Regulatory Frameworks for Cyber Security in the Electricity Sector: the European path

G. Dondossola

Web – 24 march 2021

NIS Directive EU 2016/1148

CHAPTER I - GENERAL PROVISIONS

Article 5 Identification of operators of essential services

1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall **identify the operators of essential services** with an establishment on their territory.

- Energy: Electricity, Oil, Gas;
- Transport: Air transport, Rail transpor, Water transport, Road transport;
- Banking;
- Financial market infrastructures;
- Health sector;
- Drinking water supply and distribution;
- Digital Infrastructure: Internet Exchange Points, DNS service providers, Top Level Domain name registries

NIS Directive EU 2016/1148

CHAPTER I - GENERAL PROVISIONS

Article 5 Identification of operators of essential services

2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

(a) an entity provides a service which is **essential for the maintenance of critical societal and/or economic activities;**

(b) the provision of **that service depends on network and information systems;** and

(c) an incident would have **significant disruptive effects** on the provision of that service.

NIS Directive EU 2016/1148

CHAPTER I - GENERAL PROVISIONS

Article 6 Significant disruptive effect

1. When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following **cross-sectoral factors:**

(a) the **number of users** relying on the service provided by the entity concerned;

(b) the **dependency of other sectors** referred to in Annex II on the service provided by that entity;

(c) the **impact** that incidents could have, in terms of **degree and duration,** on economic and societal activities or public safety;

(d) the **market share** of that entity;

(e) the **geographic spread** with regard to the area that could be affected by an incident;

(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the **availability of alternative means** for the provision of that service.

NIS Directive EU 2016/1148

CHAPTER II

NATIONAL FRAMEWORKS ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

Article 9 Computer security incident response teams (CSIRTs)

1. Each Member State shall **designate one or more CSIRTs** which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, **responsible for risk and incident handling in accordance with a well-defined process**. A CSIRT may be established within a competent authority.

NIS Directive EU 2016/1148

CHAPTER IV

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES

Article 14 Security requirements and incident notification

1.Member States shall ensure that **operators of essential services** take **appropriate and proportionate technical and organisational measures** to **manage the risks** posed to the security of network and information systems which they use in their operations.

2.Member States shall ensure that operators of essential services take appropriate measures to **prevent and minimise the impact of incidents** affecting the security of the network and information systems used for the provision of such essential services, with a view to **ensuring the continuity of those services.**

NIS Directive EU 2016/1148

CHAPTER IV

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES

Article 14 Security requirements and incident notification

3.Member States shall ensure that operators of essential services **notify, without undue delay,** the competent authority or the CSIRT of incidents having a **significant impact on the continuity** of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any **cross-border impact** of the incident. Notification shall not make the notifying party subject to increased liability.

Cybersecurity Act Regulation (EU 2019/881)

TITLE III CYBERSECURITY CERTIFICATION FRAMEWORK

Article 46 European cybersecurity certification framework

1. The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a **harmonised approach at Union level** to European cybersecurity certification schemes, with a view to creating a digital single market for **ICT products, ICT services and ICT processes**.

Cybersecurity Act Regulation (EU 2019/881)

TITLE III CYBERSECURITY CERTIFICATION FRAMEWORK

Article 52 Assurance levels of European cybersecurity certification schemes

1. A European cybersecurity certification scheme may specify one or more of the following **assurance levels** for ICT products, ICT services and ICT processes: 'basic', 'substantial' or 'high'. The assurance level shall be **commensurate with the level of the risk** associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.

