

# WELCOME TO THE PUBLIC CONSULTATION WORKSHOP ON THE NETWORK CODE ON CYBERSECURITY

WE ARE WAITING FOR ATTENDEES TO JOIN  
THANK YOU FOR YOUR PATIENCE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."

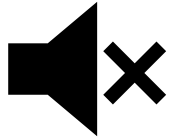


# ORGANISATIONAL DETAILS



**Workshop planning: 3 hours**

**Interactive (Q&A + MT Polls in the Chat)**



**All participants must stay muted when not speaking**

**Speak only when given the floor by the moderator**



**Recording/streaming is needed to ensure transparency and proper implementation of ENTSO-E and EU DSO Entity mandates. If you anyone objects, please do so now.**



**All the questions and comments received in the MT chat will be addressed after the workshop**



**During the Q&A the participants can raise the hand to ask a question / make a comment  
The moderator will give you the floor**

# NETWORK CODE ON CYBERSECURITY

WORKSHOP: PUBLIC CONSULTATION, 8<sup>TH</sup> DECEMBER 2021

WELCOME ADDRESS

ANDREA FOSCHINI & CHRISTIANE GABBE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



# RECAP & OVERVIEW

CHRISTIANE GABBE



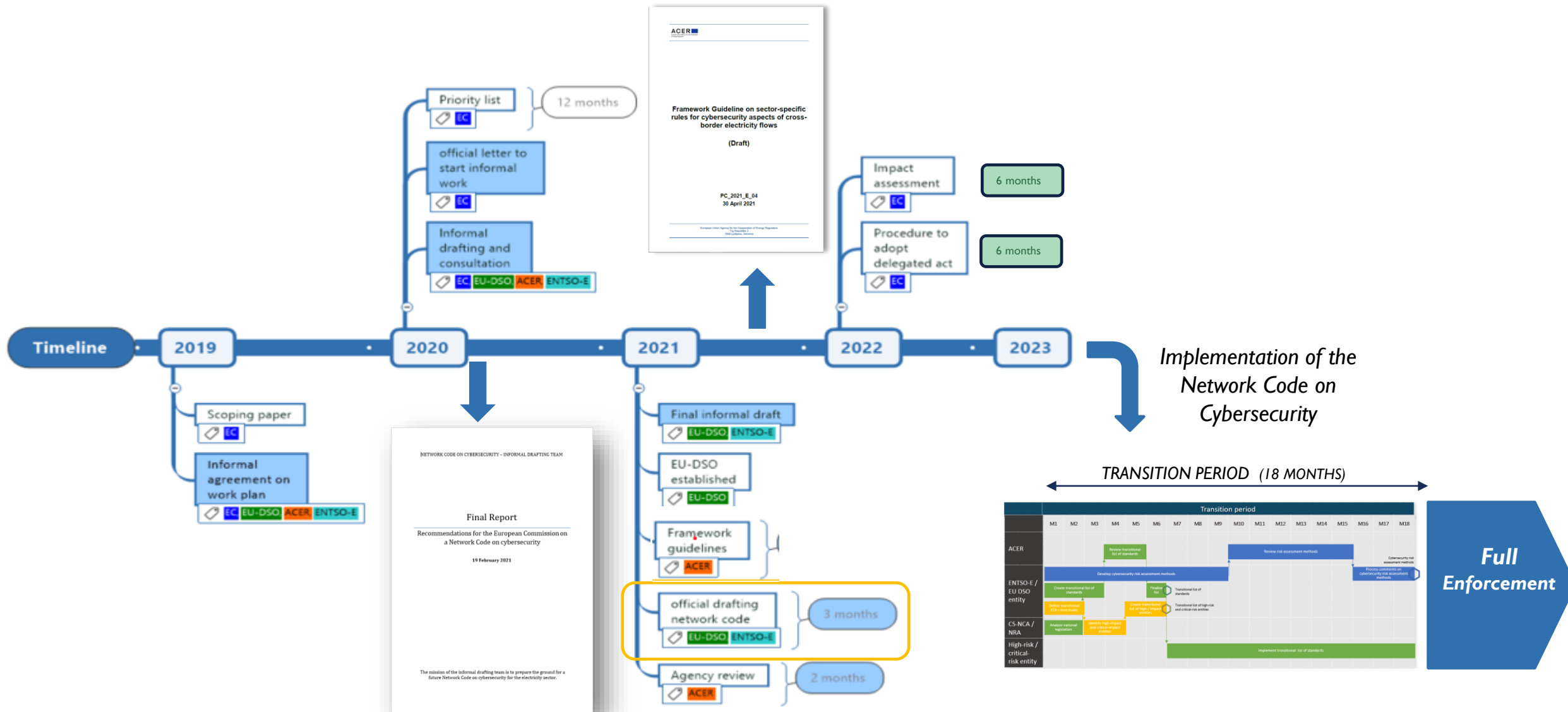
A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



# THE TIMELINE (BIRD'S VIEW)



## THE TIMELINE... WHERE WE ARE NOW?

PROJECT	TASK		START	PLAN END
Phase 1 NC CS v1	Drafting NC CS Version 1 (DT)	✓	27/07/2021	11/11/2021
	Drafting Committee review	✓		
	Transpose the NC CS v1 in legal text	✓		
	Deliver the revised NC CS v1 (DT)	✓		
Phase 2 NC CS public consultation	Stakeholders' updates	✓	12/11/2021	10/12/2021
	NC CS public consultation	✓		
	Public Consultation Workshop 1	✓		
	Public Consultation Workshop 2 (December 08 <sup>o</sup> , 2021)			
Phase 3 NC CS v2	Incorporate all comments from public consultation (DT)		13/12/2021	14/01/2022
	Deliver NC CS v2 (DT0)			
	Drafting Committee' review			
	Submit NC CS final to ACER			

## NEXT STEPS



All the relevant information (including registration to the workshop) can be found here: [Cybersecurity \(entsoe.eu\)](https://www.entsoe.eu/cybersecurity)

# TITLE I: GENERAL PROVISIONS

DAIGA DEGE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."

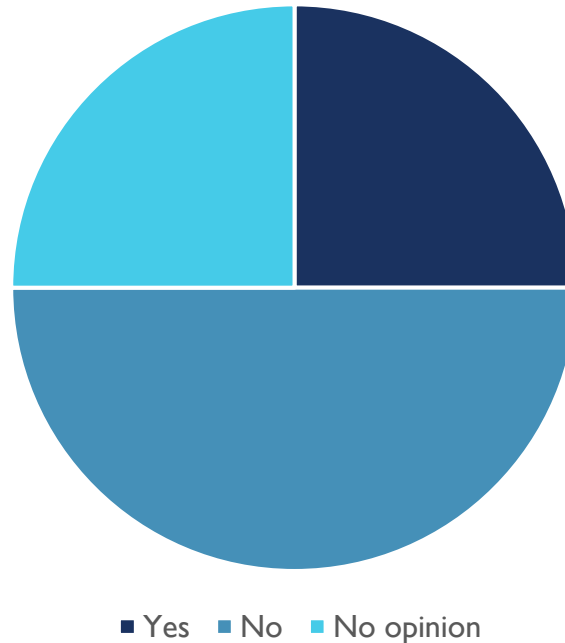




---

---

Are the objectives of the Network Code on Cybersecurity, which lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management sufficiently clear?



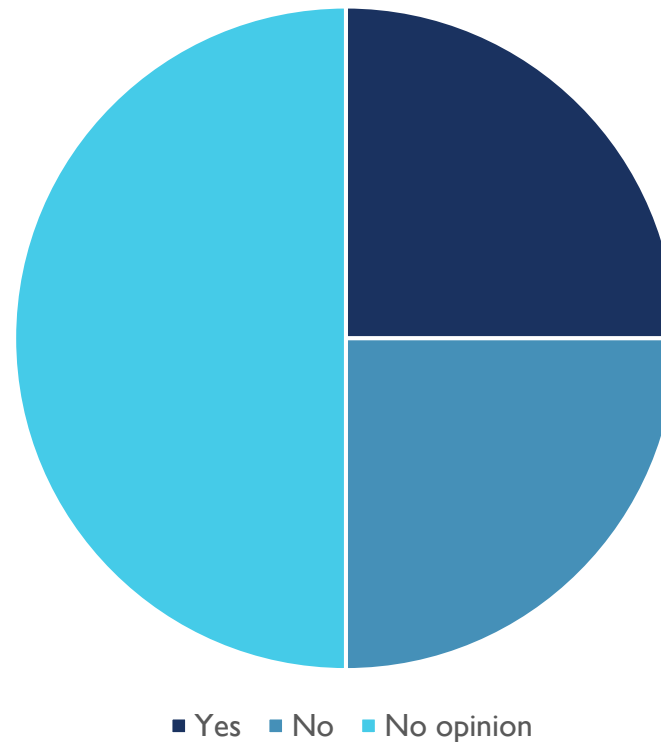
Comments:

- A suggestion to include clear verification rules by a third party;
- A suggestion to include aspects that would allow for not sharing the information under a certain circumstances (e.g. national regulations);
- The discussion on which services will have an influence on the cross-border flows will be one of the most crucial points.

---

---

The NCCS states: "Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation." Based on the statement above, are twelve months a reasonable timeframe?



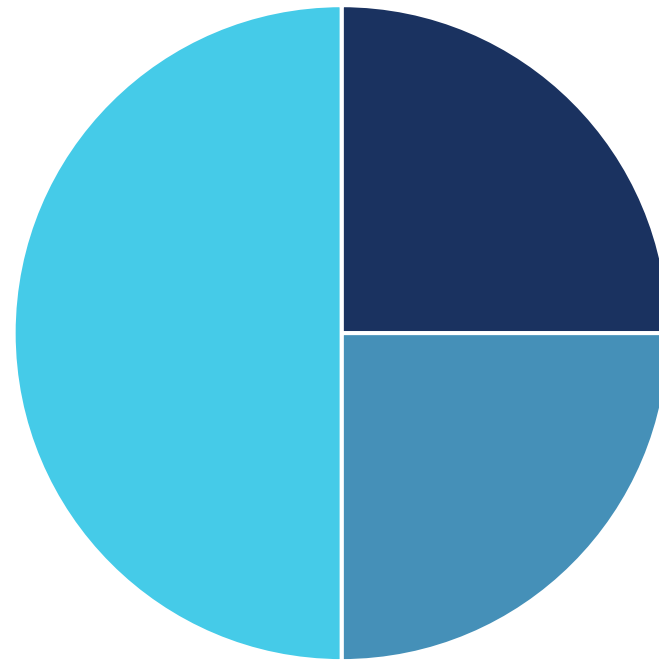
Comments:

- For many micro or small sized enterprises this is too ambitious. 18 or 24 months is more reasonable.

---

---

The NCCS states: "Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation." Based on the statement above, do you think these requirements for small and micro enterprises are of sufficient level?



