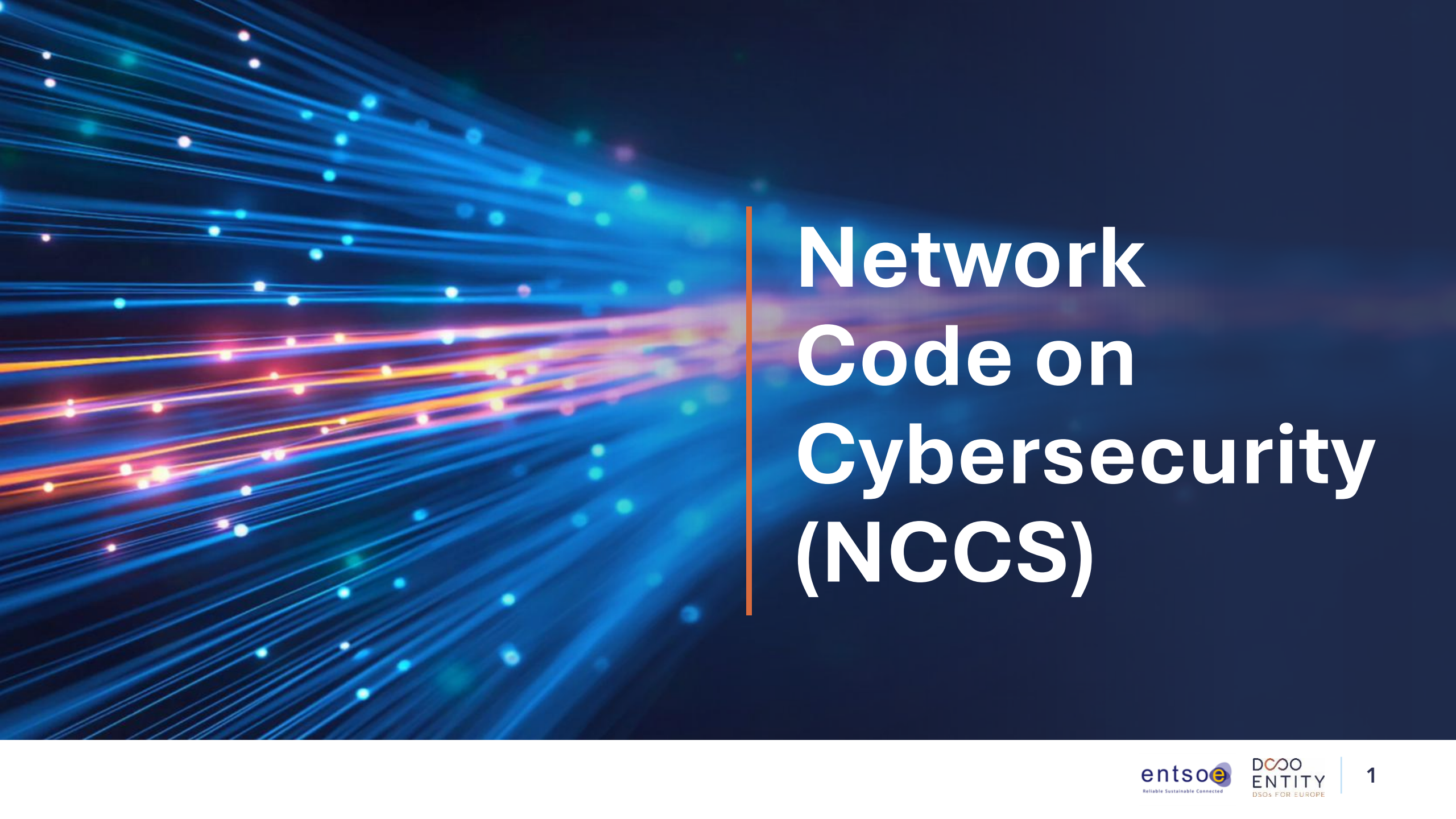




Network Code on Cybersecurity (NCCS)

Agenda

In this presentation, we will give an overview of the methodologies and provisional documents developed in the first year of the NCCS, and the next steps in the implementation

1. [General background](#)
2. [Risk assessments](#)
3. [Cyber-attacks and information flows](#)
4. [Supply chain controls and procurement recommendations](#)

1

General background

Why a network code on Cybersecurity (NCCS)?

1

Electricity is vital for European citizens and businesses

2

The interconnected European electricity grid is unique

3

The digitalisation is creating new risks and vulnerabilities

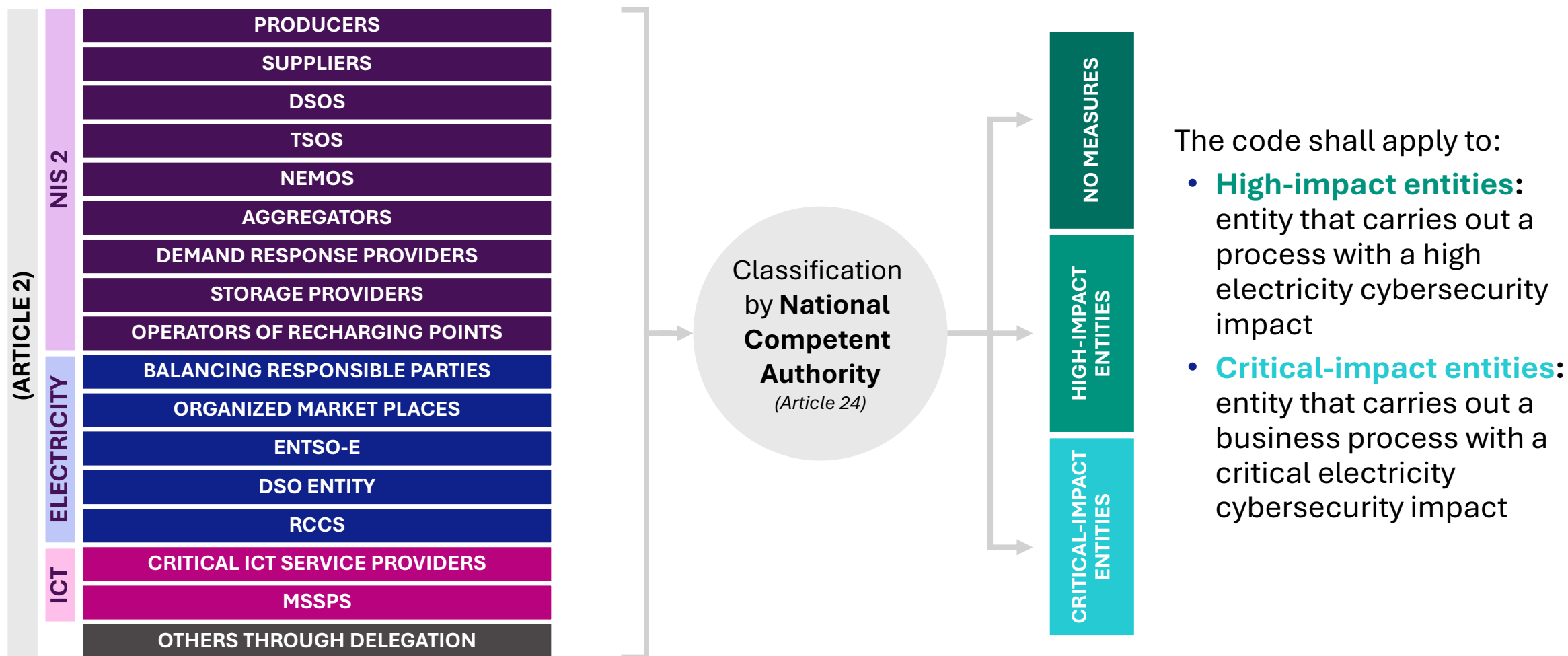
What is the NCCS' Regulatory Background?