EUCC candidate certification scheme

[Cybersecurity Certification: EUCC Candidate Scheme — ENISA (europa.eu)]

- published by ENISA on July 2020
- based on Common Criteria (ISO/IEC 15408 and ISO/IEC 18045)

Network Codes and Data Exchanges

European Electricity Sector

The code families

Connection

- Requirements for Generators
- High Voltage Direct Current Connections
- Demand Connection Code

Operations

- Operations
- Emergency and Restoration

Market

- Forward Capacity Allocation
- Capacity Allocation & Congestion Management
- Electricity Balancing

cigre
For power system expertise

Network Code on Cybersecurity

ENTSO-E / EU DSO Draft – NC structure

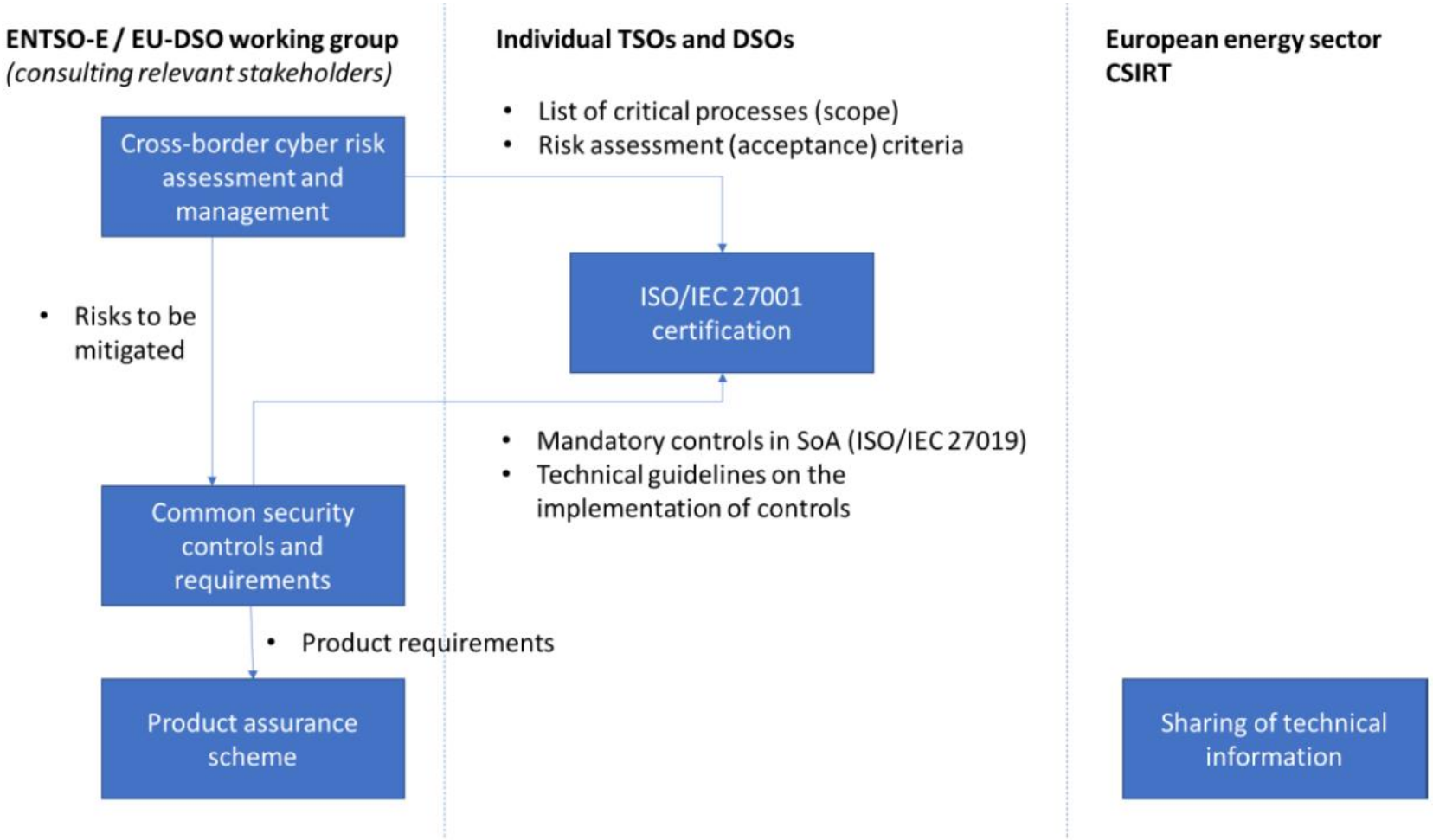
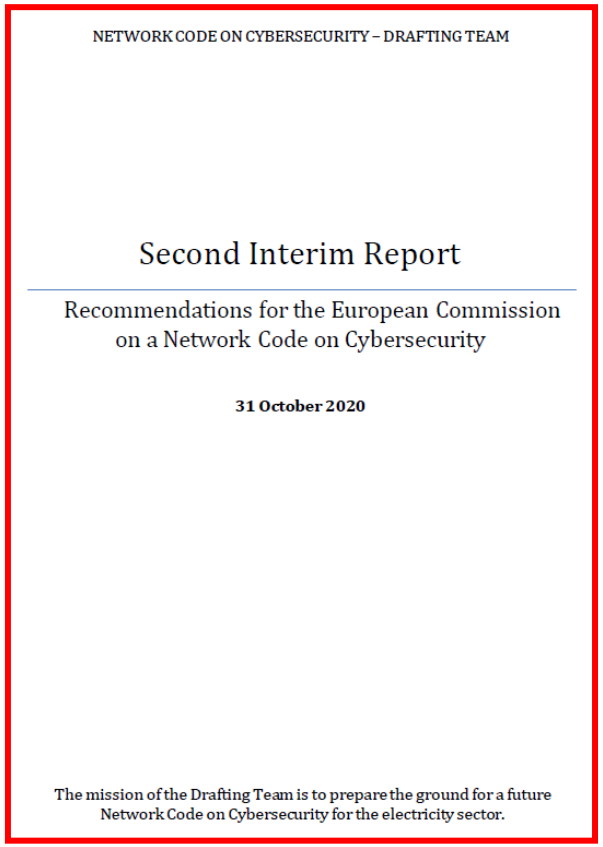


