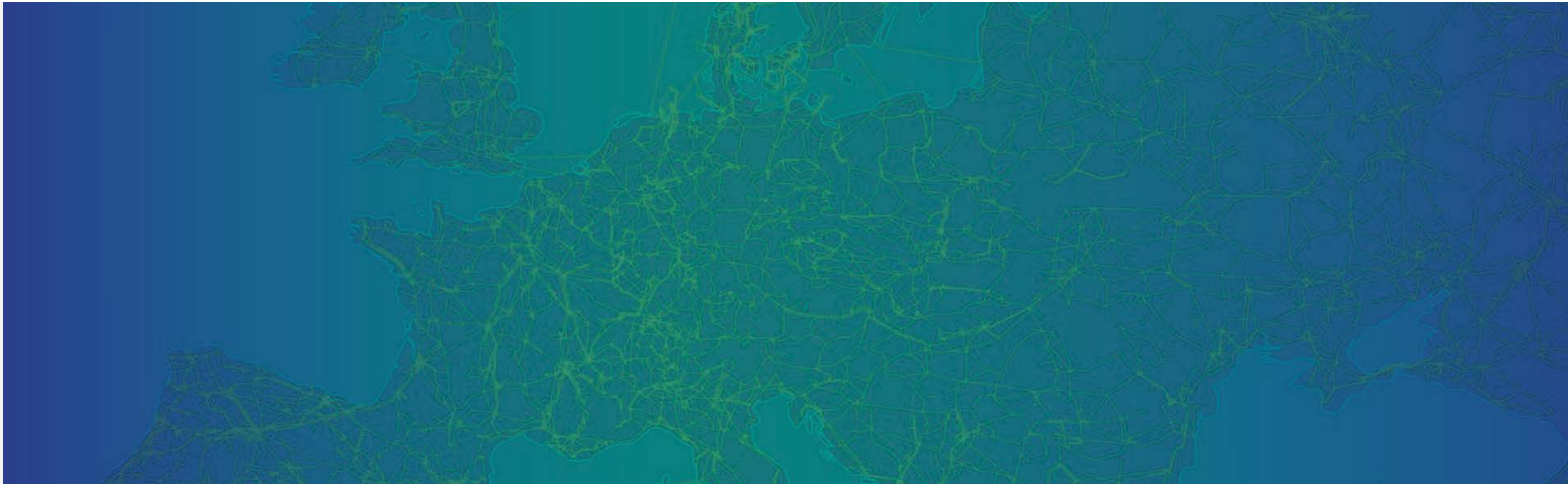