■ They are at the appropriate level    ■ They are too flexible, more strict requirements should be in place    ■ No opinion

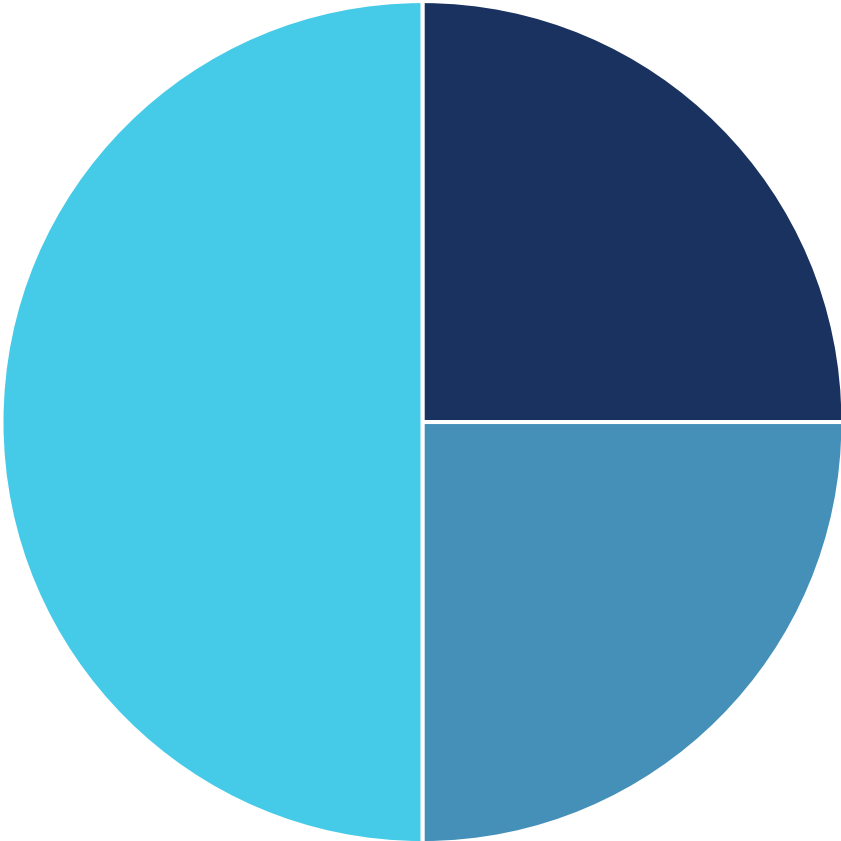
Comments:

- A suggestion to include enforcement of protection against malicious code should be included.

---

---

Do you consider the Monitoring approach defined at Article 12 to be effective to monitor the adequacy of the Network Code to the ever-changing technology landscape and evolution of applicable cybersecurity standards?

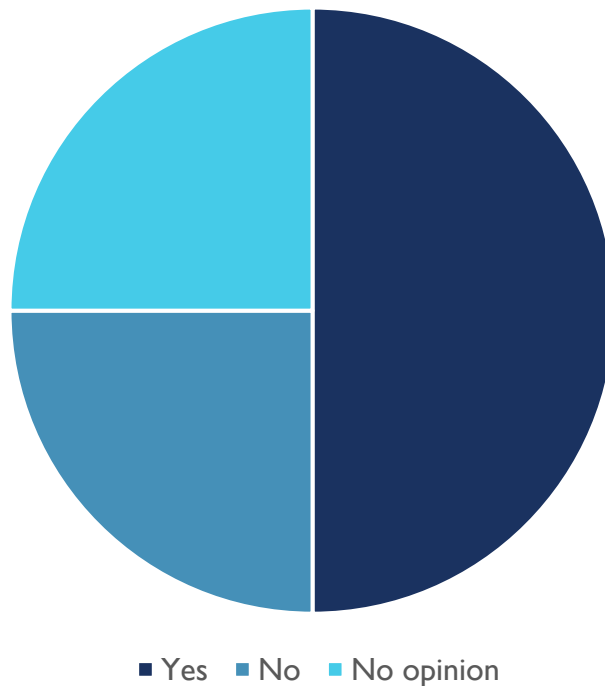


■ Yes ■ No ■ No opinion

---

---

Do you think the Benchmarking approach, as described in Article 13, is an adequate tool to assess whether current investments in cybersecurity to protect cross-border electricity flows are sufficient?



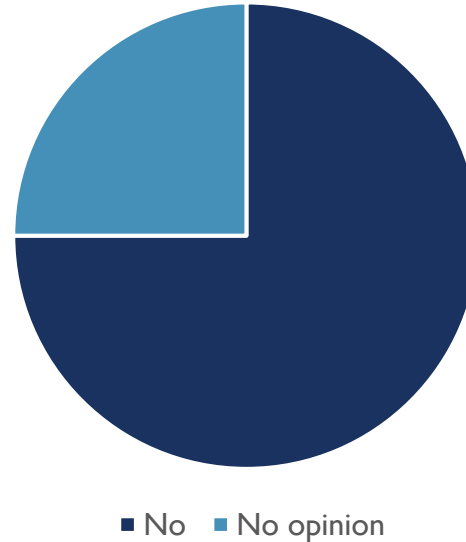
Comments:

- Benchmarking of average cost does not adequately consider the different cost structures in the Member States, meaning that higher costs would be considered as a higher level of cybersecurity without taking into account the efficiency of the measures associated with the costs.

---

---

Do the overall timelines within the Network Code on Cybersecurity seem reasonable?



Comments:

- Smaller entities do not have the same capacity as the bigger ones for the implementation process, thus more flexibility is needed;
- Multiple new legal requirements are approaching the energy sector almost simultaneously which requires coordination between different legislators to avoid overburdening entities;
- Companies currently defined as "critical generation companies", extensive processes and measures mostly based on ISO 270xx, are being implemented to ensure IT security. Provided that these are accepted in this Network Code which we consider as an absolute prerequisite, timelines should be realistic. New affected companies or significant additional requirements will hardly be implementable within the given NC deadlines. Timelines should be aligned with a typical procedure durations of ISO 270xx implementation based on statistics from certification bodies.

# QUESTIONS & DISCUSSIONS

SABINE HINZ




A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



- 
- The received stakeholder comments on the “general provisions” focus on: definitions, scope, benchmarking,
    - Definitions: the NCCS takes existing legally binding definitions into account. Proposed improvements of “new definitions” are under evaluation.
    - Scope: comments go in different directions (scope too narrow or too large).
    - Timing: timing considered as tight by most stakeholders, but different views with regard to feasibility.
    - Benchmarking: proposed criterion “cybersecurity expenditure” considered as not representative for cybersecurity level in EU Member States. Data on cybersecurity expenditure cannot be separated from IT expenditure.



# TITLE II: GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

DAIGA DEGE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



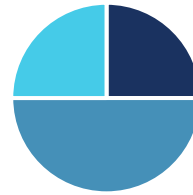
Is it reasonable that the entities involved can perform the following tasks within the time set in the network code, given resource, capability, or other constraints?

Activities led by the CS-NCA and NRA:

- a) CS-NCA and NRA to perform the member state risk assessment within 3 months (Article X)
- b) CS-NCA and NRA to make a transitional list of high-impact and critical-impact entities within 6 months after receiving the transitional ECII (Article Y)
- c) CS-NCA and NRA to identify high-impact and critical-impact entities within 6 months after receiving the ECII (Article Z)

Activities performed by entities:

- d) High-impact and critical-impact entities to report the results of their risk assessment in 6 months
- e) High-impact and critical-impact entities to implement the minimum and advanced cybersecurity controls in 6 months after their publication
- f) High-impact and critical-impact entities to provide evidence of verification of the controls in 24 months after their publication



■ Yes ■ No per activity ■ No opinion

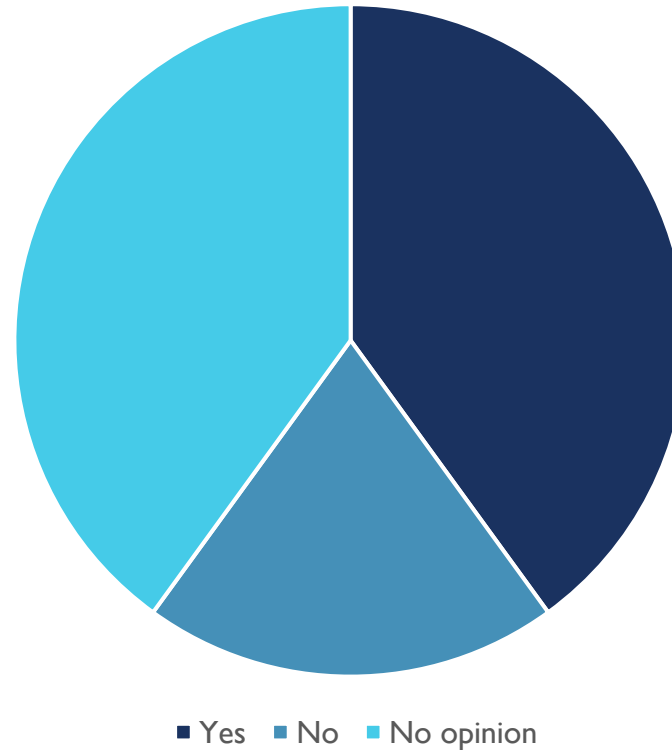
Comments:

- 6 months is too short time to implement controls unless the entity has a good basic level already. Most will not meet this requirement;
- Companies currently defined as "critical generation companies", extensive processes and measures mostly based on ISO 270xx, are being implemented to ensure IT security. Provided that these are accepted in this Network Code which we consider as an absolute prerequisite, timelines should be realistic. New affected companies or significant additional requirements will hardly be implementable within the given NC deadlines. Timelines should be aligned with a typical procedure durations of ISO 270xx implementation based on statistics from certification bodies.

---

---

Is the proposed governance for cybersecurity risk assessment clearly described and sufficient to meet the objectives of the network code on cybersecurity?



Comments:

- For individual providers of electricity services, the description cannot yet be clear, as the main details are to be determined after the NC comes into force. It is expressly pointed out that the further process after the publication of the NC must be carried out with the involvement of all stakeholders in public processes in order to ensure acceptance and the possibility of implementation in practice.

# TITLE III: RISK MANAGEMENT AT UNION AND REGIONAL LEVEL

DAIGA DEGE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

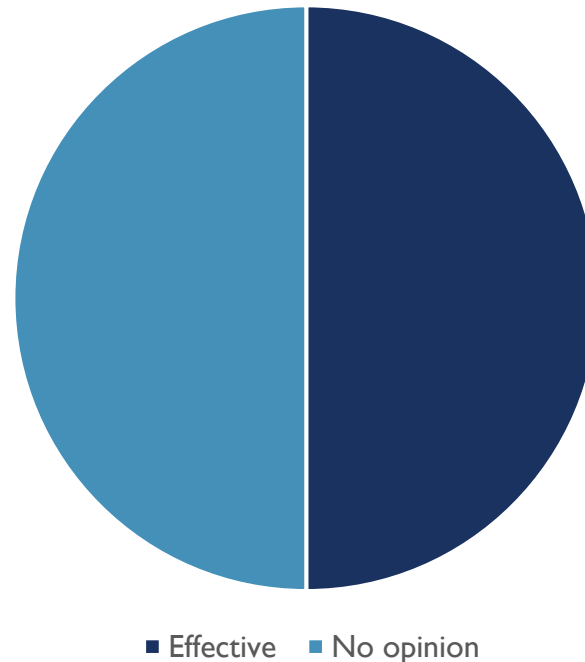
The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



---

---

Under the network code draft, cybersecurity risk assessments are performed at four levels: Union-wide, regional, member state, and entity. By integrating information from these four levels, it should be possible to get a comprehensive view on the risks. How effective do you think this multi-level process will be in assessing and reducing the cross-border cybersecurity risks in the European electricity sector?