Delegated Act by the European Commission
→ directly **applicable and legally binding in all EU Member States**.

NCCS lays down **sector-specific rules** for **cybersecurity** aspects of cross-border electricity flows.

NCCS **complements other European cyber security legislations (e.g. NIS-2)**, whenever cross-border electricity flows are concerned.

Which entities are in scope of the NCCS?



Who is responsible for the governance of the NCCS?

National Level:

**NATIONAL COMPETENT
AUTHORITIES (NCCS-NCA)**

**NATIONAL REGULATORY
AUTHORITIES (NRA)**

NIS COMPETENT AUTHORITIES

**COMPETENT AUTHORITIES FOR RISK
PREPAREDNESS (RP-NCAS)**

**COMPETENT AUTHORITIES RESPONSIBLE FOR
CYBERSECURITY (CS-NCAS)**

**COMPUTER SECURITY INCIDENT RESPONSE
TEAMS (CSIRTS)**

Regional Level:

**REGIONAL
COORDINATION
CENTERS (NEW)**

EU Level:

ENTSO-E

DSO ENTITY

ACER

ENISA

DG ENERGY

DG CONNECT

NEMOS



Energy related bodies



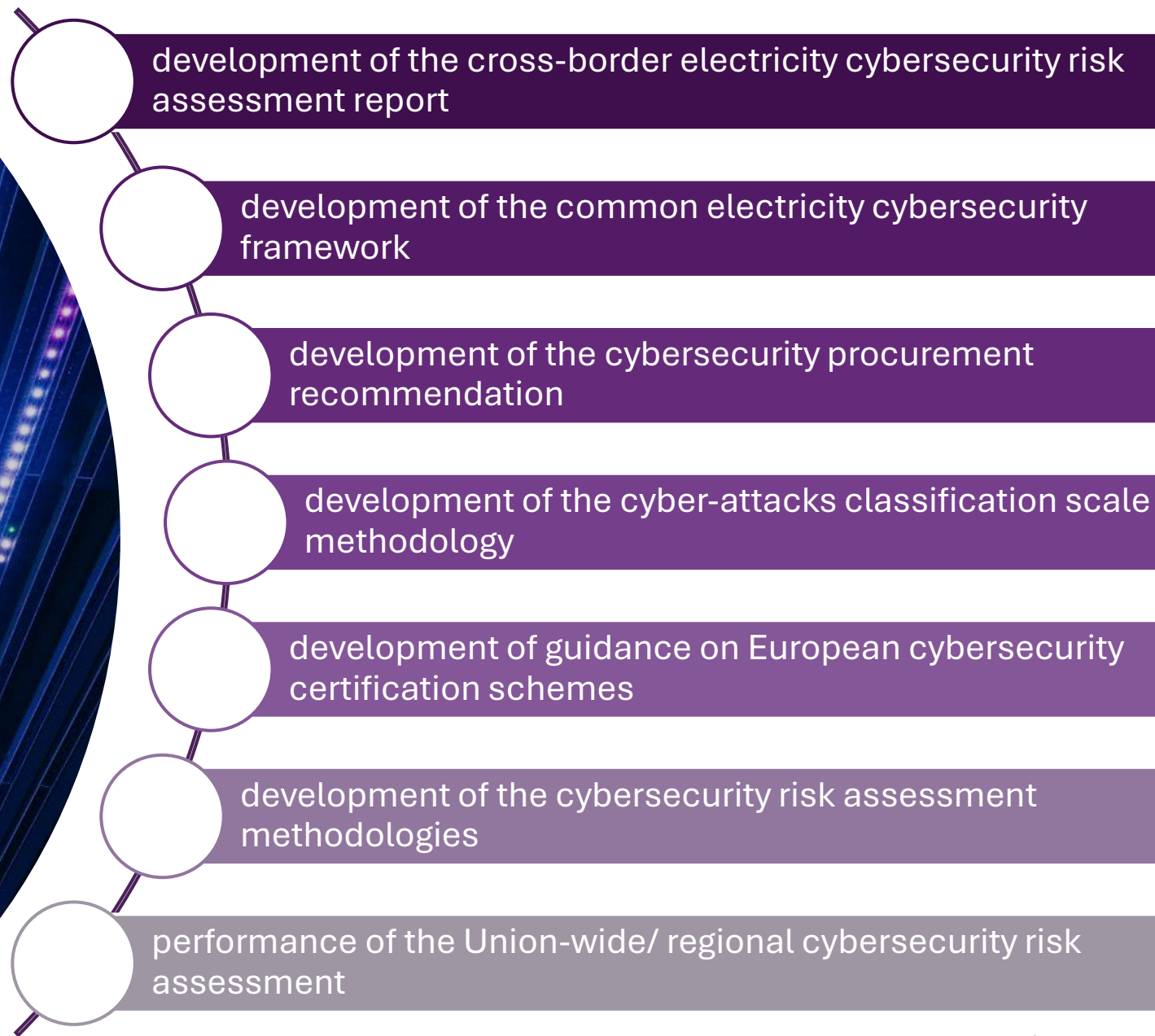
Cybersecurity related bodies

Who are National Competent Authorities (NCCS-NCAs)?