Figure 4 : NC Structure



NETWORK CODE ON CYBERSECURITY – DRAFTING TEAM

Second Interim Report

Recommendations for the European Commission on a Network Code on Cybersecurity

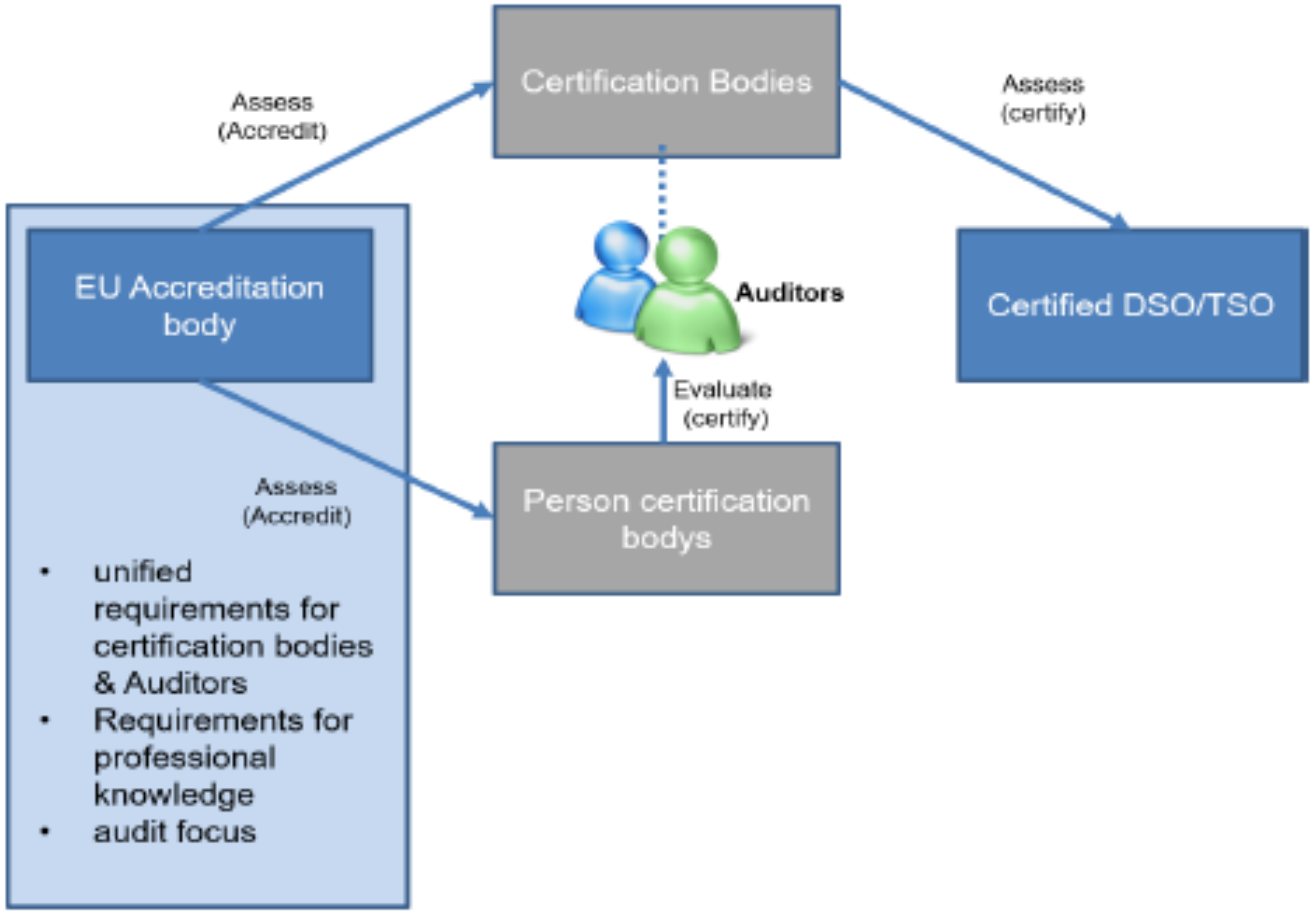
31 October 2020

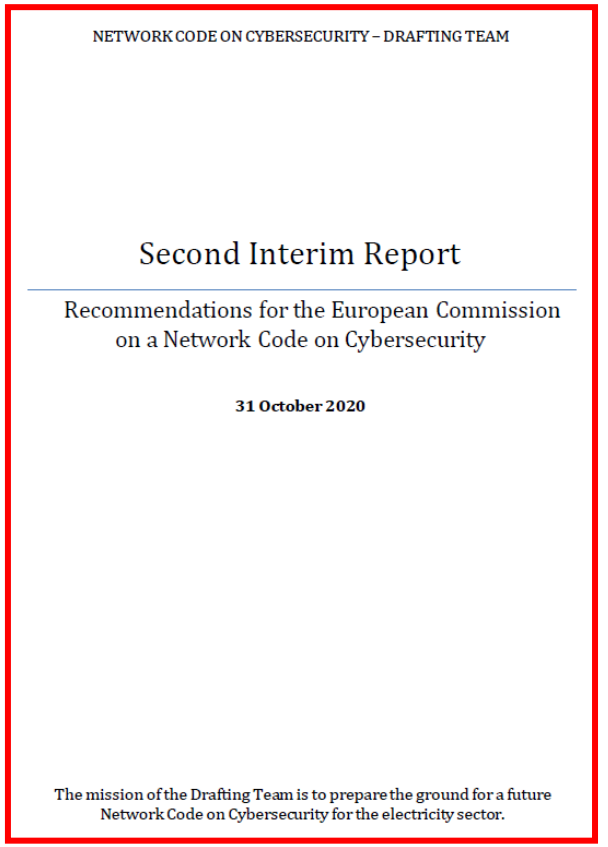
The mission of the Drafting Team is to prepare the ground for a future Network Code on Cybersecurity for the electricity sector.