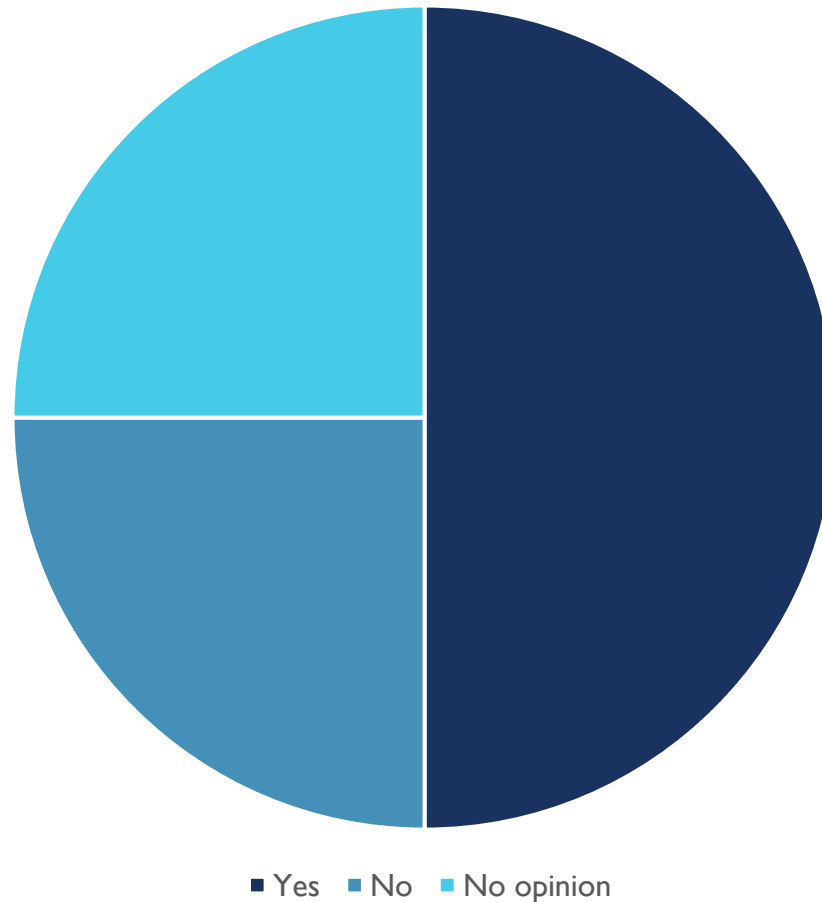
Comments:

- Bottom-up approach is an effective risk assessment strategy;
- Effective risk assessment process could be improved by automated pentesting.

---

---

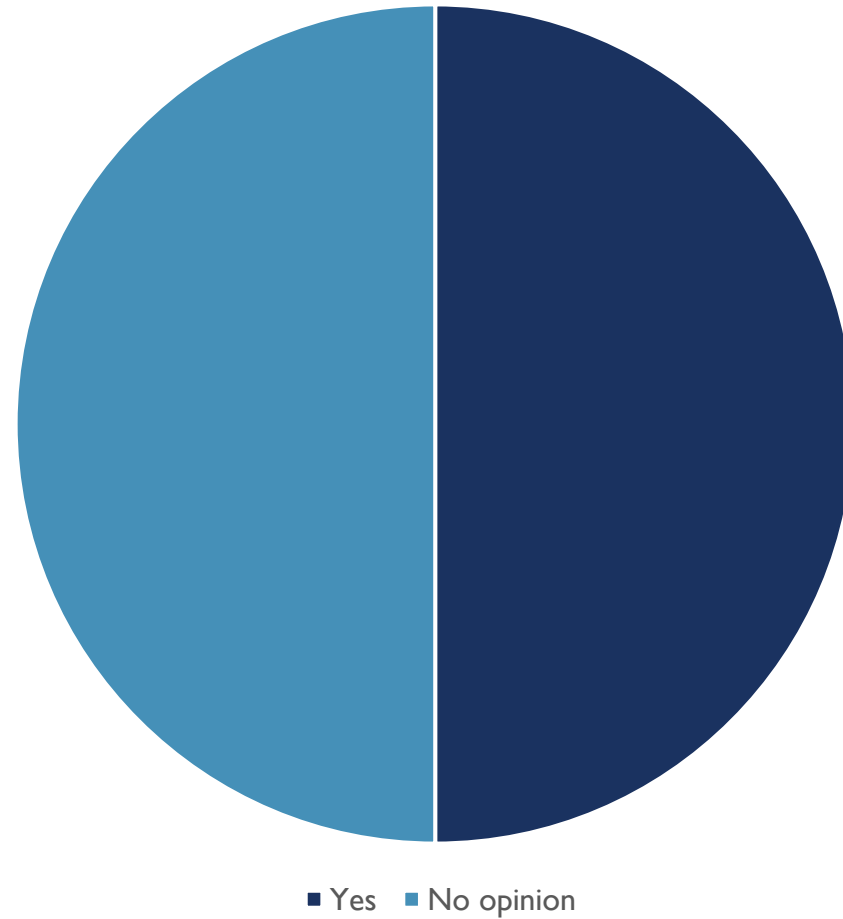
The proposed scope of the cybersecurity risk assessments is the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. Legal, financial or reputational damage of cyber-attacks are out of scope. Do you think this is a good scope to manage the cybersecurity risks to cross-border electricity flows?



---

---

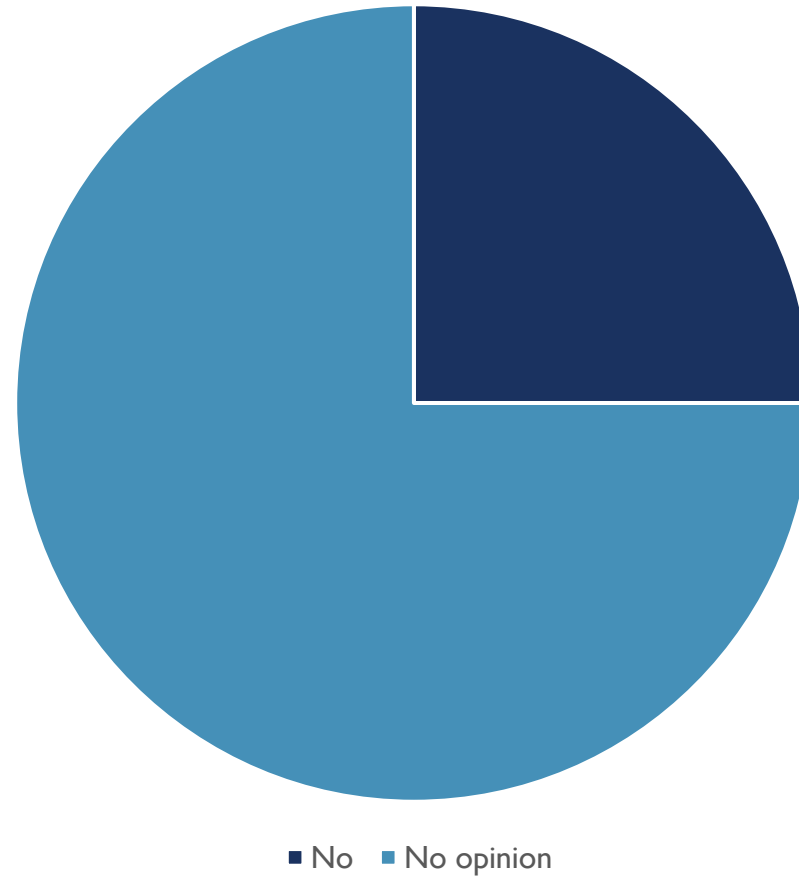
Under the proposed cybersecurity risk management process, ENTSO-E and EU DSO with the RCCs make and approve a risk treatment plan. In approving the plan, they could be seen to accept the residual risks. Do you think this is an appropriate process for accepting the residual risks?



---

---

Is the proposed risk management at union and regional level clearly described and sufficient to meet the objectives of the network code on cybersecurity?



Comments:

- More attention not only to assets but also to processes is crucial.



# QUESTIONS & COMMENTS

KEITH BUZZARD & BART LUIJKX




A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



- 
- Do Stakeholders agree that a bottom-up approach to cross-border cyber risk identification compliments the top-down approach and benefits the overall cyber risk picture?

# TITLE V: RISK MANAGEMENT AT MEMBER STATE LEVEL

DAIGA DEGE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

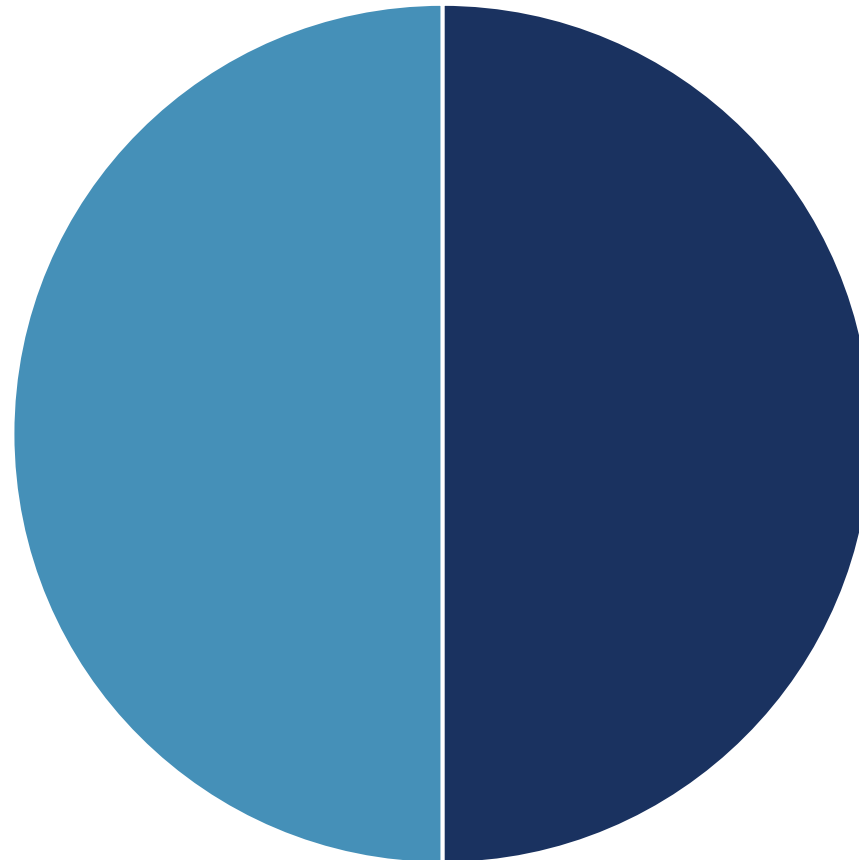
The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



---

---

CS-NCA and NRA can appoint entities as high-impact or critical-impact even where they do not individually meet the ECII level. This allows them to appoint entities for which the aggregate impact of a group of similar entities is above the high-impact or critical-impact thresholds. Do you agree with this mechanism for dealing with groups of similar entities?

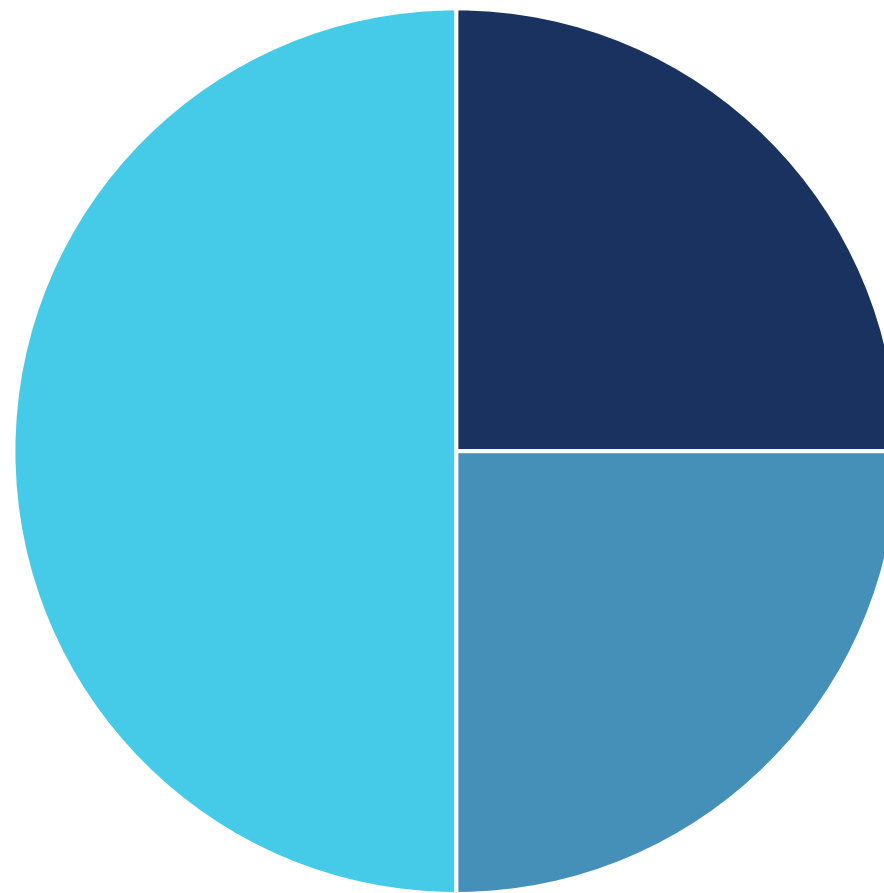


■ Yes ■ No opinion

---

---

Is the proposed risk management at member state level clearly described and sufficient to meet the objectives of the network code on cybersecurity?



