States should not decide on relevant scenarios themselves. Rather, a newly established European CERT could take the function of commonly identifying and defining relevant scenarios. This proposal is based on the Computer Incident Response Centre Luxembourg which is a government-driven initiative designed to gather, review, report and respond to cybersecurity threats and incidents.

Question 10 - Do you think that the FG covers the risks that may derive by the supply chain?

- ○ It covers too much.
- ○ It covers fairly.
- ◉ It covers fairly, but the tools and means shall be clearer.
- ○ It covers poorly.

5. Common Electricity Cybersecurity Level

Question 11 - Considering the 'minimum cybersecurity requirements' (with regard to Table 2 of the FG), select just one option:

- ○ They are applied to the right entities, they are proportional, and they fit with the purpose to protect cross-border electricity flows from cybersecurity threats.
- ○ They are applied to the right entities, they are proportional, but they do not fully fit with the purpose to protect cross-border electricity flows from cybersecurity threats.
- ◉ They are applied to the right entities, but they are not proportional, and they partially fit with the purpose to protect cross-border electricity flows from cybersecurity threats.
- ○ They are applied to the wrong categories.

Question 12 - Considering the 'advanced cybersecurity requirements' (with regard to Table 2 of the FG), select just one option:

○ They are applied to the right entities, they are proportional, and the fit with the purpose to protect cross-border electricity flows from cybersecurity threats.

○ They are applied to the right entities, they are proportional, but they do not fully fit with the purpose to protect cross-border electricity flows from cybersecurity threats.

● They are applied to the right entities, but they are not proportional, and they partially fit with the purpose to protect cross-border electricity flows from cybersecurity threats.

○ They are applied to the wrong category and entities.

Please, explain your reasoning for your answer to question 11 and 12, if necessary

600 character(s) maximum

> It is difficult to respond to the question as essential and important entities are not clearly defined under the NC. As mentioned under question 4, a burden of duplication should be prevented. Only a harmonised and efficient cross-sectoral regime will allow for optimal strengthening and usage of existing and future Cyber Security (CS) capacities.

Question 13 - Please select the option(s) which in your view better represent how a common cybersecurity framework protecting cross-border electricity flows, should be established and enforced?

○ Through common electricity cybersecurity level that shall be certifiable by a third party (e.g. by the application of ISO/IEC 27001 certification).

○ The framework shall be based on a set of agreed requirements that shall be assessed, and their implementation shall be subject to governmental inspections.

○ A peer accreditation process shall be established, where electricity undertakings evaluate each other against a set of agreed requirements set by governmental authorities.

● A combination of those above.

○ Another better solution.

Please, briefly describe it:

600 character(s) maximum

> A combination of the suggestions the ensures common minimum requirements are met is most desirable. There should be the possibility that these minimum requirements can be met through different approaches. For example, entities already certified under a certain standard should be able to make use of their certification while other entities will have the possibility to meet the requirements through other measures proposed.

Question 14 - The proposed FG extends the obligation of the cybersecurity measures and standards to "essential service suppliers" to which an entity may outsource essential services, operations of essential assets and services, or a full essential process, that has an impact on the cybersecurity of cross-border electricity flows. Do you think this approach is correct?

● Yes
○ No

6. Essential information flows, Incident and Crisis Management

Question 15 - The FG proposes the use of designated Electricity Undertaking Security Operation Centre (SOC) capabilities to enable information sharing and to smooth incident response flows from all electricity undertakings in order to:

- Provide agility to all electricity undertakings with respect to sharing and handling important cybersecurity information for cross-border cybersecurity electricity flows;
- Avoid interference and additional workload on the National CSIRTs and to their existing cooperation;
- Promote a responsible, autonomous, flexible, timely, coordinated and controlled approach to information sharing and incident handling, in line with current electricity practices and in line with the specific operational needs.

Considering the proposed approach, please select one option:

○ The proposed approach is feasible, can foster trust and provide enough flexibility and reliability, which are essential for the cross-border electricity flows.

○ The proposed approach is feasible and can foster trust but it is not ideal for meeting the requested flexibility and reliability level.

○ The proposed approach is feasible, but can hardly foster trust and it is not ideal for meeting the requested flexibility and reliability level.

◉ The proposed approach is not feasible, therefore needs to be reviewed.

Please, explain the reasoning for your choice (and if not feasible, explain the alternatives you would envisage)

600 character(s) maximum

> CSIRTs are best placed to enable information sharing and incident response, as such we support an approach in which European CSIRTs are strengthened and provided with sufficient resources to enable them to take on these additional responsibilities. This is particularly important as cybersecurity is a cross-sectoral issue that cannot be treated only sector specifically.

Question 16 – The draft FG proposes the adoption of SOC to overcome other needs that go beyond the simple information sharing:
while it will offer the possibility to let the electricity sector to autonomously structure the information sharing infrastructure, ideally sharing resources and cooperating with the aim to reduce costs, offering high-end cybersecurity protection to cross border electricity flows, the same SOC may be delegated to other certain tasks for which a SOC is better placed in order to offer services (e.g. orchestrating cooperation with other CSIRTs, providing support in planning and execution of cybersecurity exercises, support and cooperate with critical and important electricity undertakings during crisis management situations and more);
Do you think that this secondary role is appropriate for the SOC?

○ Yes
◉ No

Please, provide your reasoning:

600 character(s) maximum

> The secondary role of SOCs may unnecessarily increase the points of contact needed for information sharing and lead to repetition of reporting.

Question 17 - Do you believe a Cybersecurity Electricity Early Warning System as described in the proposed FG chapter 5.4 is necessary?

- ◉ Yes, it is necessary.
- ○ No, it is not necessary.