- A national governmental or regulatory authority **responsible** for carrying out the tasks assigned to it in the NCCS (*Art. 5*).
- Designated by each member state **six months** after entry into force (*Art. 5*).
- They **shall coordinate and cooperate** with cybersecurity competent authorities, NRAs, RP-NCAs, CSIRTs and other authorities determined by each Member State to ensure fulfilment of NCCS and avoid duplication of tasks (*Art. 5*).
- The competent authorities **may delegate tasks** to other national authorities (*Art. 4*).
- They **may perform inspections** of critical-impact entities according to national law to verify their compliance to the NCCS (*Art. 25*)

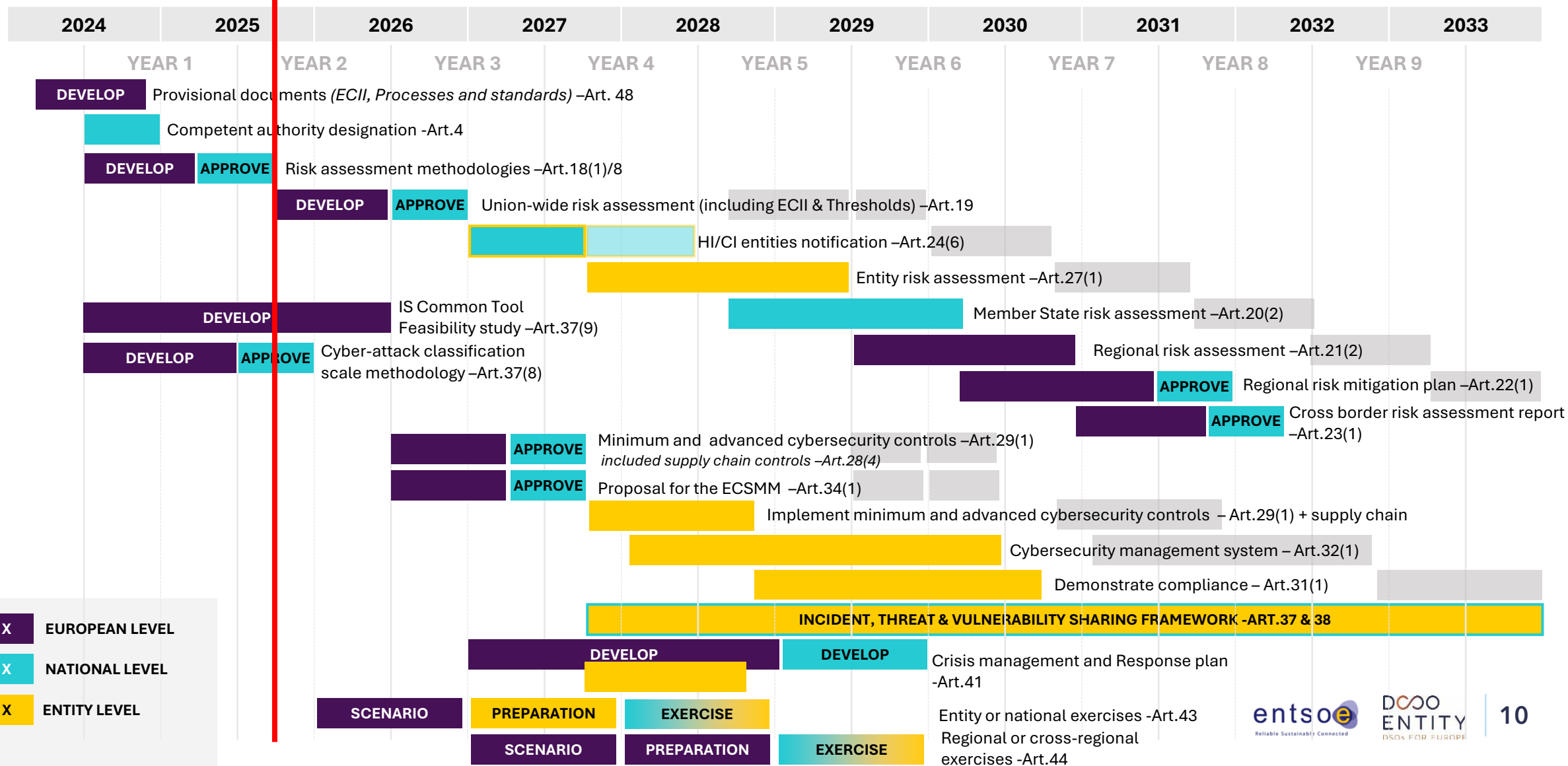
ENTSO-E and DSO Entity cooperate in:

(Art. 16)



How and until when will the NCCS be implemented?

We are here



Terms, conditions, and methodologies (TCMs) to be developed

Cybersecurity risk assessment methodologies

Comprehensive Cross-border electricity cybersecurity risk assessment report

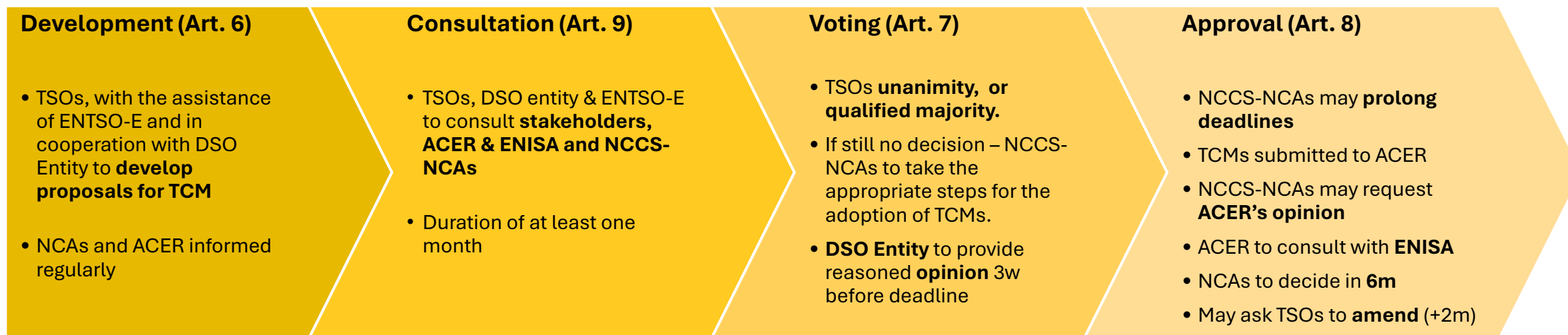
Minimum and advanced cybersecurity controls

Minimum and advanced cybersecurity controls in the supply chain

Cybersecurity procurement recommendations

Cyber-attacks classification scale methodology

What is the process behind the development of terms, conditions, and methodologies (TCMs)?



The process represents EU-level TCM development process. Regional TCMs development process may differ.