■ Yes ■ No ■ No opinion

# QUESTIONS & COMMENTS

KEITH BUZZARD & BART LUIJKX




A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



- 
- Do Stakeholders understand and have the resources required to perform the work as defined by the bottom-up cyber risk approach?

# TITLE VI: RISK MANAGEMENT AT ENTITY LEVEL

DAIGA DEGE

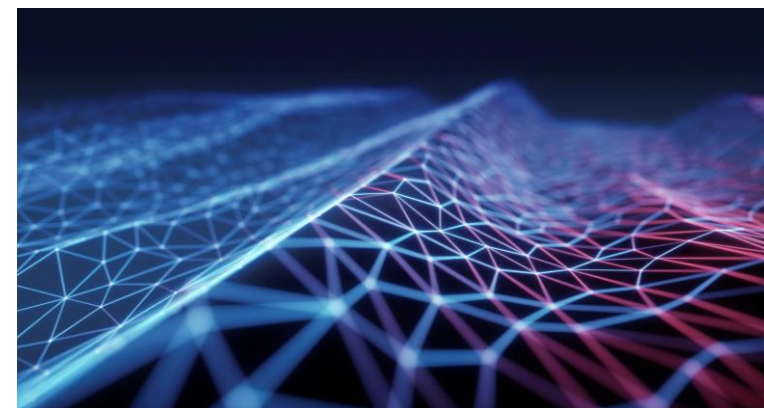


Reliable Sustainable Connected

A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."

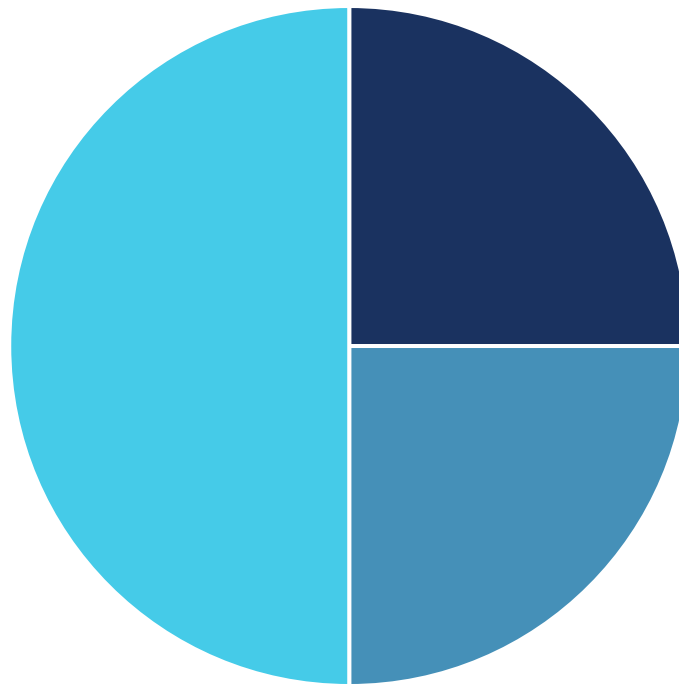




---

---

In Article 31, the network code requires entities to report information about existing controls, threats and vulnerabilities to their national regulators (CS-NCA and NRA). The regulators then report this information to ENTSO-E and the EU DSO entity for the regional risk assessment (Article 26). The information will give a good and detailed view of the cybersecurity risks to cross-border electricity flow. But the information could also be exploited by potential threat actors if they could obtain it. Do you think the benefit of collecting the information will be large enough to outweigh the risk of the information being compromised?

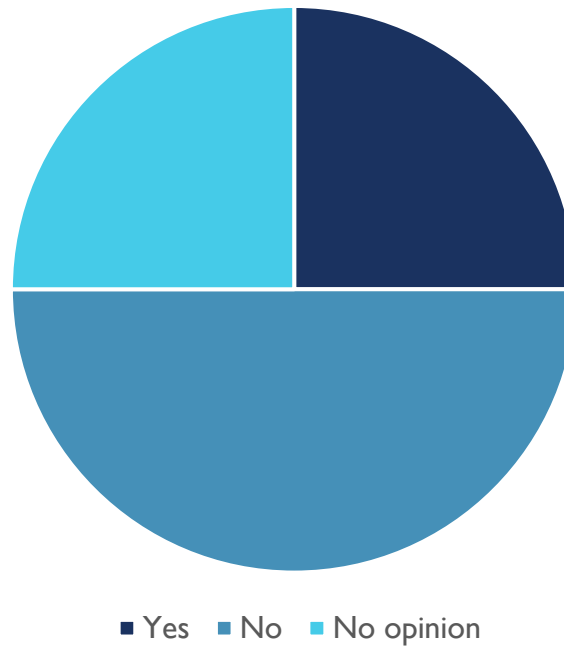


■ Yes ■ No ■ No opinion

---

---

Entities determine the scope of the entity level risk assessment based on the outcomes of the Union-wide risk assessment, in particular the list of Union-wide high-impact and critical-impact processes. Do you think the process for determining the entity-level risk assessment scope is clear, and that the scope will cover all assets the entity needs to support cross-border electricity flows?



Comments:

- For the connected network users, such as generators, it is not clear at this point in time how they will find themselves in the scope, possibly indirectly. Where entities already implemented ISO 270xx procedures or plan to do so, the processes shall be adoptable.

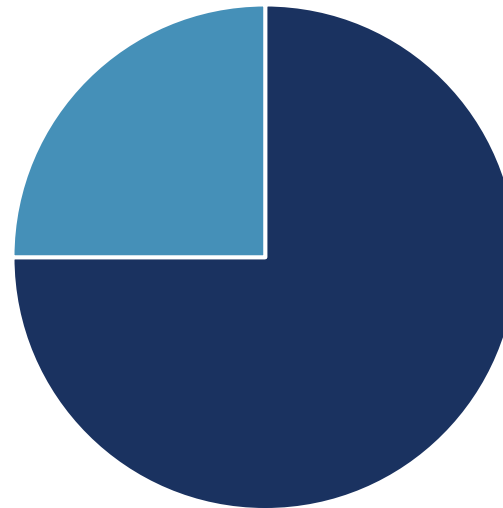
---

---

The network code allows the CS-NCA and NRA to give derogations based on three criteria:

- (a) in exceptional circumstances, when the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefit;
- (b) The entity can provide a risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable according to the risk acceptance criteria pursuant to Article 25.3.b. The risk treatment plan shall be verified through one of the options pursuant to Article 33.
- (c) The results of the risk assessment of the entity do not show any direct or indirect impact on cross-border electricity flows.

Do you agree with the criteria and process for providing derogations?

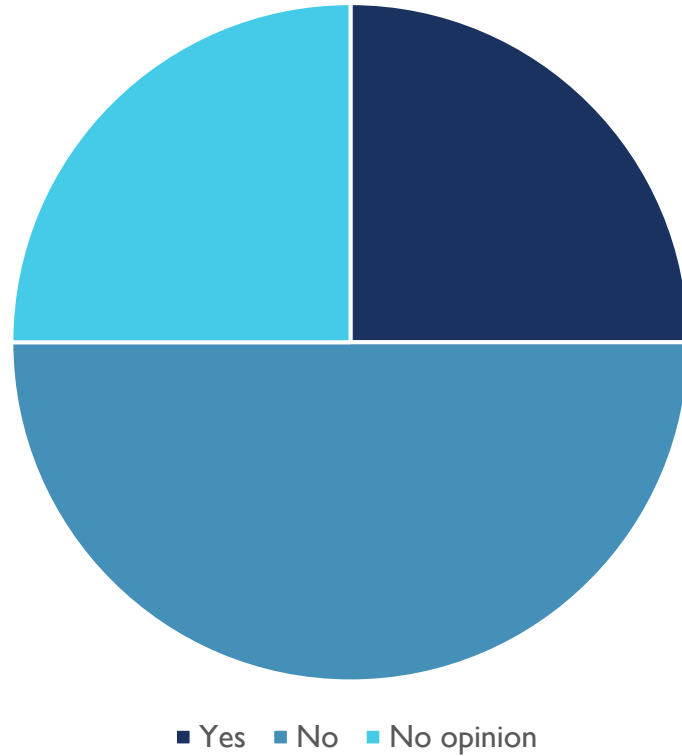


■ Yes ■ No opinion

---

---

Is the proposed risk management at entity level clearly described and sufficient to meet the objectives of the network code on cybersecurity?



Comments:

- For the connected network users, such as generators, it is not clear at this point in time how they will find themselves in the scope, possibly indirectly.

# TITLE IV: COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

DAIGA DEGE & MAARTEN HOEVE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

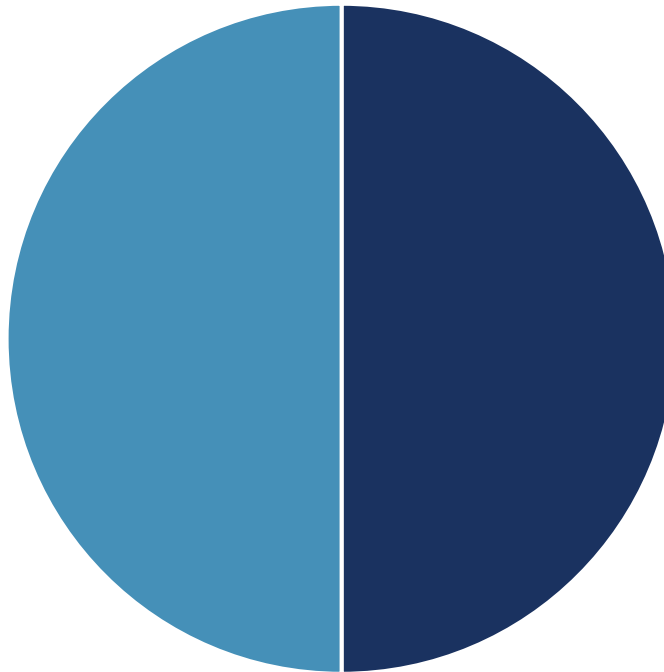
The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



---

---

The network code proposes cybersecurity hygiene requirements in Annex A to ensure that all entities that can affect the cybersecurity of the electricity grid have a baseline security. Do you think the proposed hygiene requirements are appropriate for reducing cross-border cybersecurity risks?