Question 18 - Concerning the obligation for essential electricity undertakings to take part to cybersecurity exercise as described in chapter 6 of the draft FG, please select one of the following options:

- ◉ It is in line with the objectives, and it contributes to the substantial improvement of the cybersecurity posture necessary for cross-border electricity flows.
- ○ It is in line with the objectives, and it contributes to the substantial improvement of the cybersecurity posture necessary for cross-border electricity flows, but the applicability should be extended to all electricity undertakings.
- ○ It is in line with the objectives, but it does not really contribute to the improvement of the cybersecurity posture necessary for cross-border electricity flows.
- ○ It is not in the objectives, and it should be abandoned.

7. Protection of information exchanged in the context of this data processing

Question 19 - The proposed FG provides for rules to protect all information exchanged in the context of the data processing concerning the network code.
Considering the proposed rules and principles, please select one of the following options:

- ○ The proposed rules and principles are appropriate and cover all aspects needed to secure the information exchanges in the context of the network code.
- ○ The proposed rules and principles are appropriate but miss some additional aspects needed to secure the information exchanges in the context of the network code.
- ◉ The proposed rules and principles are not appropriate and miss many additional aspects needed to secure the information exchanges in the context of the network code.
- ○ The proposed rules are excessive, and a relaxation of rules and principles is suggested.

Please, describe the reasoning behind your choice:

600 character(s) maximum

8. Monitoring, benchmarking and reporting under the network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

Question 20 - The proposed FG suggest monitoring obligations to verify the effectiveness in the implementation of the NC. In this respect, do you think they are appropriate?

- ○ The proposed monitoring obligations are appropriate and they cover all aspects needed to carefully monitor the implementation of the network code.

○   The proposed monitoring obligations are appropriate but they do not cover all aspects needed to carefully monitor the implementation of the network code.

○   The proposed monitoring obligations are not appropriate and they do not cover all aspects needed to monitor the implementation of the network code.

◉   The proposed monitoring obligations are excessive, and a major revision of the principles is suggested.

Please, describe the reasoning behind your choice

600 character(s) maximum

> A gap-analysis should be conducted before additional monitoring, benchmarking, and reporting obligations are put in place. It is necessary to look closely at the existing obligations of entities to ensure efficiency (both in terms of monetary cost and time) and avoid unnecessary duplications. Please refer to our answer to Question 1.

Question 21 - The proposed FG suggests benchmarking obligations to control the efficiency and prudence in cybersecurity expenditure, resulting from the implementation of the NC. Moreover, benchmarking, together with the identification of cybersecurity maturity levels of electricity undertakings, may constitute the grounds to further incentivise cybersecurity culture for cybersecurity electricity flows in the future.
In this respect, do you think that the benchmarking obligations are appropriate?

○   The proposed benchmarking obligations are appropriate and cover all aspects needed to monitor the efficiency and prudence in cybersecurity expenditure during the implementation of the network code.

○   The proposed benchmarking obligations are appropriate but they do not cover all aspects needed to monitor the efficiency and prudence in cybersecurity expenditure during the implementation of the network code.

○   The proposed benchmarking obligations are not appropriate and they do not cover all aspects needed to monitor the efficiency and prudence in cybersecurity expenditure during the implementation of the network code.

◉   The proposed benchmarking obligations are excessive, and a major revision of the principles is suggested.

Please, describe the reasoning behind your choice:

600 character(s) maximum

> We welcome appropriate benchmarking obligations, however benchmarking must not focus solely on the cybersecurity expenditure but also consider the overall maturity of cybersecurity measures in place. Furthermore, benchmarking obligations in the NC should not duplicate existing obligations or require excessive additional effort without justification.

Question 22 - The proposed FG suggests reporting obligations: the aim of the reporting obligations is to facilitate informed high-level decisions on the revision of the network code.
Considering the proposed reporting obligations, please select one of the following options:

○   The proposed reporting obligations are appropriate and cover all aspects needed to monitor the achievement of the objectives of the network code.

○   The proposed reporting obligations are appropriate but they do not cover all aspects needed to monitor the achievement of the objectives of the network code.

○   The proposed reporting obligations are not appropriate and they do not cover all aspects needed to monitor the achievement of the objectives of the network code.

◉   The proposed reporting obligations are excessive, and a major revision of the principles is suggested.

○   The proposed reporting obligations are very limited, and a major revision of the principles is suggested.

Please, describe the reasoning behind your choice:

600 character(s) maximum

> As proposed above, a gap-analysis should be conducted and potential reporting obligations should carefully be evaluated to ensure efficiency and prevent unnecessary duplications. Please refer to our answer to Question 1.

Question 23 - Do you think the proposed FG sufficiently cover cybersecurity aspects of:

	Partially covered	Fairly covered	Substantially Covered	Fully covered
Real-time requirements of energy infrastructure components.	○	●	○	○
Risk of cascading effects.	○	●	○	○
Mix of legacy and state-of-the-art technology.	○	●	○	○

Question 24 - Do you have any other comment you want to share and that are not included in the previous questions, with regard to the rest of the content of the draft FG ?

1000 character(s) maximum

> We would like to underscore that the FG should be based on established international standards for managing cybersecurity - namely NIST (National Institute for Standards and Technology) and the Cybersecurity Framework (CSF), and not only rely on the ISO/IEC 2700X standards referenced in the current proposed FG. Recently the aforementioned standards have been used as a basis for guidance on cyber resilience, such as CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure and G7 Fundamental Elements of Cybersecurity for the Financial Sector.
>
> As a more general comment, we would also like to highlight that additional stakeholder engagement would be greatly appreciated as this process continues.

Contact

[Contact Form](#)