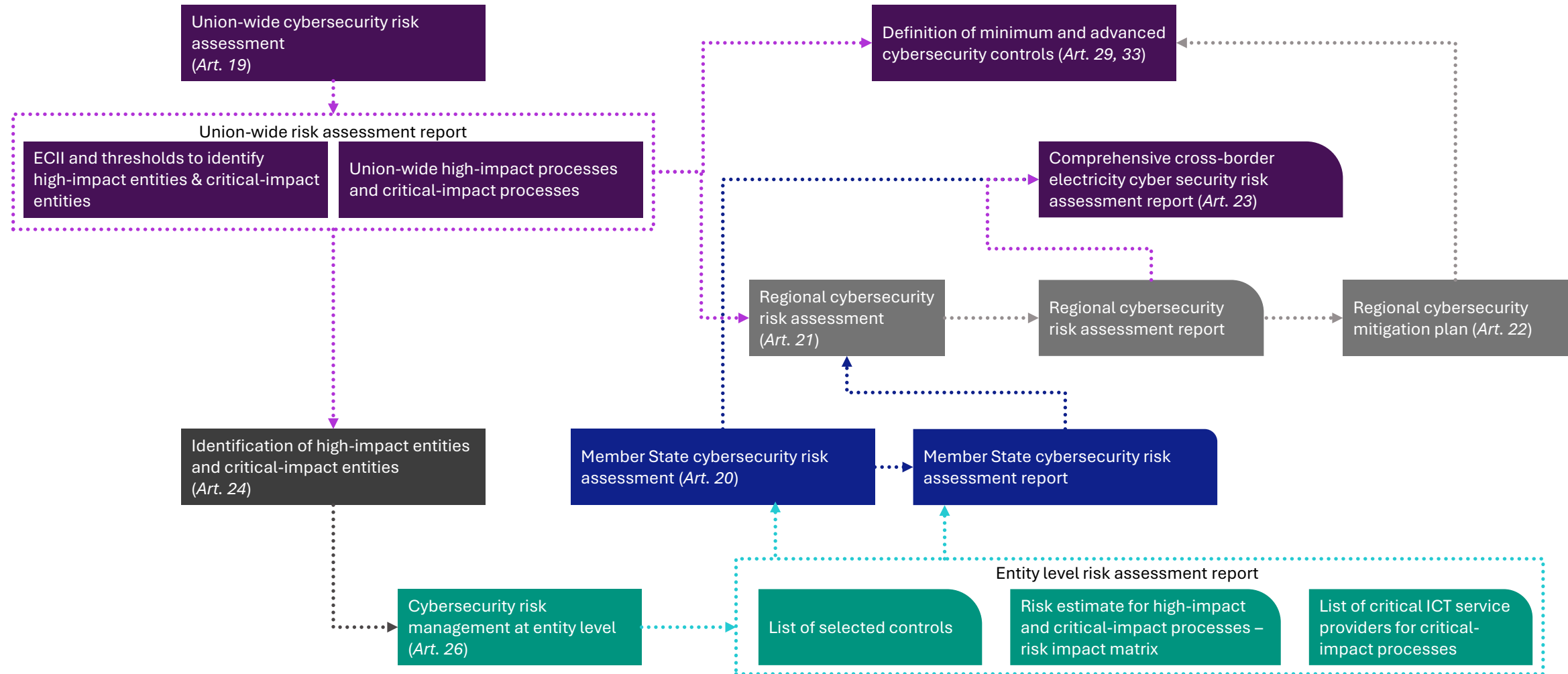
To **contribute to the methodologies**:

- TSOs and DSOs can be part of working groups through ENTSO-E and EU DSO Entity
- Other stakeholders can participate in the consultation round for TCMs