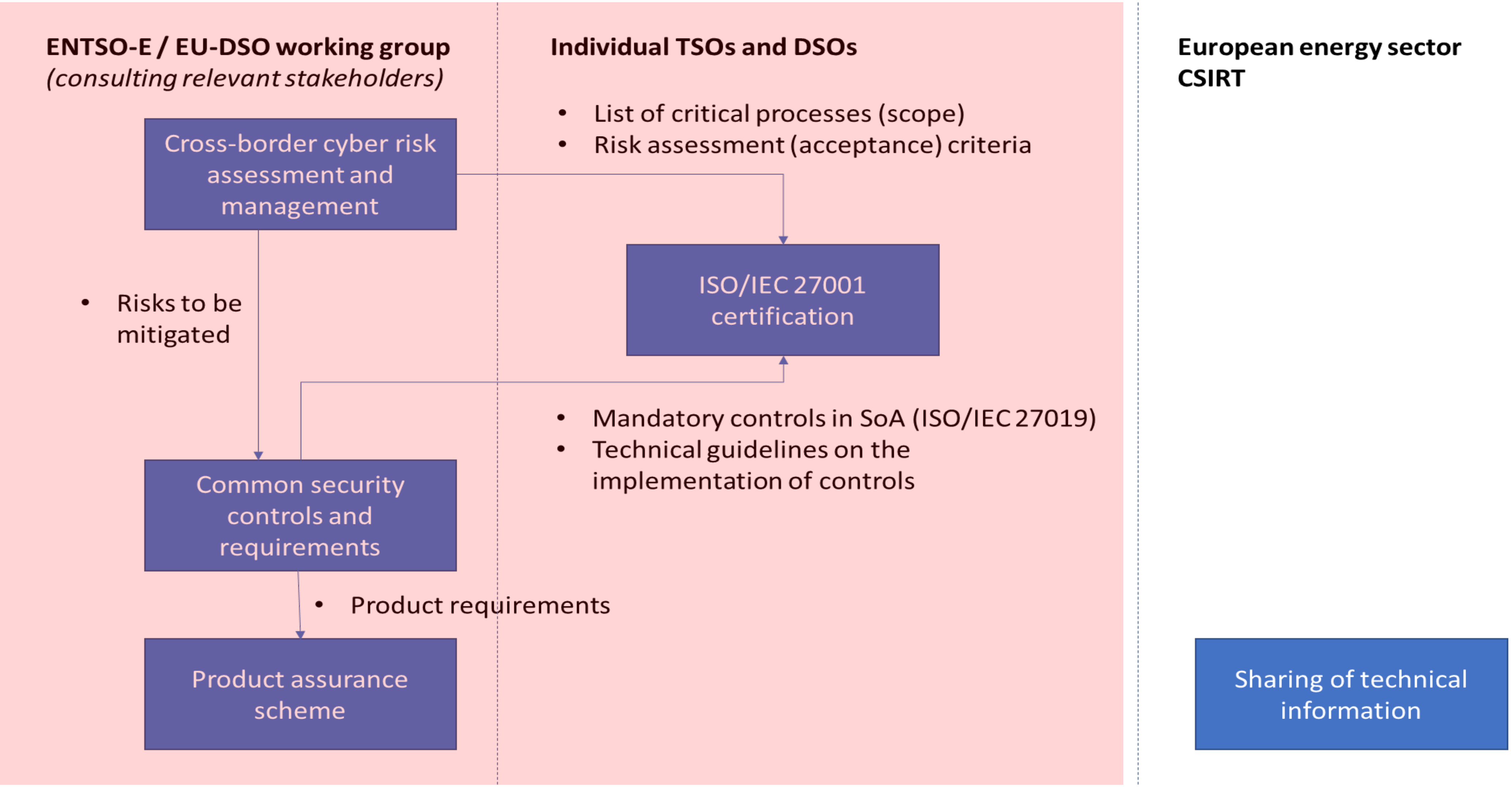
Network Code on Cybersecurity