■ No ■ No opinion

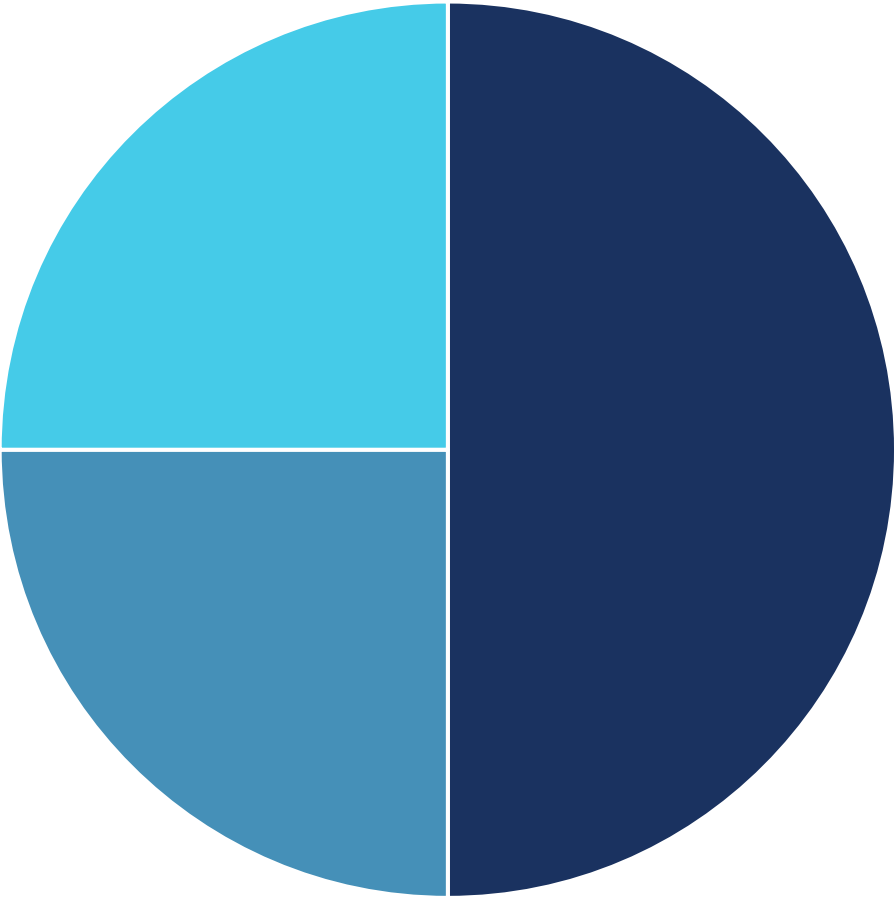
Comments:

- The requirements could be more precise not to give misleading observations, e.g. 'use secure passwords where possible'. It shall always be possible to use secure passwords.

---

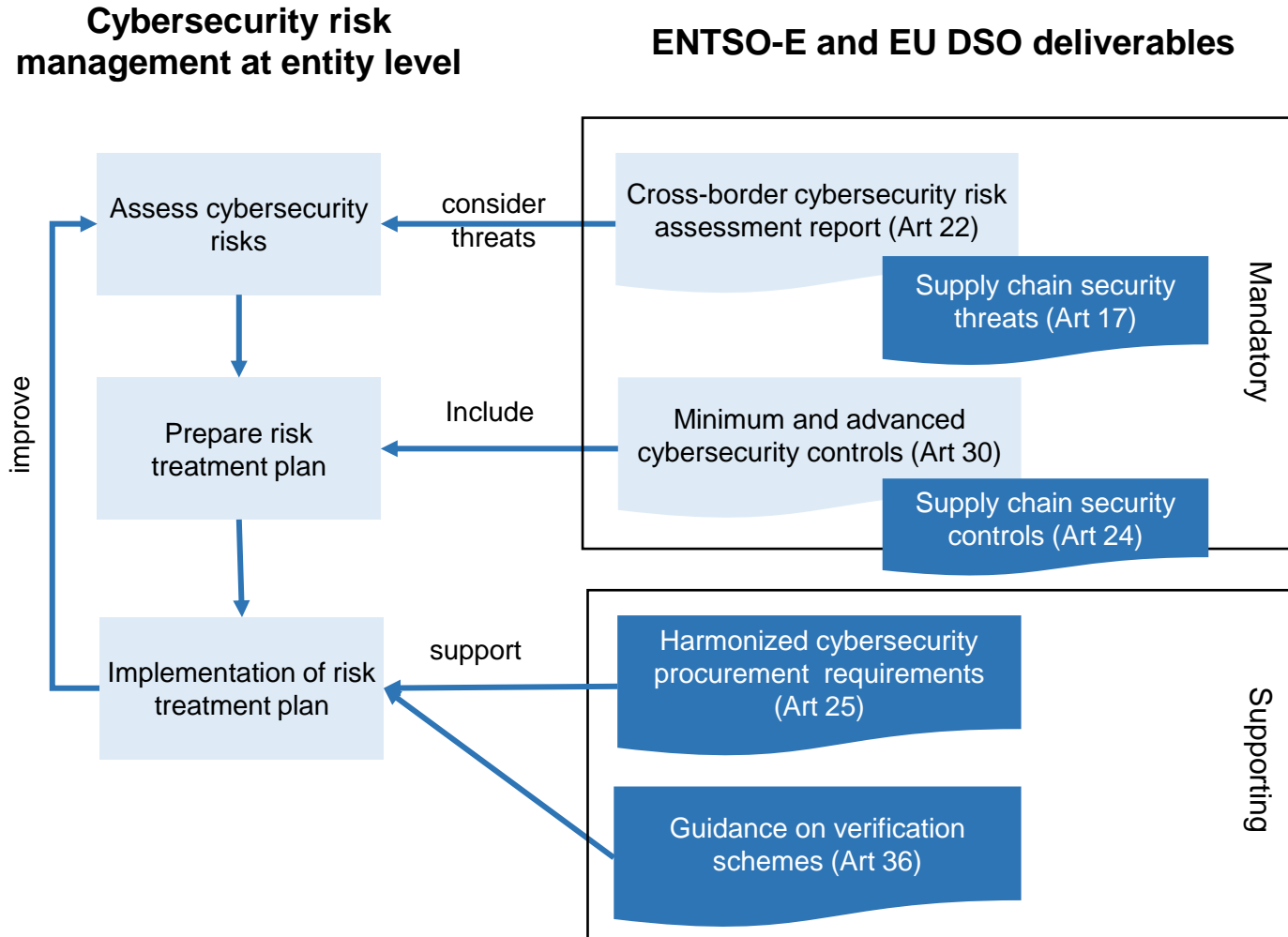
---

Is the proposed common electricity cybersecurity framework clearly described and sufficient to meet the objectives of the network code on cybersecurity?



■ Yes ■ No ■ No opinion

# INTEGRATED APPROACH TO SUPPLY CHAIN SECURITY

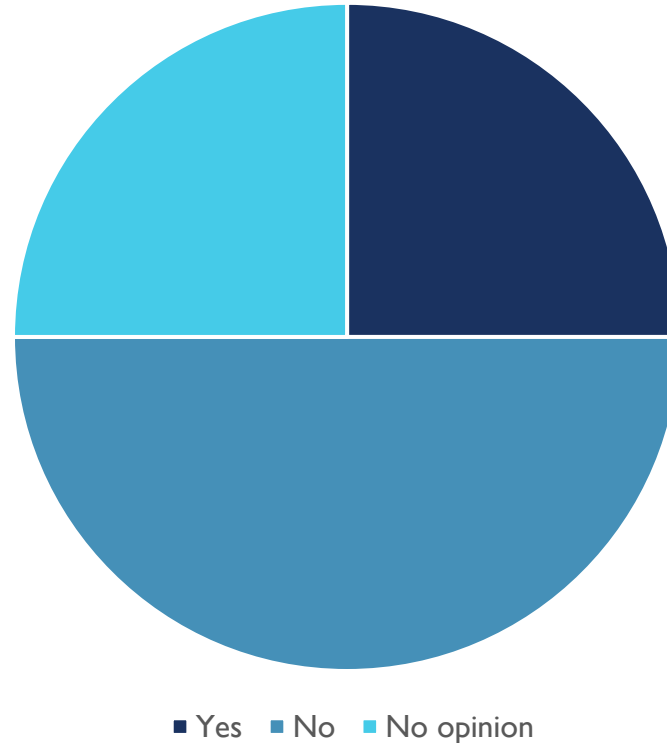




---

---

Are the minimum cybersecurity controls for supply chain security in Article 24 (2) clear and sufficient?



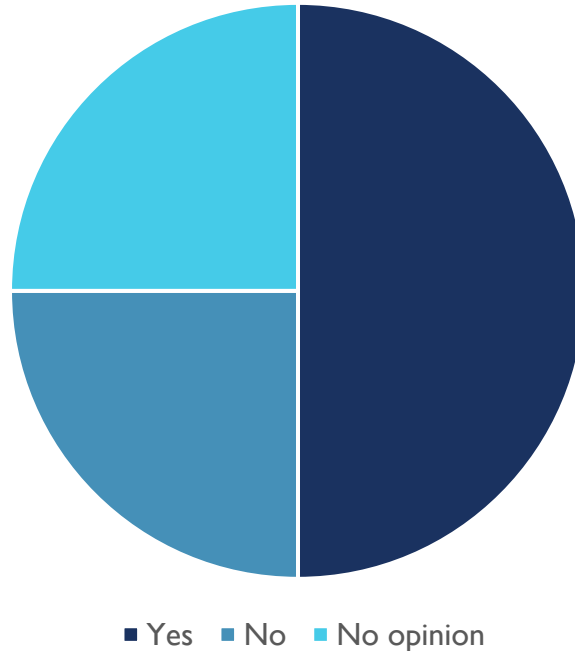
Comments:

- Certification should be optional. Other international certifications should be deemed as possible alternatives;
- Background verification checks of all supplier staff are neither possible nor realistic.

---

---

The supply chain controls now require entities procuring new products and systems to set and enforce security requirements to suppliers. Should the network code also include controls that directly require suppliers to take certain measures?



Comments:

- The procedures and exact requirements for product certification are unclear. Manufacturers and service providers must take full responsibility for the embedded products in their supply chain instead of shifting this responsibility to the operators/generators;
- A potential obligation of operators to use certified products is not practical.

# QUESTIONS & COMMENTS

CHRISTIANE GABBE & MAARTEN HOEVE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

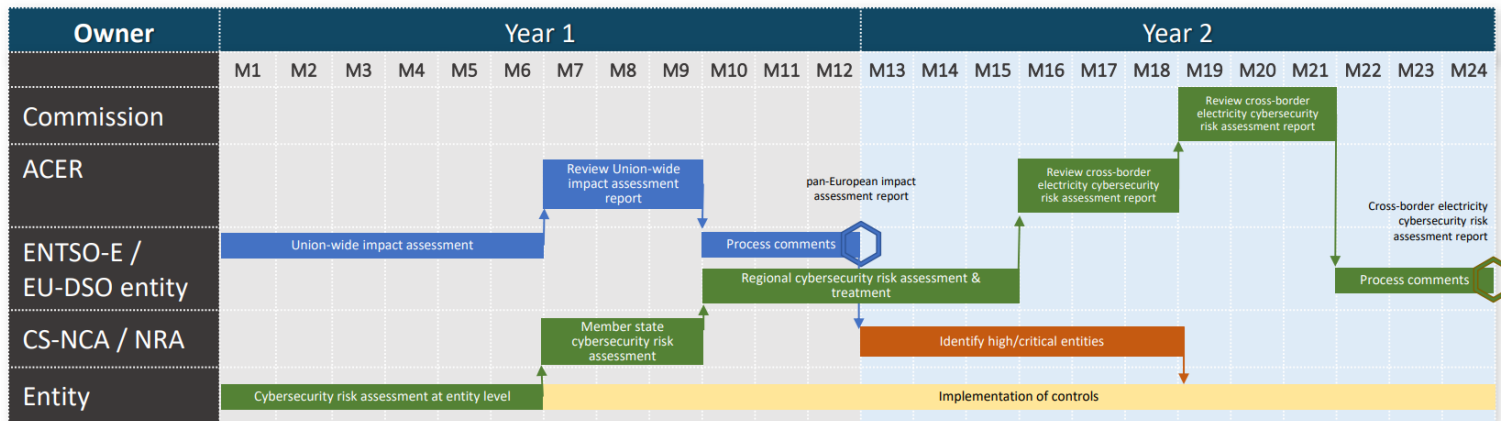
## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



# QUESTIONS

- **POLL:** Do you think cybersecurity hygiene requirements for SMEs should be included in the NCCS? (Yes/No)
- Do you see the added value of the cybersecurity electricity framework or do you think the use of a single certification scheme would better lead to a common baseline level of security?
- **POLL:** Do you think that peer-review is a valid tool for verification and audit of the minimum level of cybersecurity? (Yes/No)
- Do you think the timeline for the risk management on entity level is reasonable? If not – what timeline would be appropriate?



# SUPPLY CHAIN SECURITY - QUESTIONS

Article 24 contains a list of points to be covered by the minimum cybersecurity supply chain controls:

- What additional points should be included?
- Should the network code also directly require suppliers to take certain measures?