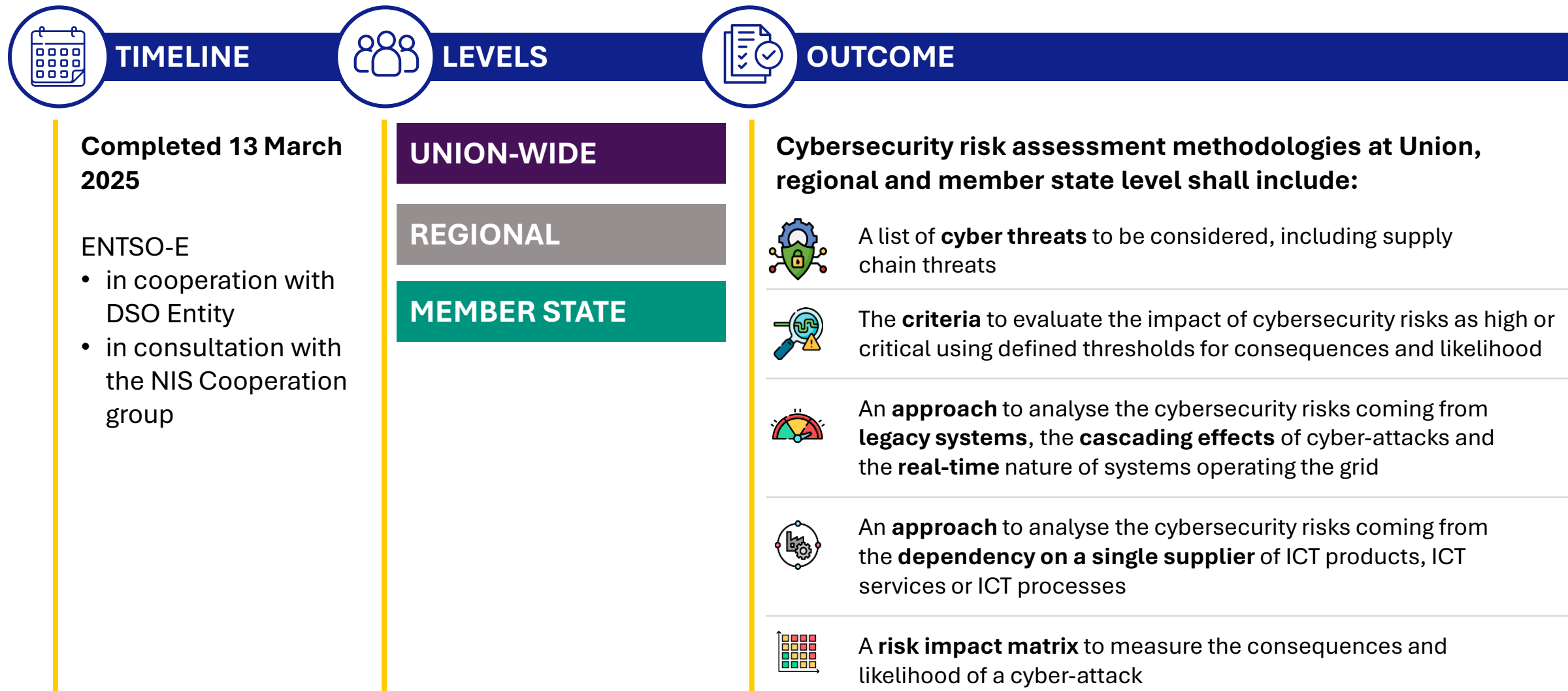
2

Risk assessments

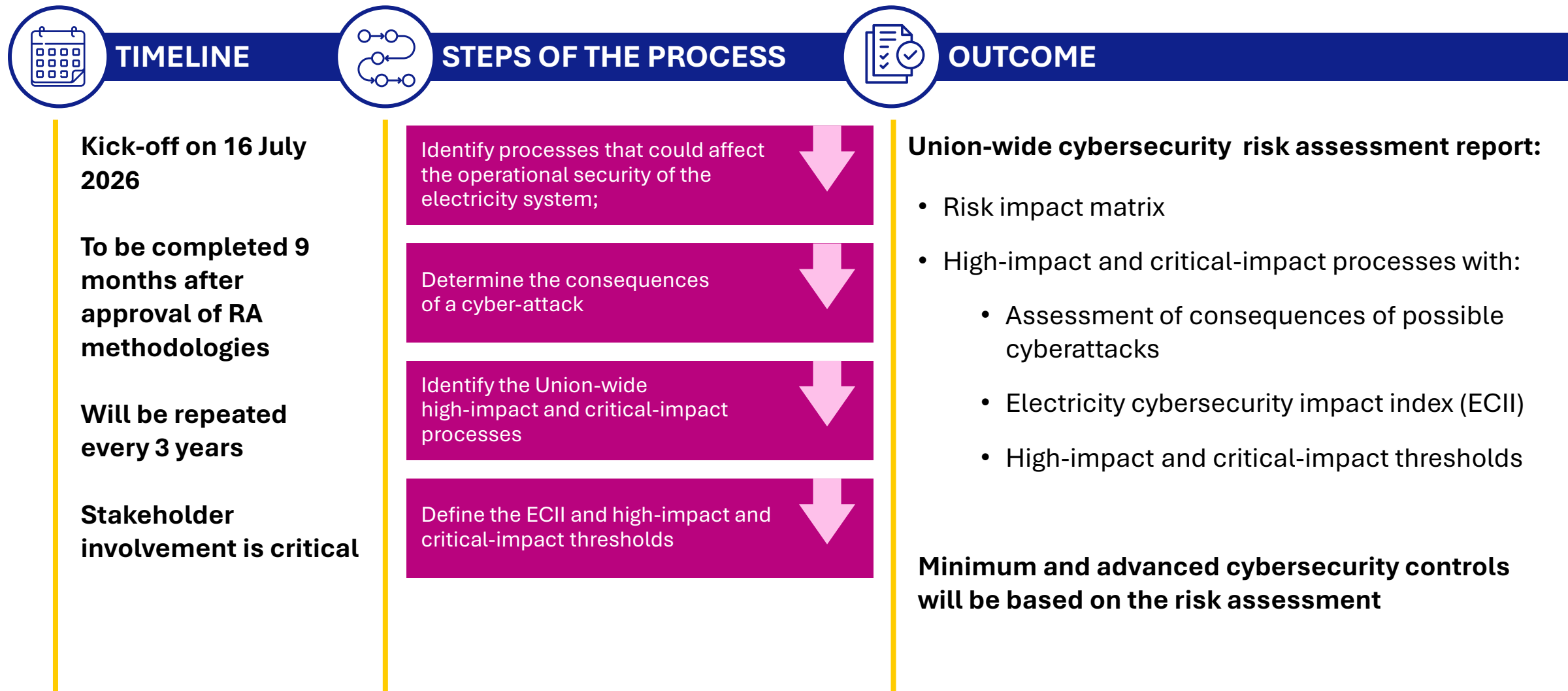
Cybersecurity risk assessment cycle



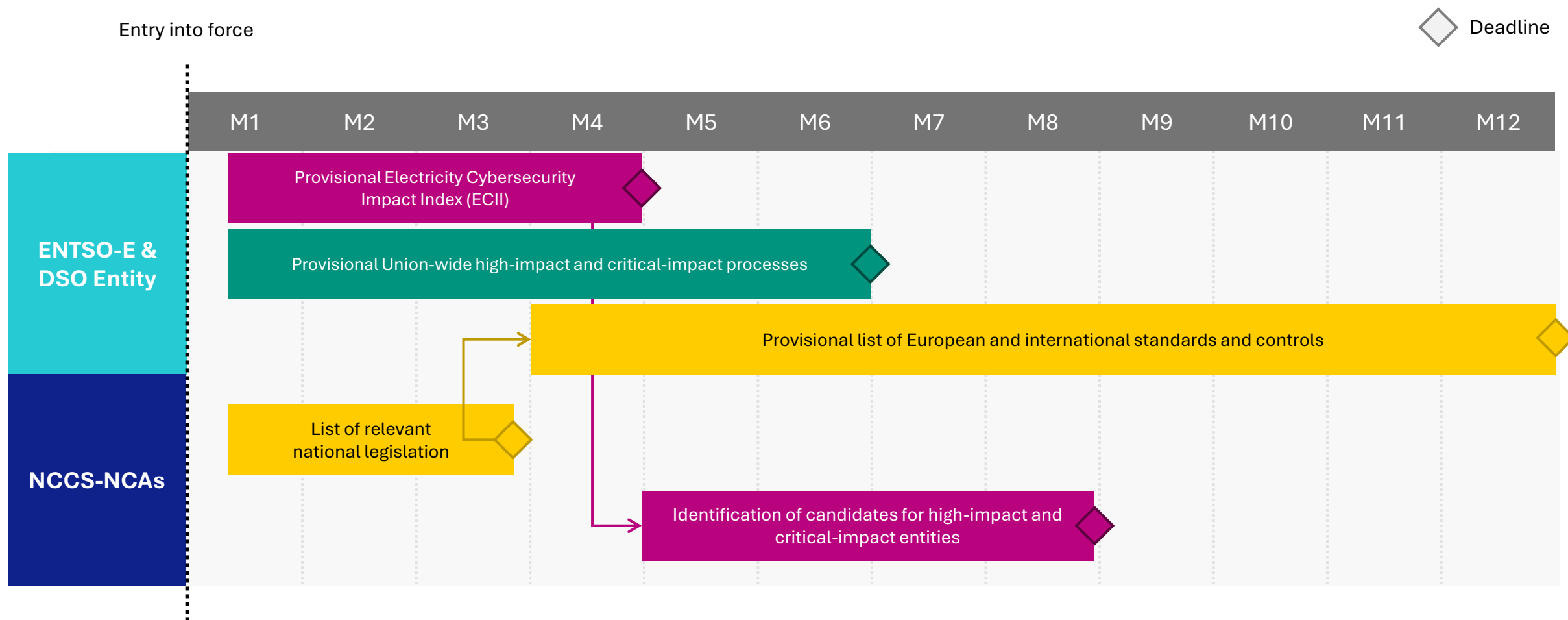
Cybersecurity risk assessment methodologies (Art. 18)



Next step: Union-wide cybersecurity risk assessment (Art. 19)



What is the timeline for the provisional documents (Art. 48)?



NCCS-NCAs must notify candidates for high-impact and critical-impact entities by month 9 after entry into force.

NCCS obligations are **voluntary** for the candidates for high-impact and critical-impact entities.

1. ECII – Electricity Cybersecurity Impact Index

link: [Provisional ECII.pdf](#)

Article 5

High-impact and critical-impact thresholds

1. Provisional thresholds for identifying high-impact and critical-impact processes are given in Table 2. The same thresholds apply to entities and processes.

Table 2: Provisional thresholds.