cigre
For power system expertise

Network Code on Cybersecurity

ENTSO-E / EU DSO Draft – certification process





NETWORK CODE ON CYBERSECURITY – DRAFTING TEAM

Second Interim Report

Recommendations for the European Commission on a Network Code on Cybersecurity

31 October 2020

The mission of the Drafting Team is to prepare the ground for a future Network Code on Cybersecurity for the electricity sector.

cigre
For power system expertise

Common Security Controls

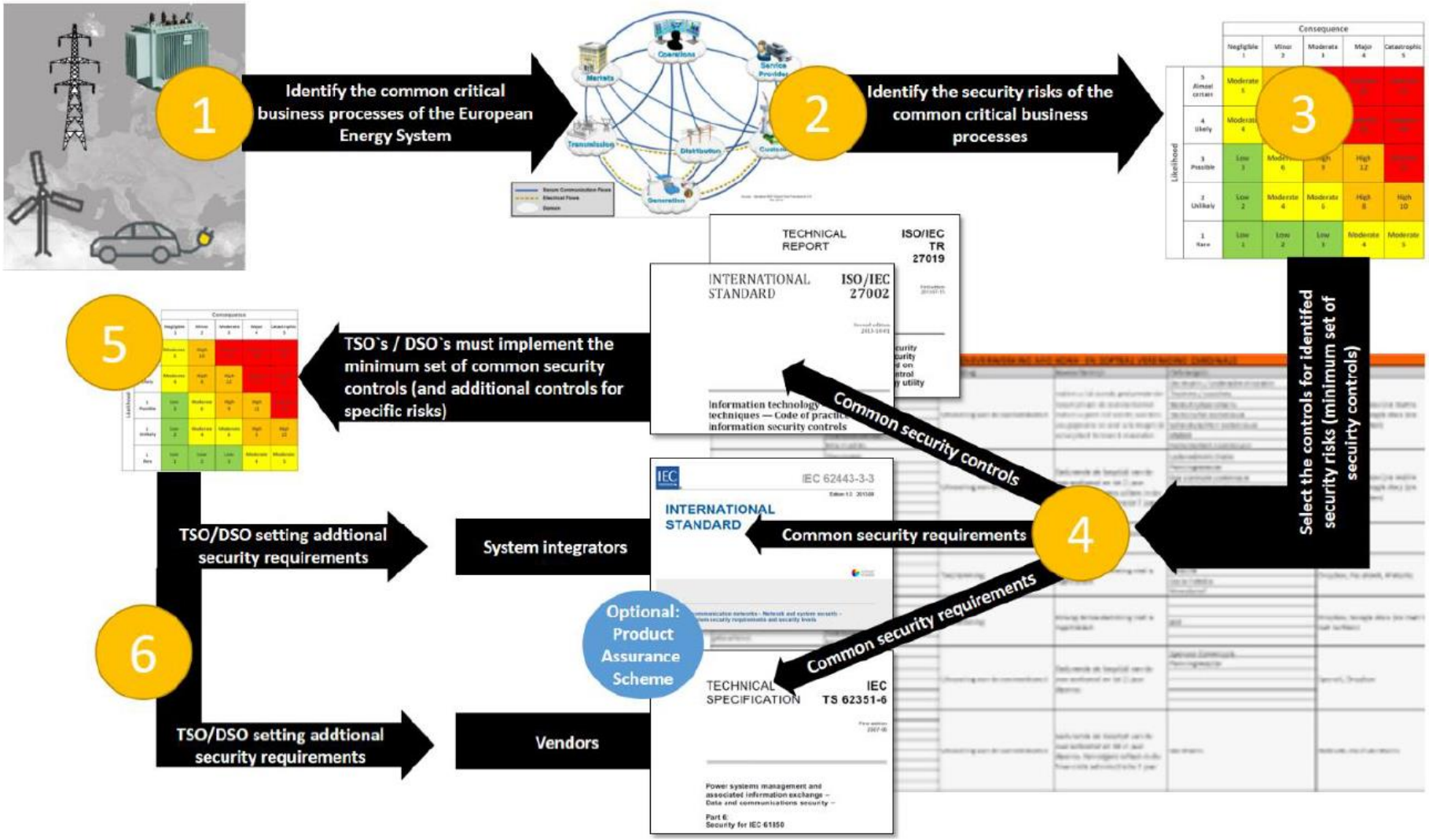


Figure 7 : Process to use the common security controls

Network Code on Cybersecurity

ENTSO-E / EU DSO Draft – NC structure

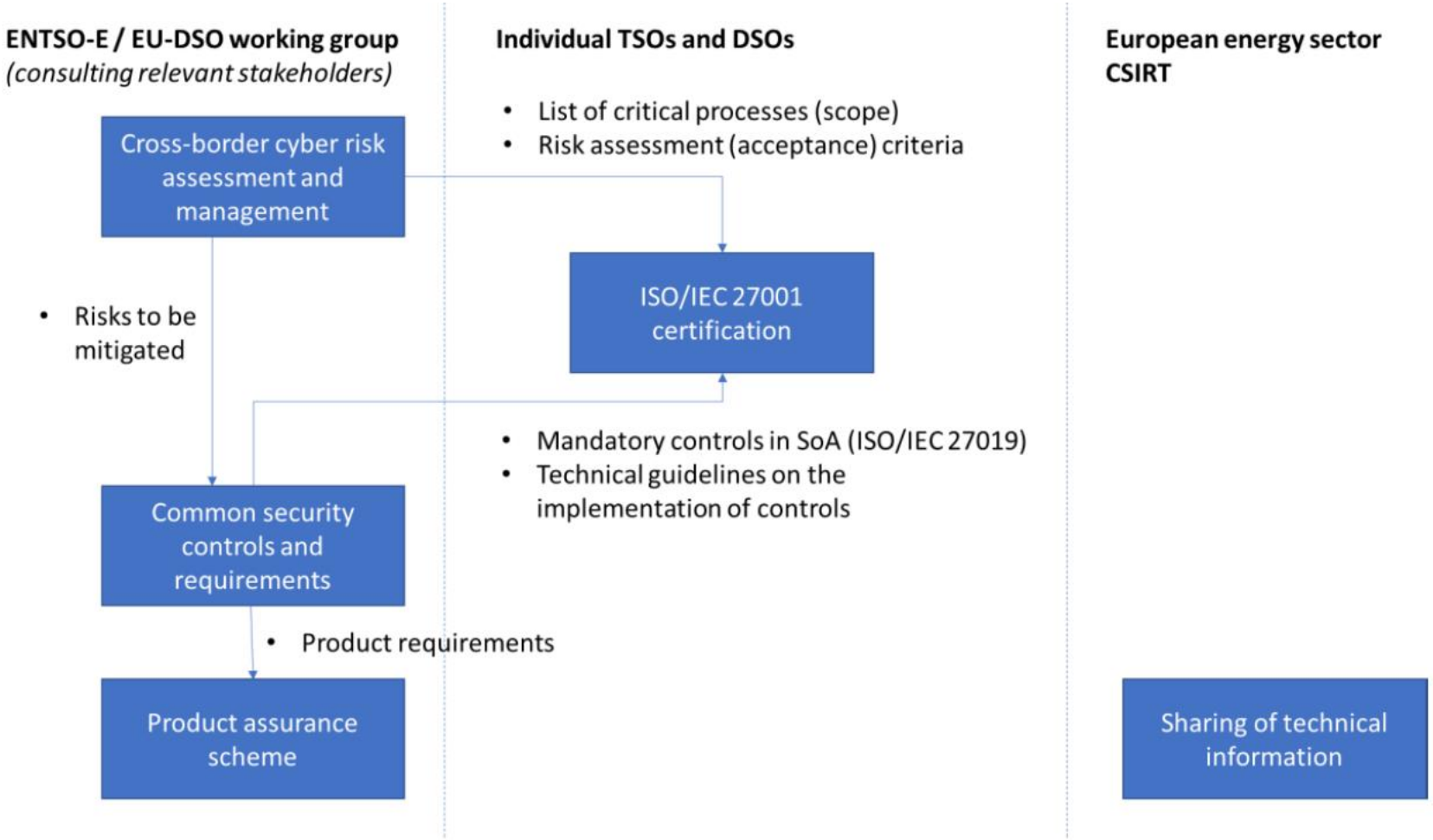
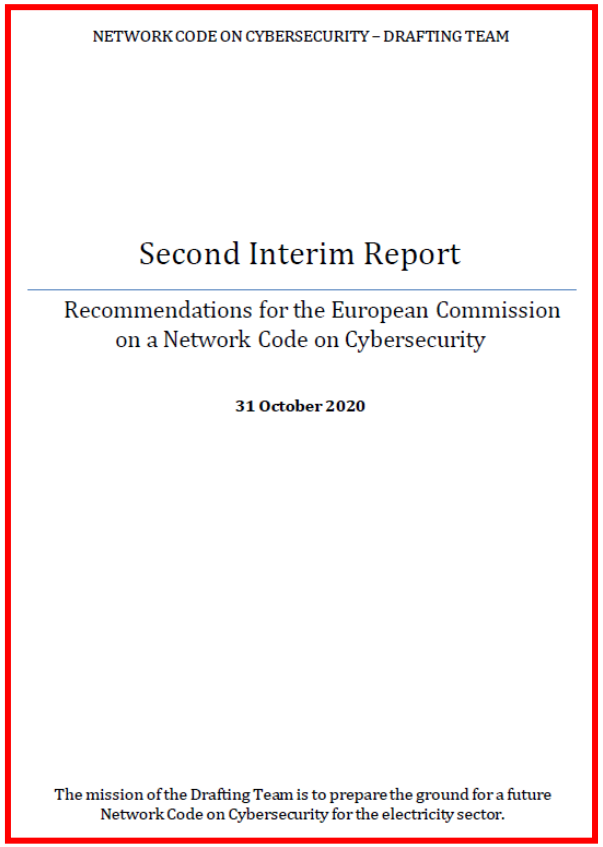