# TITLE VII: HARMONISING PRODUCT AND SYSTEM REQUIREMENTS AND VERIFICATION

MAARTEN HOEVE & DAIGA DEGE



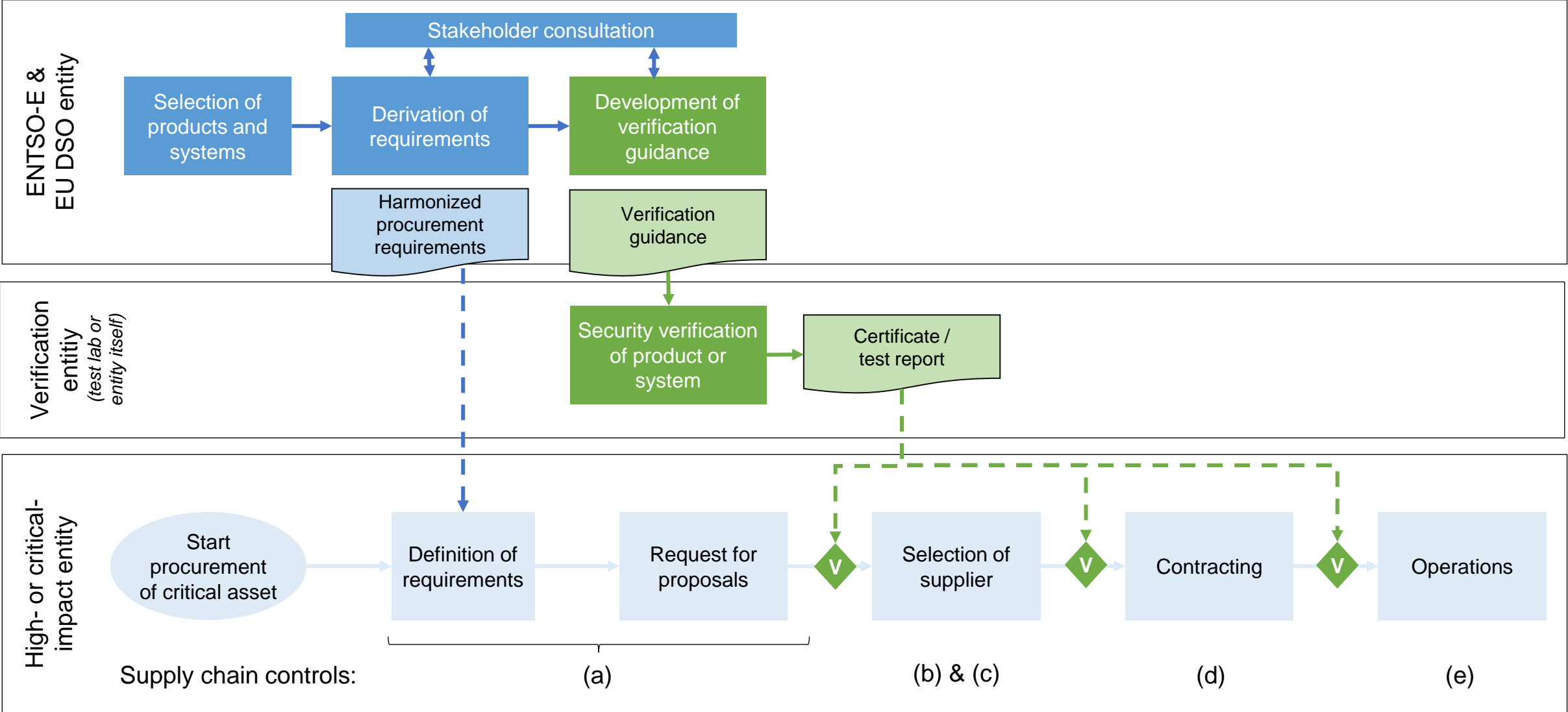
A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



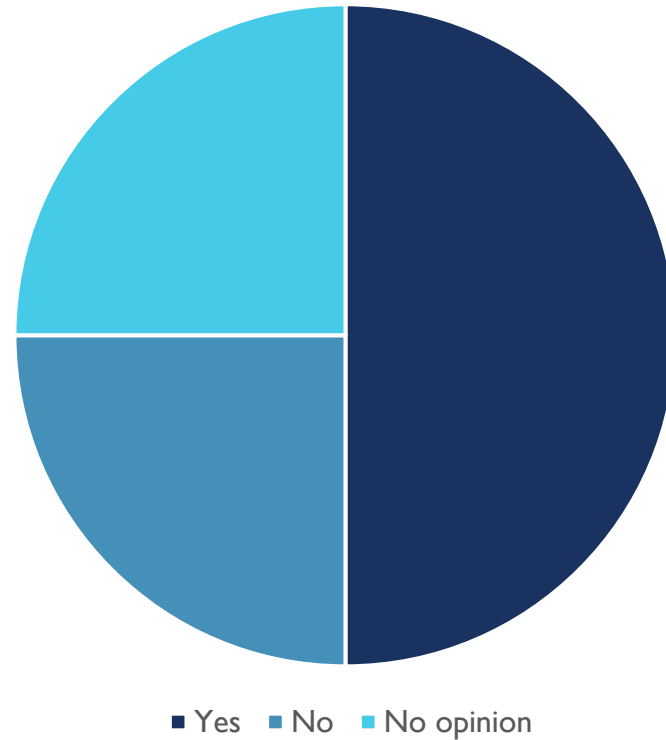
# HARMONIZED REQUIREMENTS AND VERIFICATION



---

---

Is the proposed approach for harmonizing the cybersecurity procurement requirements and verification schemes clearly described and sufficient to meet the objectives of the network code on cybersecurity?



Comments:

- Verification schemes still need to be developed and are therefore not clear by this point in time.



# QUESTIONS & COMMENTS

MAARTEN HOEVE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



# HARMONIZED REQUIREMENTS - QUESTIONS

Under the network code, ENTSO-E and the EU DSO entity will develop harmonized cybersecurity procurement requirements and guidance on verification and certification schemes

- How should the requirements and guidance be related to (international) standardization?

# TITLE VIII: ESSENTIAL INFORMATION FLOWS INCIDENT AND CRISIS MANAGEMENT

DAIGA DEGE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."

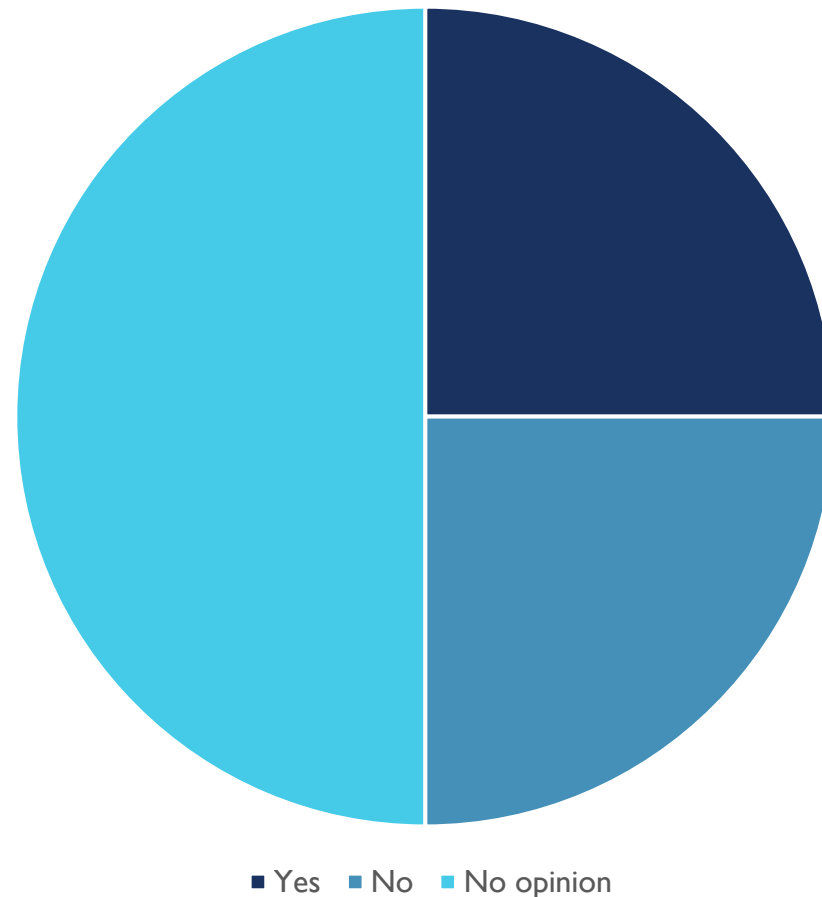


---

---

Article 37 request CS-NCA to provide electricity entities with information on cybersecurity incidents, threats, and vulnerabilities to enhance the electricity entities' defense.

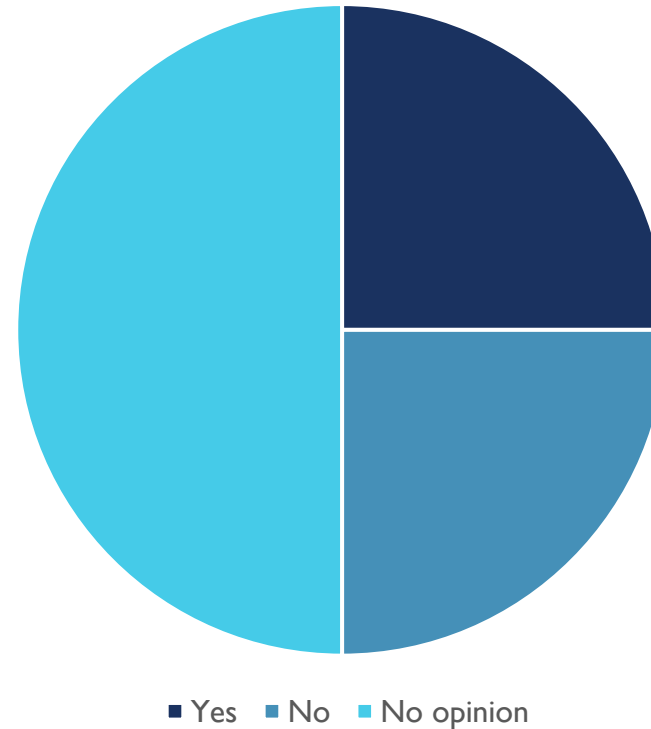
Do you agree that the network code will help electricity entities to receive effective and adequate information to increase their threat awareness and ability to handle cybersecurity incidents?



---

---

Article 39 and Article 40 present the support electricity entities receive in the event of an incident (Art.39) and crisis (Art.40).  
Do you think that enough support is provided?



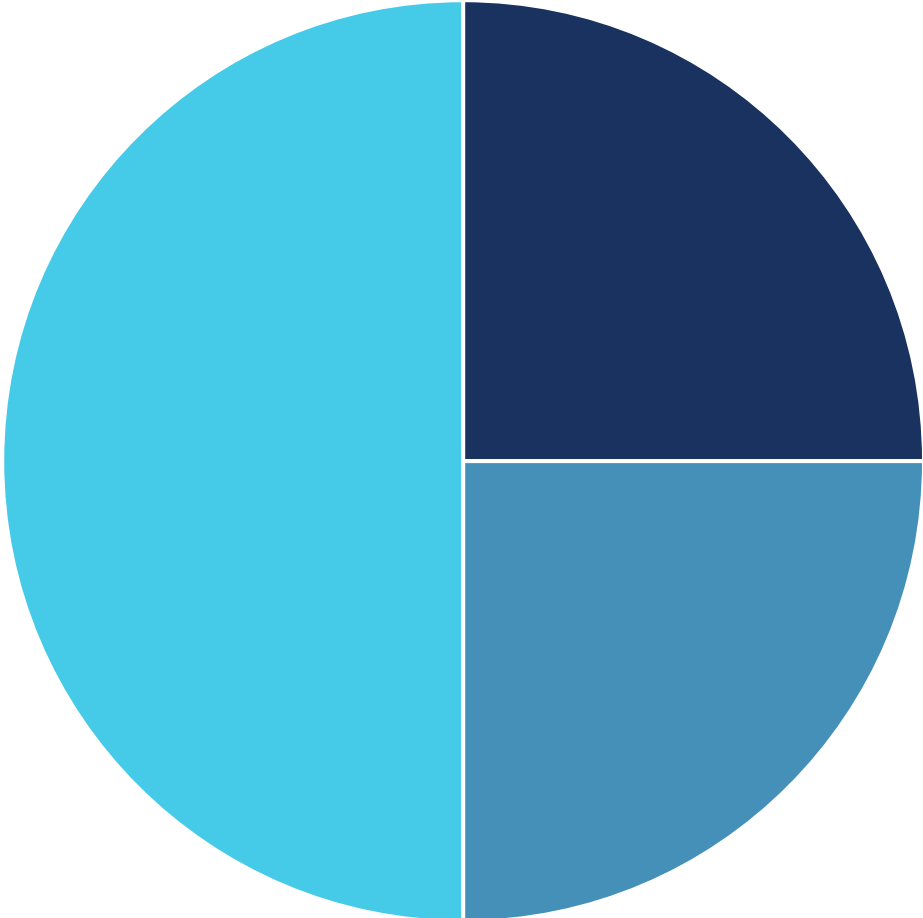
Comments:

- There should be a clear standardised standard/process in place.