Member state	High-impact threshold	Critical-impact threshold
Austria	500 MW	3,000 MW
Belgium	1,500 MW	3,000 MW
Bulgaria	250 MW	3,000 MW
Croatia	250 MW	3,000 MW
Cyprus	250 MW	800 MW
Czech Republic	500 MW	3,000 MW
Denmark	1,000 MW	3,000 MW
Estonia	500 MW	900 MW
Finland	1,500 MW	3,000 MW
France	1,500 MW	3,000 MW
Germany	1,500 MW	3,000 MW
Greece	500 MW	3,000 MW
Hungary	500 MW	3,000 MW
Ireland	500 MW	700 MW

What is it for?

- To determine which entities will likely need to implement the NCCS measures
- Competent authorities notified provisional high- or critical-impact entities by 13 March 2025
- These entities may **voluntarily** fulfil the NCCS obligations up to half 2027

Critical-impact threshold →

High-impact threshold →

CRITICAL-IMPACT ENTITIES

HIGH-IMPACT ENTITIES

NO MEASURES

2. LIST OF UNION-WIDE HIGH-IMPACT AND CRITICAL-IMPACT PROCESSES

link: [Provisional list of Union-wide high-impact and critical-impact processes.pdf](#)

Operational security processes for the distribution system

The following processes are for the operational security of the distribution system.

Distribution system monitoring and control

Description	This process concerns the continuous monitoring and control of the distribution system from the central control rooms of the DSO and locally from substations. The process includes real-time connections from the DSO to its TSO, including the real-time data exchange required by Article 44 of the SO GL.
Expected impact	Critical
Entities involved	DSOs (see Article 2 (1) (a) of the NCCS Regulation)
Supporting assets involved	- DSO SCADA system - DSO EMS and (A)DMS systems, including systems for power flow calculations - DSO substation automation systems - DSO distribution automation systems - Backup communication channels such as satellite phone or radio - Weather forecast systems - Load forecast systems

What is it for?

- To determine to which business processes inside the entity the NCCS measures will apply
- Entities should perform a risk assessment on all processes in the list
- If the assessment shows the process is high- or critical-impact (based on ECII), it is in scope for the NCCS



RISK
ASSESSMENT

CYBER-ATTACKS
(POTENTIAL
IMPACT)

MINIMUM &
ADVANCED
CYBERSECURITY
CONTROLS

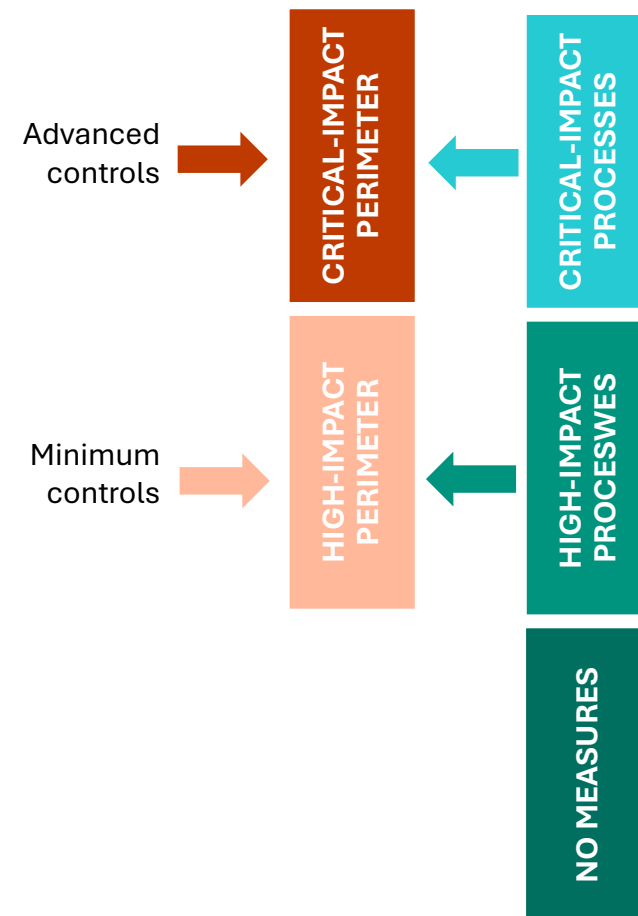
3. Provisional list of standards and controls

link: [Network Code on Cybersecurity](#)

ISO/IEC 27001: 2022 Annex A control identifier	ISO/IEC 27001:2013 Annex A control identifier	Minimum controls	Advanced controls
5,1	05.1.1, 05.1.2	X	X
5,2	06.1.1	X	X
5,3	06.1.2	X	X
5,4	07.2.1	X	X
5,5	06.1.3	X	X
5,6	06.1.4		X
5,7	New		X
5,8	06.1.5, 14.1.1	X	X
5,9	08.1.1, 08.1.2	X	X
5,10	08.1.3, 08.2.3	X	X
5,11	08.1.4	X	X
7,6	11.1.5		
7,7	11.2.9		
7,8	11.2.1		X
7,9	11.2.6		
7,10	08.3.1, 08.3.2, 08.3.3, 11.2.5		X
7,11	11.2.2		X
7,12	11.2.3		X
7,13	11.2.4		X
7,14	11.2.7		X
8,1	06.2.1, 11.2.8	X	X
8,2	09.2.3	X	X
8,3	09.4.1	X	X
8,4	09.4.5	X	X
8,5	09.4.2	X	X
8,6	12.1.3	X	X
8,7	12.2.1	X	X

What is it for?

- To determine which controls should be implemented by the entity
- Minimum controls apply inside high-impact perimeter
- Advanced controls apply inside critical-impact perimeter
- Implementation is **voluntary** in provisional phase