Energy Community, 15 December 2020

ENTSO-E



Network Code on Cybersecurity – Second Interim report – five recommendations



ENTSO-E / EU-DSO working group
(consulting relevant stakeholders)

Cross-border cyber risk assessment and management

- Risks to be mitigated

Common security controls and requirements

- Product requirements

Product assurance scheme

Individual TSOs and DSOs

- List of critical processes (scope)
- Risk assessment (acceptance) criteria

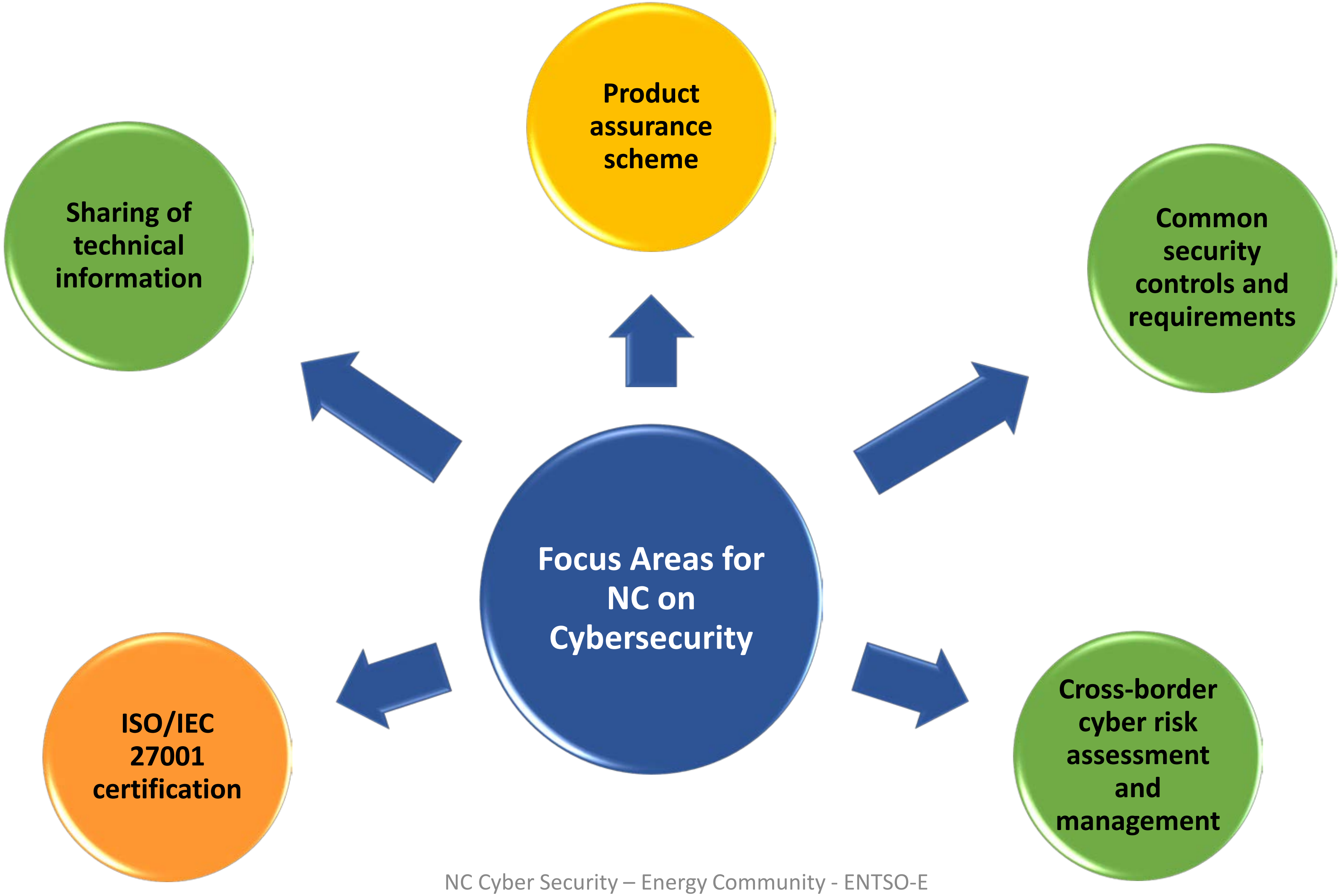
ISO/IEC 27001 certification

- Mandatory controls in SoA (ISO/IEC 27019)
- Technical guidelines on the implementation of controls

European energy sector CSIRT

Sharing of technical information

Network Code on Cybersecurity – Possible challenges and Future achievements



Focus Areas for NC on Cybersecurity

Product assurance scheme

Sharing of technical information

Common security controls and requirements

ISO/IEC 27001 certification

Cross-border cyber risk assessment and management

Thank you for your attention!

Backup / Details

Key points

- **Cross border cyber risk assessment -** ENTSO-E/EU-DSO working group with a mandate to perform cyber risk assessments impacting cross border transmission and/or distribution, specifically tasked with the identification of “critical business processes and events” which if successfully cyber-attacked could cause serious cross border transmission and/or distribution issues.

- **ISO/IEC 27001 certification** - Any organization (grid participant) which performs one or more of these identified cross border “critical business processes” and who meets the thresholds set will come into scope for ISO/IEC 27001 certification (mandatory), thus ensuring a common minimum-security level of Cybersecurity for all grid participants performing “critical business processes”.

Key points

- **Functional and non-functional security requirements** - ENTSO-E/EU-DSO working group with mandate to define appropriate functional and non-functional security requirements to adequately protect “critical business processes” from cyber-attack and the IT/OT systems which support them. Security controls based upon ISO/IEC 27002 and 27019, forming a common basis for the procurement of systems, components and services by all grid participants.

- **Product assurance scheme** – energy sector specific scheme, created and used to test/measure the effectiveness of systems, components and services whose security controls claim to conform to the defined set of functional and non-functional security requirements.

Key points

- **European Energy sector CSIRT (Cybersecurity Incident Response Team)** – with a mandate and trusted to receive technical incident and vulnerability information from all grid participants and disseminate this information in a sanitized form so that all grid participants can protect themselves against the same types of cyber-attack.