

Network Code on Cybersecurity

Briefing

25 August 2026

Introduction

The aim of this brief is to provide T&D Europe members with a concise overview of the [Network Code on Cybersecurity \(NCCS\)](#), which entered into force on 13 June 2024. It outlines the key obligations for technology providers arising from this regulation.

The NCCS, mandated by Article 59 of the [Electricity Regulation \(EU\) 2019/943](#), and the 2022 [EU Action Plan to Digitalize the Energy System](#), was adopted by the European Commission as a Delegated Regulation. Its goal is to ensure a high and harmonized level of cybersecurity of cross-border electricity flows in Europe.

The Network Code establishes sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management. It also provides a clear definition of the roles and responsibilities of the different stakeholders for each activity.

Scope and Applicability

The NCCS applies to several entities, including electricity undertakings as defined in Article 2(57) of [Directive \(EU\) 2019/944 on common rules for the internal market for electricity](#), that provides functions such as generation, transmission, distribution, aggregation, demand response, energy storage and supply, among others, that are identified as high-impact or critical-impact, based on the Electricity Cybersecurity Impact Index (ECII) and thresholds defined in the Union-wide cybersecurity risk assessment report.

The provisional ECII and high-impact and critical-impact thresholds have been published by ENTSO-E and the DSO Entity. As of the date of publication, those indicators are still recommendations and are not legally binding. The public document [can be found here](#).

The aforementioned entities can also include:

- Critical ICT Service Providers, meaning an entity, which provides an ICT service, or an ICT process that is necessary for a critical-impact or high-impact process affecting cybersecurity aspects of cross-border electricity flows.
- Managed Security Service Providers (MSSP), meaning a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management. Note that no provisional ECII are defined for managed security service providers.
- Entities that are not established in the Union but deliver services to entities in the Union.

Each competent authority may identify additional entities in its Member State as high-impact or critical-impact, if the entity is part of a group of entities for which there is a significant risk that they will be affected simultaneously by a cyber-attack, and if the ECII aggregated over the group of entities is above the high-impact or critical-impact thresholds.

Key Provisions

The Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows are structured in eight chapters with 49 articles.

- Chapter I „GENERAL PROVISIONS” defines the scope of the NCCS, the involved parties as well as modes and rules of the cooperation to be established. Article 6 outlines the terms and conditions of methodologies that the TSOs in cooperation with the EU DSO Entity must prepare, together with proposals for the regional cybersecurity risk mitigation plans, following by the approval and adoption by ACER and the competent authorities. Articles 9 and 10 defines the stakeholder involvement in the process and the required public consultation.

- Chapter II “RISK ASSESSMENT AND IDENTIFICATION OF THE RELEVANT CYBERSECURITY RISKS” focuses on the risk assessment. In Article 18, the high-level cybersecurity risk assessment methodologies are described. The risk assessment shall have different levels: the Union-wide level; the member state level; and the regional level (Articles 19-21). Article 24 outlines the identification of the high-impact and critical impact entities by the competent authorities.
- Chapter III “COMMON ELECTRICITY CYBERSECURITY FRAMEWORK” outlines the common technical requirements, process requirements and requirements for the supply chain that shall be developed based on voluntary selected European and international standards. Article 33 covers the minimum and advanced cybersecurity controls in the supply chain that mitigate the supply chain risks identified in the Union-wide cybersecurity risk assessments.
- Chapter IV “CYBERSECURITY PROCUREMENT RECOMMENDATIONS” focuses on procurement recommendation and addresses the supply chain security. Under Article 35, the TSOs in cooperation with ENTSO-E and the EU DSO Entity shall develop sets of non-binding cybersecurity procurement recommendations for high-impact and critical-impact entities. Recommendations should be consistent across regions. Procurement must follow established principles and align with the latest relevant European cybersecurity certification schemes for ICT products, services, or processes.
- Chapter V “INFORMATION FLOWS, CYBER-ATTACKS AND CRISIS MANAGEMENT” covers the management of cyberattacks. Article 37 defines the information flows between the competent authorities in the Union in case of an incident.
- Chapter VI “ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK” defines requirements for cybersecurity exercises on member state and entity level. The exercises shall be executed in a three-year cycle (Article 44).
- Chapter VII “PROTECTION OF INFORMATION” addresses the principles for the protection of the exchanged information and the confidentiality of this information (Articles 46-47).