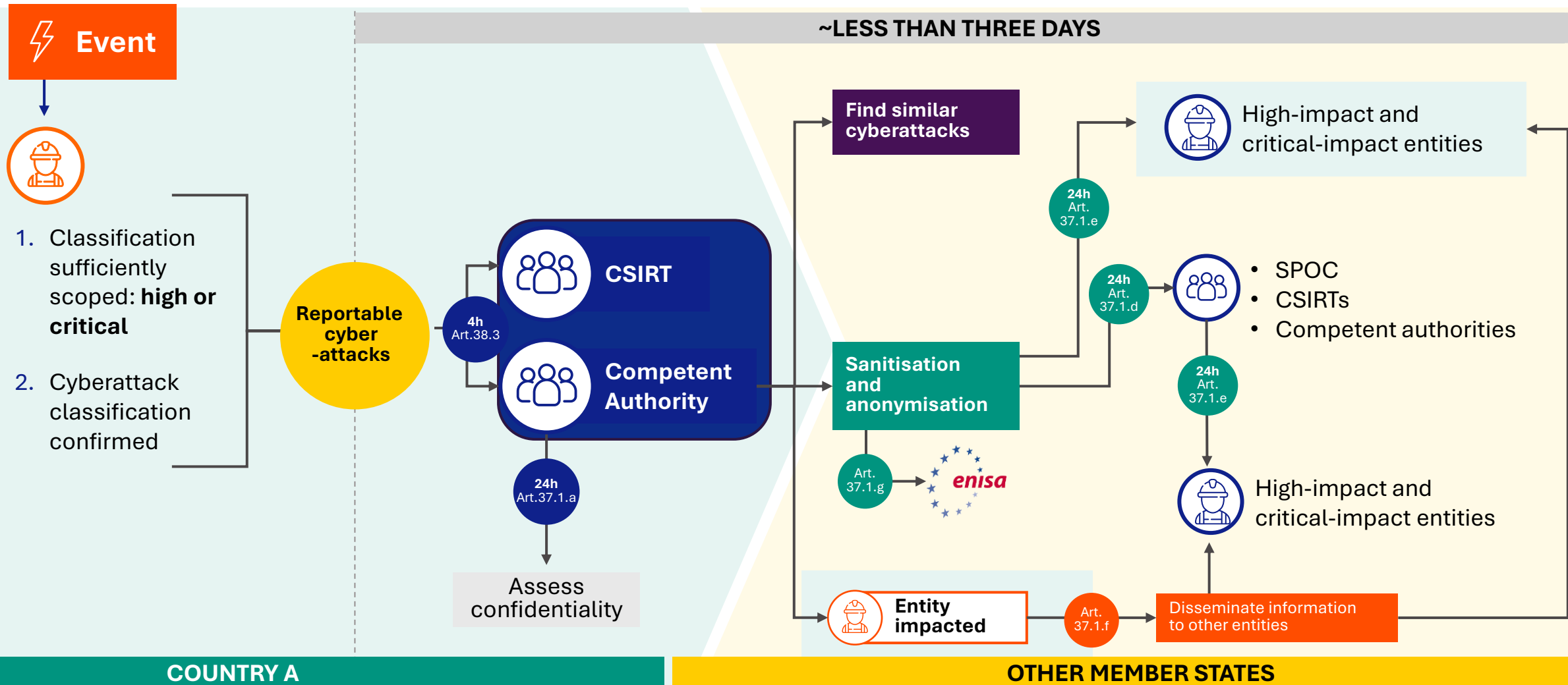
3

Cyber-attacks and Supply chain controls and procurement recommendationsflows

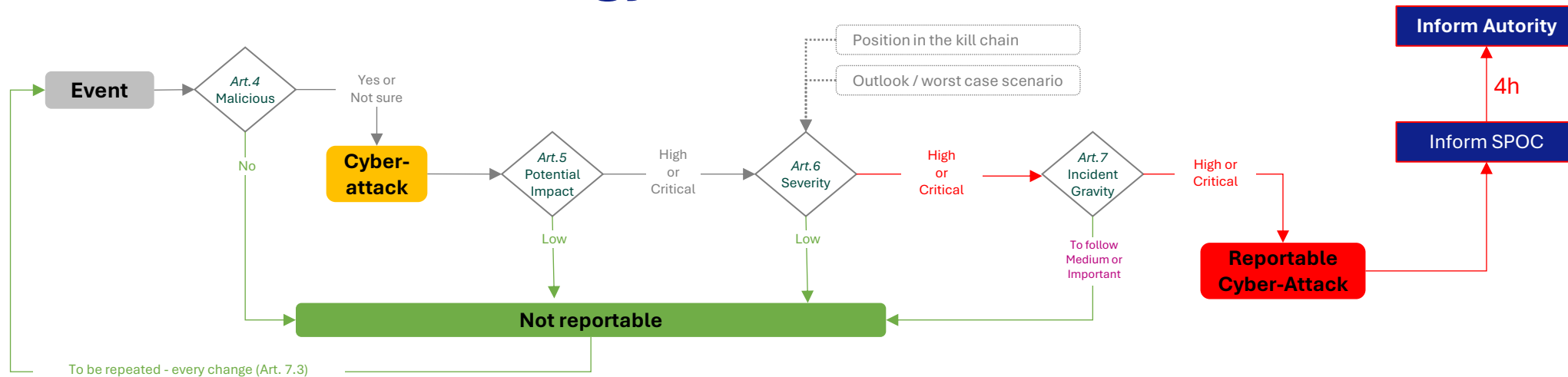
What is it for?

To clarify what kind of incident must be reported

NCCS : Reporting cyber-attacks



The CACS methodology



- **Malicious root cause** : the origin of the event is any human intention to deliberately cause harm or damage.
- **Not malicious root cause** means that the origin of the event is without any human intention to deliberately cause harm or damage.
- **Uncertain root cause** : consider Malicious

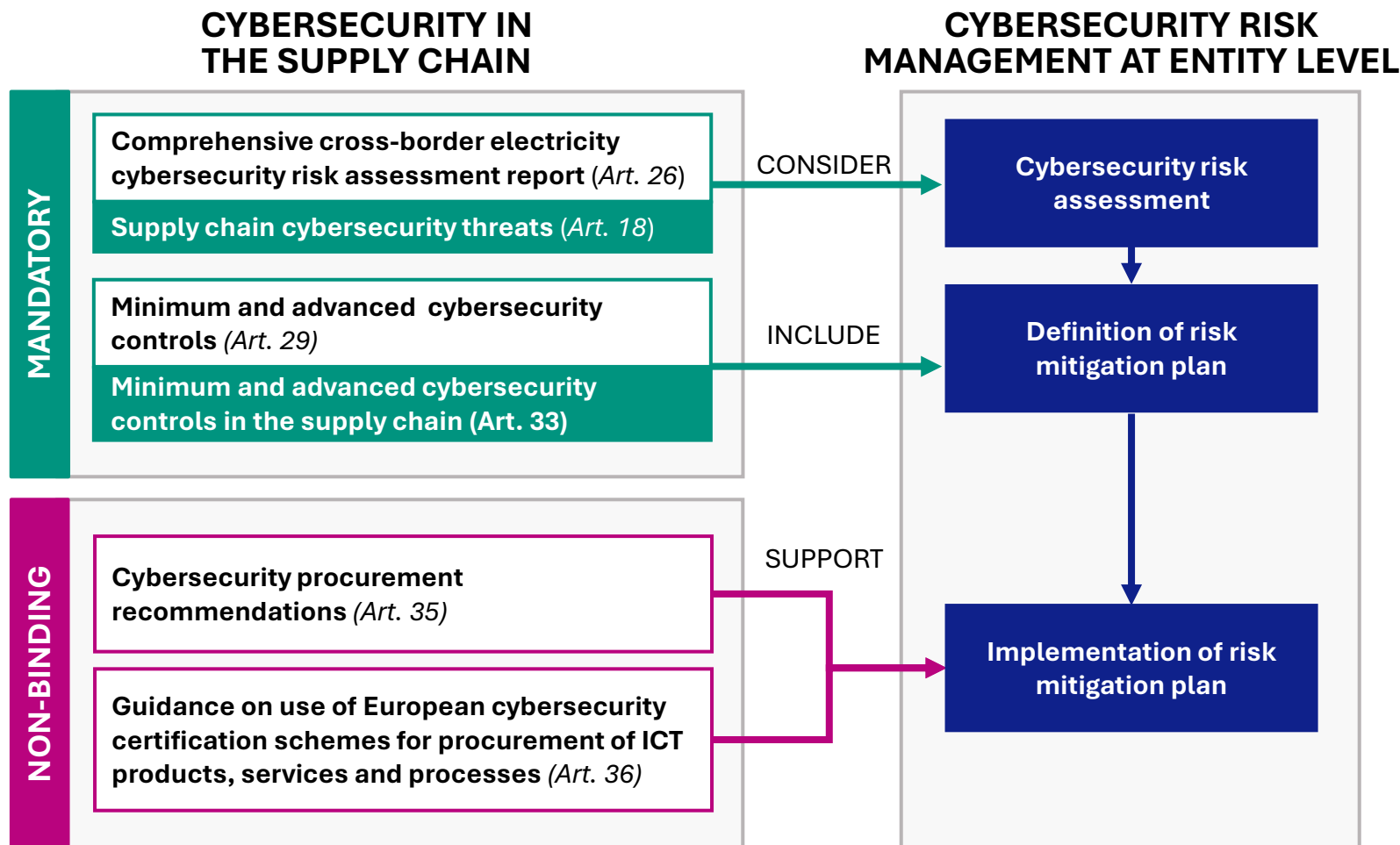
1,5GW for big countries but in fact dépend of the country (250MW-1,5GW)
For 3GW >> from 800MW to 3GW

