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

[redacted]

* Last Name

[redacted]

* Company/Institution

Terna Rete Elettrica Nazionale S.p.A.

* Type of business

TSO

Address

* Contact email

[redacted]

Phone

Country

IT - Italy

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

As the future NC will apply only to the electricity sector, its support will be limited to electricity crisis and an ongoing risk will remain until all essential sectors will be aligned. The supply chain of the electricity sector involves a large group of stakeholders to be consulted, delaying NC implementation. It is important to identify the essential stakeholders for which the FG should strictly frame the systems and services for the security of the supply chain. The FG requirements are ambitious for smaller parties and their implementation hard: appropriate thresholds shall then be defined

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

These aspects should also be covered:a)definitions of legacy systems,functional/non-functional requirements, random security audits, excess of disclosure of information;b)consideration of National Competent Authorities for Risk Preparedness participating in cross-border risk assessment, for consistency between specific new cybersecurity risks and the RPP cybersecurity scenarios;c)definition of responsibilities in the asset inventory;d)providing a short summary in each chapter explaining the goal of the focus areas;e) the Zero Trust of Supply Chain,Penetration Tests,Cross Border Threat modelling

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

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

The role of RCCs is overqualified and not in line with Regulation 2019/943, which do not give to ACER the competence to assign new tasks to RCCs.
In addition, RCCs have no competence in cyber domain. Gaining such expertise and the necessary resources/skills would require a significant effort and a long time, delaying the NC implementation.
FG should consider more the role of ECG by assigning to it the tasks supposed to be carried out by RCCs. With Members States, ENTSO-E, ACER and EU DSO entity, the needed expertise can be committed to support the cross-border cyber risk assessment.

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

The suggested criteria consider financial and economic fundamentals of the undertakings to establish if they should belong to the scope or not. Terna recommends improving these criteria introducing further metrics: power managed (generated, transported, distributed, aggregated) by the undertaking and the number of final EU user impacted in case of interruption of essential service provided by undertaking. These metrics are directly dependent on the essence of the “essential service” provided by the undertakings, that constitute the relevant value to be protected with the enforcement of the NC.

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

- [x] No

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

600 character(s) maximum

Cybersecurity cross-border electricity flow process is detailed enabling good/secure environment. Governance of this process is not appropriate if RCCs have an active role in drafting methodologies /standards, as they do not have the appropriate competence and means to perform an active role during/ after a cross-border cyber incident (resources/skills/IT solutions). RCCs' services are only vs TSOs.
It is doubtful ACER's role in supervising the cybersecurity requirements, as NRAs don't have this role under national legislation. National competent authorities should assume this role.

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?

- [x] 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

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

We suggest not to create new cybersecurity region, but to adapt the SOR concept, identifying a unique SOR competent for cybersecurity where a single undertaking is part of more than one SOR. RCCs role is overqualified and not in line with Reg 943, where RCCs are mandated and provide services only for TSOs. The FG should consider more the role of ECG by assigning to it the tasks supposed to be carried out by RCCs. With MS, ENTSO-E, ACER and EU DSO entity, the needed expertise can be committed to support the cross-border cyber risk assessment. FG should provide more info on the role of CERT EU.

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

It is recommended a top-down Business Process Risk approach to cyber risk identification, evaluation and treatment, rather than the asset management bottom-up approach recommended by the FG. Taking the (critical) business processes as starting point for risk assessment will be both more efficient and effective.

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

The governance for the cybersecurity cross-border risk management where the RCCs have an active role is not appropriate for the reasons detailed answering to question 4.

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

We deem it essential that the scope of the future network code reflects the NIS Directive. Indeed, considering other standards to be adhered to, e.g. ISO/IEC 27001 certification, would imply expanding the set of requirements to be implemented. This would drive significant additional costs/resources/processes without substantial additional benefits.
We consider the most pragmatic approach would be the one based on coordination among affected system operators and active involvement of competent national authorities.

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.

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

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.

Please, briefly describe the reasoning behind your choice:

600 character(s) maximum

The exercise framework/scheme is very extensive and will bring added value to all participants. As all TSOs and other entities have their own specific needs, such cyber exercises should be prepared in close alignment with the participants to allow triggering and following the topics of interest for them. With reference to the chapter on cyber exercises,main concern is related to the timing between exercises.Indeed, the FG should consider at least 3 years between such events to ensure there is enough time to study the "lessons learned" or implementing any changes before the next exercise begins

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

While the monitoring and benchmarking provisions in principle meet the objectives of the NC, reporting obligation shall consider national laws, which can prohibit sharing certain info. The proposed FG set several clauses requiring to report and/or gather information that could be of a security sensitive nature, either in it's own right or when combined and aggregated with other data. It is important that such sensitive information is gathered exclusively if there is a clear benefit in doing so, if not in contrast with national legislation.

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.

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

The role of RCCs should be excluded from reporting tasks, due to the lack of expertise, skills and IT solutions. Also, the description and mandate of RCCs pursuant to the Regulation (EU) 2019/943 does not enable them to carry out such tasks.

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 deem it essential that the scope of the future NC reflects the NIS Directive, avoiding to refer to other standards to be adhered to which would result in an ineffective extension of the requirements to be implemented

It is important that the EPSMM is the basis for the model and that the network code will not develop an entirely new model that would knock over all work already done within the area of cyber security.

The asset inventory shall assess and clarify the existence and interdependence of physical and virtual assets.

Contact

Contact Form