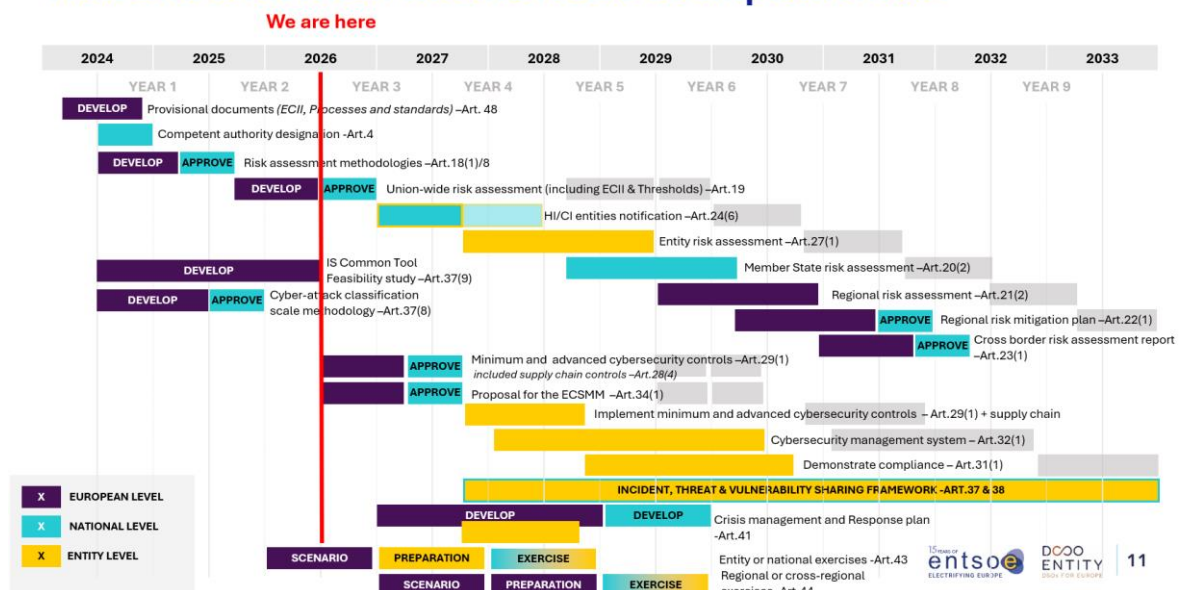
- Ultimately, chapter VIII “FINAL PROVISIONS” defines the temporary provisions and the enforcement (Articles 48-49).
- The development and implementation of the entire NCCS covers a timeframe reaching from 2024 to beyond 2031. After this, activities like risk assessments and cybersecurity exercises move into periodic schedules.

Implementation milestones

Given the scope, the NCCS implementation is planned to take multiple years. The current target is for it to be completed by the year 2033.

The overall implementation milestones are shown in the Figure below.

How and until when will the NCCS be implemented?



Enforcement and Penalties

The NCCS does not specify enforcement or penalties – these are only addressed in Article 66 of [Regulation \(EU\) 2019/943](#) on the internal electricity market.

Article 66 requires each member state to establish penalties for violating the regulation, including the Network Code on Cybersecurity mentioned in Article 59.

Penalties for non-compliance with the EU Network Code on Cybersecurity should not exceed 1% of a utility's total turnover from the previous year.

Impact on Grid technology manufacturers

Following the EU NCCS implementation, it is expected that TSOs and DSOs will develop minimum and advanced cybersecurity controls (Article 33).

The minimum and advanced cybersecurity controls in the supply chain shall cover at least the following aspects for the manufacturers:

- Execution of background verification checks of the supplier involved in the supply chain, and when dealing with sensitive information or with access to the high-impact or critical-impact assets of the entity → Article 33(2)(a)(i)
- Implementation of secure processes for development, production and appropriate technical measures → Article 33(2)(a)(ii)
- Secure network and information systems design, following the least privilege principle → Article 33(2)(a)(iii)
- Secure supplier management for the sub-supplier → Article 33(2)(a)(vi)
- Support of security updates throughout the entire lifetime of products, services or processes → Article 33(2)(a)(viii)
- Right of supplier audits for design, development, production and risk profile → Article 33(2)(a)(ix) & Article 33(2)(a)(x)
- Requirements for suppliers shall also be fulfilled by all sub-suppliers → Article 33(2)(b)
- Consider risk assessment results required by the NCCS in the supply chain → Article 33(2)(c)
- Criteria to select and contract the supplier, and criteria to reduce the risk of vendor lock-in → Article 33(2)(d) & Article 33(2)(e)

- Certification according to the European cybersecurity certification scheme or adequate verification from an entity. This measure is valid for critical-impact entities only. → Article 33(4)

Under Article 35, the TSOs in cooperation with ENTSO-E and the EU DSO Entity shall develop sets of non-binding cybersecurity procurement recommendations that high-impact and critical-impact entities may use as a basis for the procurement of ICT products, services and processes in the high-impact and critical-impact perimeters.

This will lead to a harmonized baseline set of technical and process requirements based on the non-binding cybersecurity procurement recommendations.

T&D Europe recommendations for manufacturers of grid technology

The Network Code on Cybersecurity will change the market dynamics around cybersecurity needs and create opportunities for new solutions and services. It is T&D Europe's understanding that suppliers will need to evolve and prepare to support grid operators even more on their journey to a higher level of cybersecurity in Europe.

T&D Europe's recommendation to its members is to take appropriate preparatory measures to prevent a shortage of skills, products and solutions during this transition period, where demand for qualified professionals and secure solutions will increase.

So far, the most relevant measures to consider that have been identified are the following:

- Understand the high-impact and critical-impact processes, published in the provisional list of Union-wide high-impact and critical-impact processes
- Identify what are the technologies provided by your organization to support the critical-impact and high-impact processes and take appropriate measures following your internal risk assessment. The recommended cybersecurity framework should incorporate internationally recognized standards, including ISO/IEC 27000, IEC 62443, and IEC 62351.

- Ensure that products commercialized for the sector have an adequate cybersecurity level to the risk anticipated and follow a certified secure development lifecycle
- Review the supply chain requirements for high-impact and critical-impact entities and ensure an appropriate level of compliance and a mapping of your current cybersecurity organizational measures
- Intensify cybersecurity educational campaigns targeting engineering teams with a specific focus on cybersecure solutions regarding engineering, testing, deployment and commissioning
- Prepare for supporting coordinated cybersecurity exercises with selected customers
- Prepare with service teams the support needed for the installed base