		Potential Impact		
		Low PI <1,5GW	High PI [1,5GW ; 3GW]	Critical PI >3GW
Severity of the Attack	Low Severity	the attackers are trying to get access to one or more asset. To follow gravity	Medium gravity	Important gravity
	High Severity	the attackers have at least limited access to one or more assets Medium gravity	High gravity	High gravity
	Critical Severity	more than one assets are impacted by lateral movement, or [the attackers] appear to be able to interrupt the process or perpetuate actions on one or multiple assets to destabilize the entity Important gravity	High gravity	Critical gravity

4

Supply chain controls and procurement recommendations

Cybersecurity in the supply chain and cyber risk management at entity level



During the cybersecurity **risk assessment phase**, each high-impact and critical-impact entity shall **identify potential cybersecurity risks** considering:

- the **cyber threats** identified in the **latest comprehensive cross-border electricity cybersecurity risk assessment report**;
- potential **supply chain threats**.

Reference: Art. 26 (4a)(iii)

During the cybersecurity **risk treatment phase**, each high-impact and critical-impact entity shall establish an **entity-level risk mitigation plan** by selecting **risk treatment options** appropriate to manage the risks and identify the residual risks

Reference: Art. 26 (5)

Minimum and advanced cybersecurity controls in the supply chain (Art. 33)



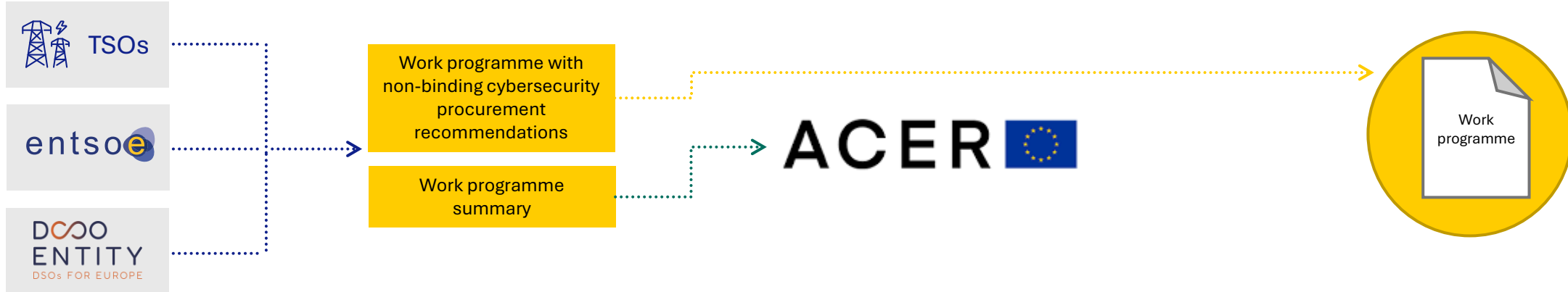
Minimum controls in the supply chain shall include:

- **Recommendations for procurement** of ICT products, services and processes
- **Background verification checks** of supplier's stuffs
- **Secure systems development lifecycle**
- **Zero trust**
- **Secure supplier access**
- **Contractual obligations**
- **Traceability** of the application of the requirements
- Support for **security updates**
- Right to **audit** cybersecurity
- Assessment of **risk profile** of the supplier

Advanced controls in the supply chain shall include:

- **Verification** of cybersecurity specifications of ICT products services and processes via:
 - European cybersecurity certification schemes
 - Verification activities selected by the entity

Non-binding cybersecurity procurement recommendations (Art. 35)



TSOs, together with **ENTSO-E**, and in cooperation with the **DSO** entity, shall develop, in a **work programme**, **sets of non-binding cybersecurity procurement recommendations** that **high-impact and critical-impact entities** may use for the procurement of **ICT products, services and processes**.

Reference: Art. 35(1)

ENTSO-E, in cooperation with the **DSO entity**, shall **provide ACER with a summary of the work programme within 6 months** after the adoption of the regional cybersecurity risk assessment report, which means the latest by 13 June 2031, or its update, which occurs every three years.

Reference: Art. 35 (2)

The work programme shall also include:

1. a **description and classification** of the types of **ICT products, services and processes used by high-impact and critical-impact entities**;
2. the **types of ICT products, services and processes for which the recommendations shall be developed**.

Reference: Art. 35 (1)

Work programme update: Regional risk assessment report + 6 months

Gateway Security Profile



Substation gateways are key components in grid automation systems, enabling the remote control of the grid by SCADA systems.



The Gateway Security Profile is a non-binding recommendation and is based on the following standards:

- **IEC 62443-4-1:** Secure product development
 - **IEC 62443-4-2:** Technical security requirements
- It also follows the rules set out in **IEC 62443-1-5**.

In line with IEC 62443-1-5, the security profile includes a risk assessment and a set of security requirements, developed according to the following process:



To tailor IEC 62443 requirements to the specific context of gateways, three types of contextualization and clarification were introduced:

- **Contextualizations:** Clarify how to apply the requirements in the operational context of the gateway (mandatory)
- **Interoperability suggestions:** Provide technical implementation ideas to promote compatibility between systems (optional)
- **Implementation guidelines:** Offer practical recommendations to support the application of the requirements (optional)



For each security requirement, its nature is defined as follows:

- **M (Mandatory):** Required to be compliant with the profile
- **C (Conditional):** Required only if a specific condition applies
- **Not selected:** Not required by the profile but may be implemented voluntarily

Thank you

To learn more about NCCS, please visit the ENTSO-E or DSO Entity websites and YouTube channels.