---

---

Is the proposed approach for essential information flows and crisis management clearly described and sufficient to meet the objectives of the network code on cybersecurity?



■ Yes ■ No ■ No opinion

# QUESTIONS & COMMENTS

PETER PONGRACZ




A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



- 
- Art.38.1 requests high-impact and critical-impact entities to establish CSOC capabilities. Do you think establishing CSOC capabilities should be mandatory for high-impact entities?
  - Art.37.8 requests ENTSO-E to study - *within 2 years* - how a common tool could be effectively developed to facilitate information sharing between electrical entities and CSIRTs.  
Do you think such tool is:
    - a)urgent - it should be developed within the proposed 2 years
    - b)helpful but not essential
    - c)not necessary - this is a waste of time and money



# TITLE IX: ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

OLIVIER CLEMENT & DAIGA DEGE

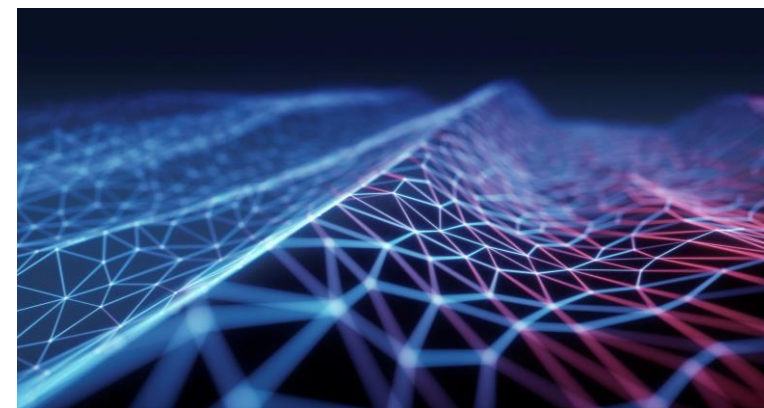


Reliable Sustainable Connected

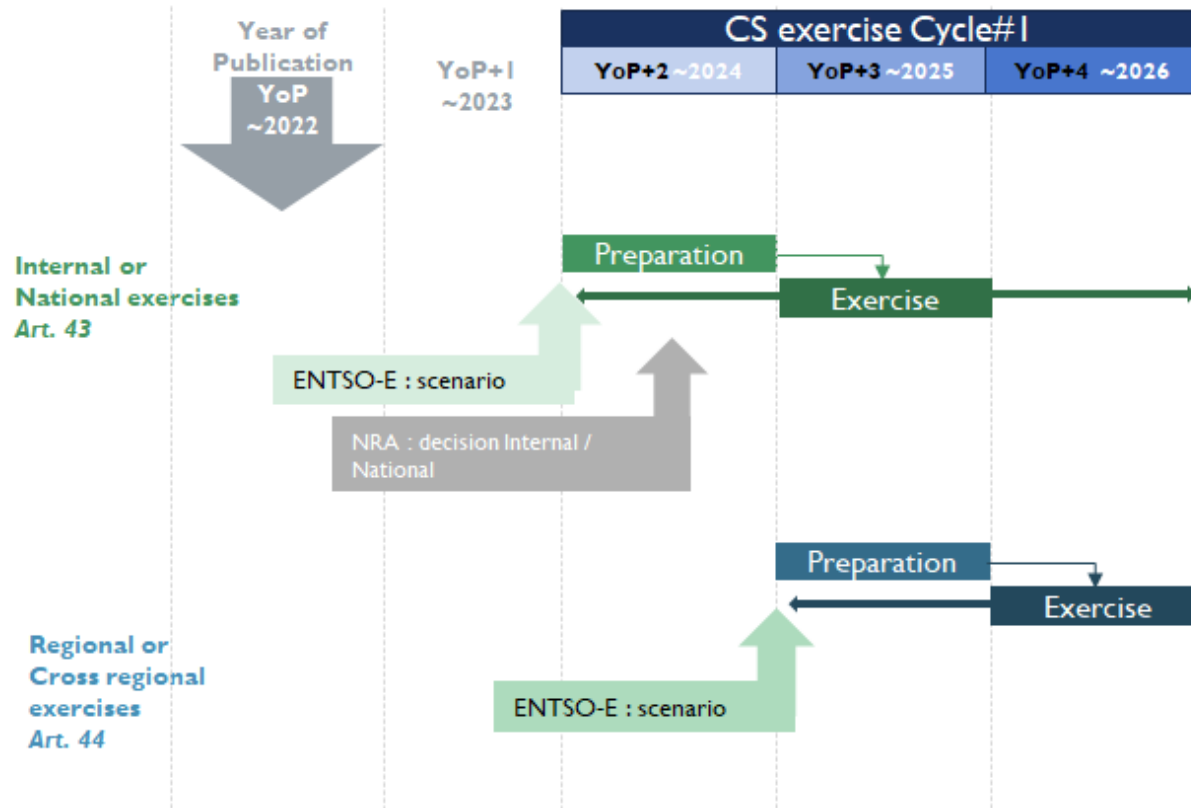
A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



# CYBERSECURITY EXERCISES : 2 EXERCISES EVERY 3 YEARS



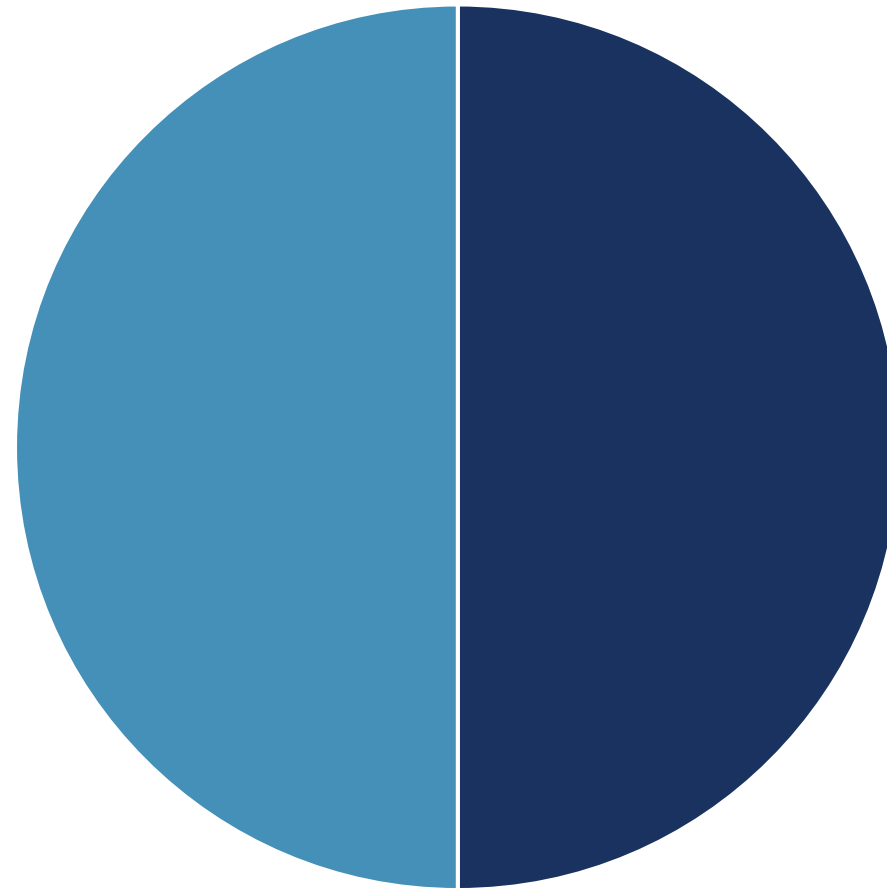
## Critical impact entities:

- shall organize and perform a cybersecurity at entity level every three years (Art.43.1) or by derogation shall participate to a national cybersecurity exercise (Art.43.2)
- Shall participate to a regional or cross regional exercise organized every three years (Art. 44.1)

---

---

Article 4I requires critical entities to perform two exercises every three years.  
Do you have the capabilities to perform the mandatory cybersecurity exercises?

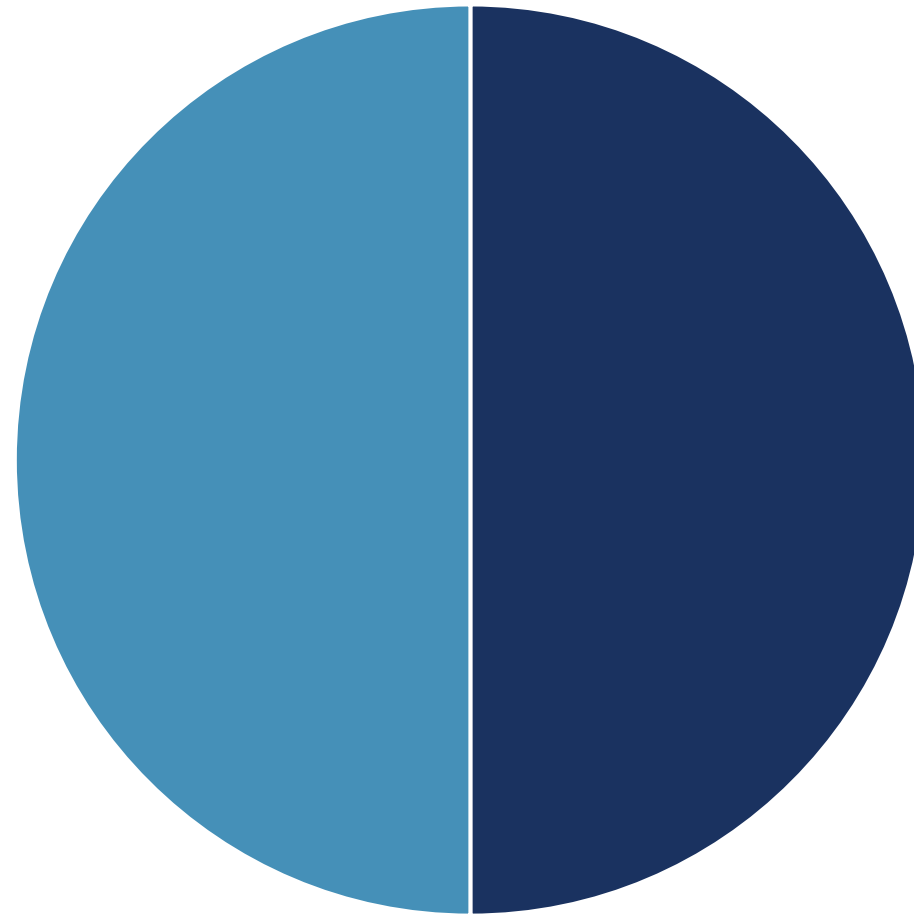


■ Yes ■ No opinion

---

---

Is the proposed electricity cybersecurity exercise framework clearly described and sufficient to meet the objectives of the network code on cybersecurity?