Figure 4 : NC Structure



NETWORK CODE ON CYBERSECURITY – DRAFTING TEAM

Second Interim Report

Recommendations for the European Commission on a Network Code on Cybersecurity

31 October 2020

The mission of the Drafting Team is to prepare the ground for a future Network Code on Cybersecurity for the electricity sector.

cigre
For power system expertise

Sources

1. NIS Directive EU 2016/1148 https://eur-lex.europa.eu/eli/dir/2016/1148/oj
2. the Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector from Energy Expert Cyber Security Platform (2017) https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
3. the Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity from the European Commission Smart Grid Task Force-Expert Group 2-Cybersecurity (2018) https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf
4. the European Commission Recommendation C(2019)2400 on cybersecurity in the energy sector https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf
5. the Cybersecurity Act Regulation (EU 2019/881) https://eur-lex.europa.eu/eli/reg/2019/881/oj
6. ENISA CYBERSECURITY CERTIFICATION (2020) Cybersecurity Certification: EUCC Candidate Scheme — ENISA (europa.eu)
7. ENTSO-E / EU DSO, «Recommendations for the European Commission on a Network Code on Cybersecurity», Second Interim Report, 31 October 2020
8. Clean Energy for all Europeans Package, European Union 2019

cigre
For power system expertise

Thank you

Giovanna.Dondossola@rse-web.it

cigre

For power system expertise