■ Yes ■ No opinion

# QUESTIONS & COMMENTS

OLIVIER CLEMENT




A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



- 
- Art.43.1 & 43.2 request critical-impact entities to participate in 2 exercises every 3 years: one internal or national exercise, and one regional or cross-regional exercise. This 3 years cycle requested by the Framework Guideline is not aligned with the 2 years risk assessment cycle (top-down & bottom-up cycle). Do you think these 2 cycles should be aligned?

# TITLE X: PROTECTION OF INFORMATION EXCHANGED IN THE CONTEXT OF THIS DATA PROCESSING

DAIGA DEGE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

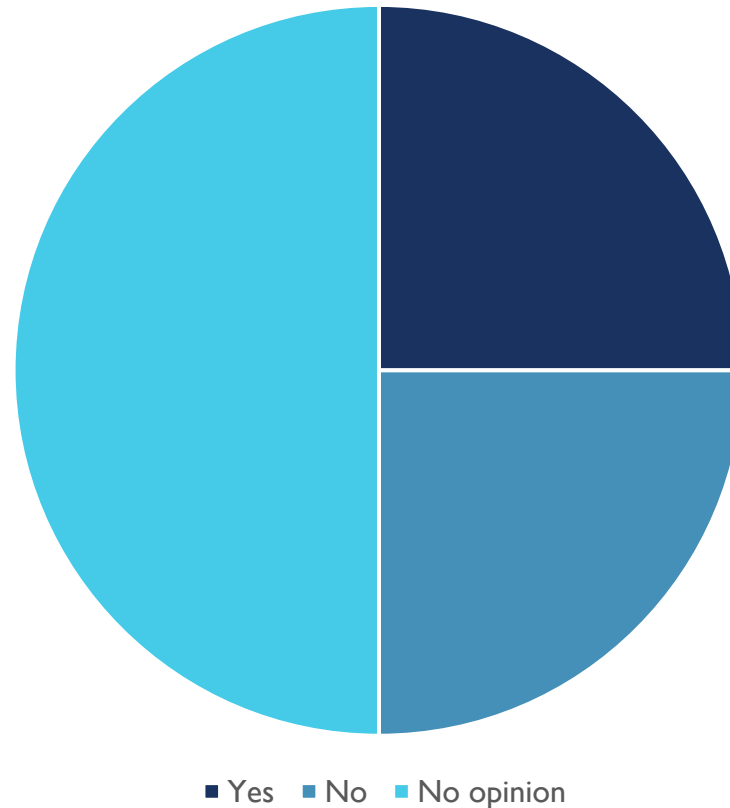
The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



---

---

Are the principles and implementation rules for protection of information adequate to protect classified and sensitive information to be exchanged in a trusted way?



Comments:

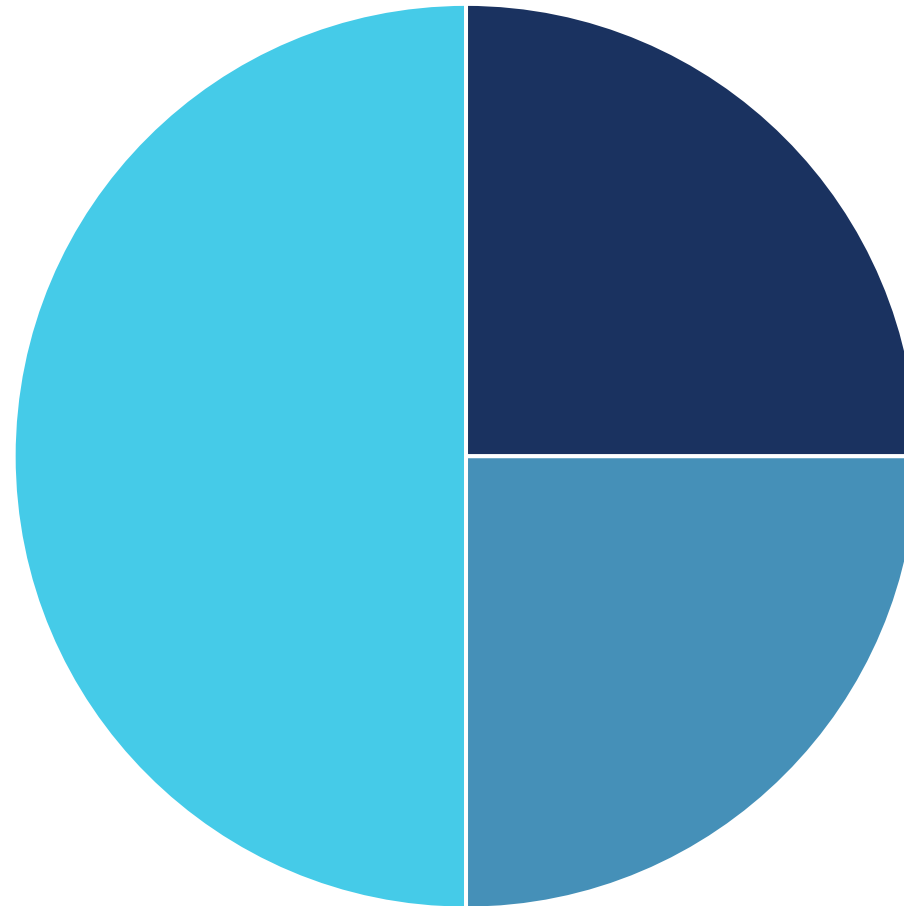
- It is important to note that national legislation may prohibit individual member states from being able to exchange this kind information.



---

---

Is the proposed protection of information exchanged in the context of this data processing clearly described and sufficient to meet the objectives of the network code on cybersecurity?



■ Yes ■ No ■ No opinion

# QUESTIONS & COMMENTS

OYSTEIN KORUM



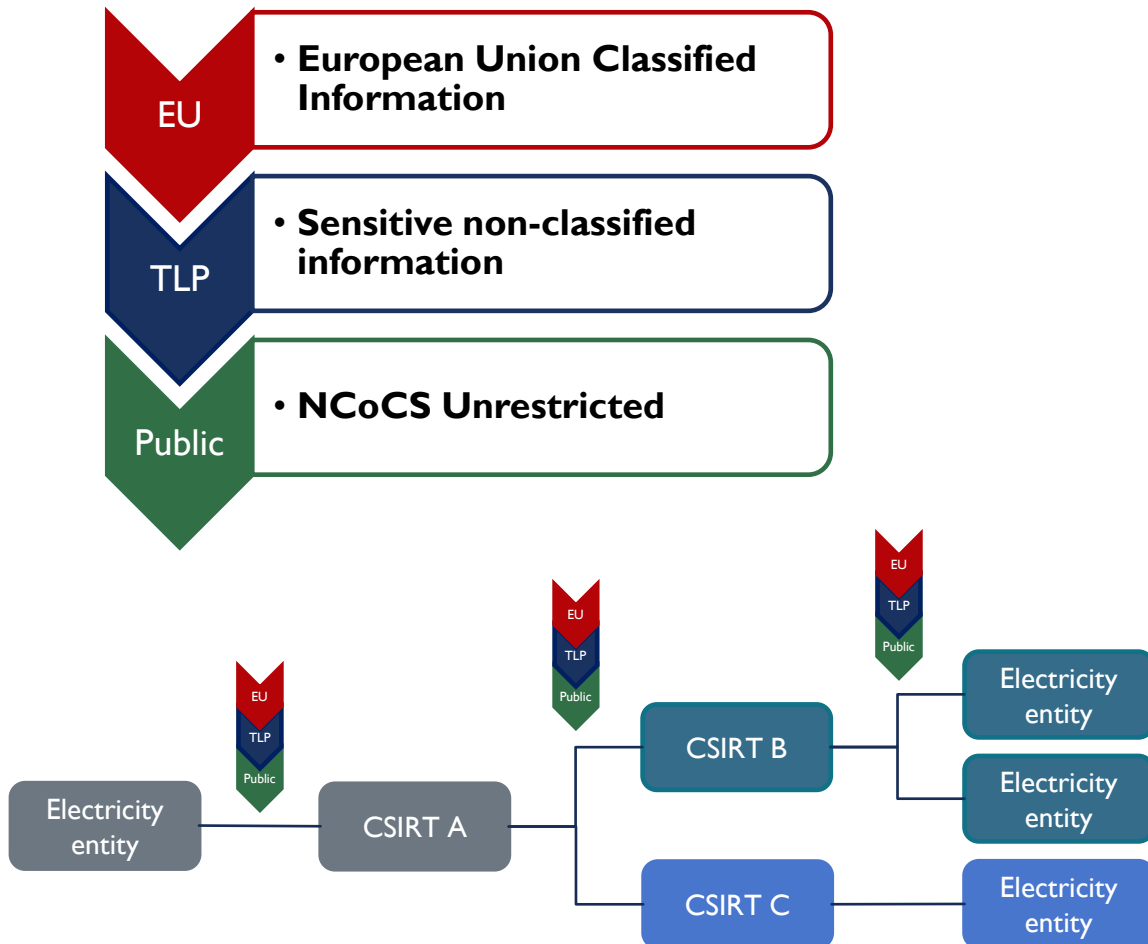
A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



## Q35. ARE THE PRINCIPLES AND IMPLEMENTATION RULES FOR PROTECTION OF INFORMATION ADEQUATE TO PROTECT CLASSIFIED AND SENSITIVE INFORMATION TO BE EXCHANGED IN A TRUSTED WAY?



In the context of title VIII (information sharing):

- each electricity entity sending information shall:
  - classify the information & determine the distribution restrictions (Art.48.1)
  - alert its CSIRT by clearly identifying specific information that could cause harm (Art.39.6)
- CSIRT shall anonymize and sanitize the information received (Art. 48.3) in order to avoid any harm

# GENERAL COMMENTS

DAIGA DEGE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOs)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



■ **Do you see any areas where the network code on cybersecurity can be aligned better with the revised NIS directive now under development?**

- No;
- Entities would have to report the same incident twice to two different authorities;
- The NIS2 editing process has not yet been completed. It is incomprehensible of why the editing process of the NC was not coordinated with the publication of the NIS2.

■ **Do you have any other comments you want to share and that are not included in the previous questions, with regard to the draft network code on cybersecurity?**

- all the production infrastructure should be standardised (checklist);
- all production infrastructure should be removed from the internet. All data in transit should be encrypted;
- Since many processes and measures are only developed after the NC has been published, the questions posed in the consultation can rarely be answered concretely.
- The recognition of existing processes and measures based on international and European standards as well as national laws is essential: There must be neither double regulation nor legal uncertainties in interpretation for the operators concerned. Recognised norms/standards/specifications and proven industry-specific regulations represent the state of the art and are preferable to be applied.
- The reporting of security incidents should focus on previously defined, serious IT security incidents with cross-border significance. Various reporting systems have already been put in place in individual countries. The forwarding of reports to the defined bodies should be ensured and multiple reports should be avoided.
- The further process after the publication of the NC must be carried out with the involvement of all stakeholders in public processes in order to ensure acceptance and the possibility of implementation in practice.

# NEXT STEPS

DAIGA DEGE



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



---

---

Workshop documents published in the homepage:  
[https://www.entsoe.eu/network\\_codes/nccs/](https://www.entsoe.eu/network_codes/nccs/)

Public Consultation ends on 10<sup>th</sup> December 2021

Drafting Team`s review of the Public Consultation  
comments & Legal review

Drafting Committee, ENTSO-E and EU DSO Entity  
final review & approval

Submission to ACER by 14<sup>th</sup> January 2022

# NETWORK CODE ON CYBERSECURITY

WORKSHOP: PUBLIC CONSULTATION, 8<sup>TH</sup>  
DECEMBER 2021



A NEW ASSOCIATION FOR THE EUROPEAN  
DISTRIBUTION SYSTEM OPERATORS (DSOS)

## The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."

