IBERDROLA

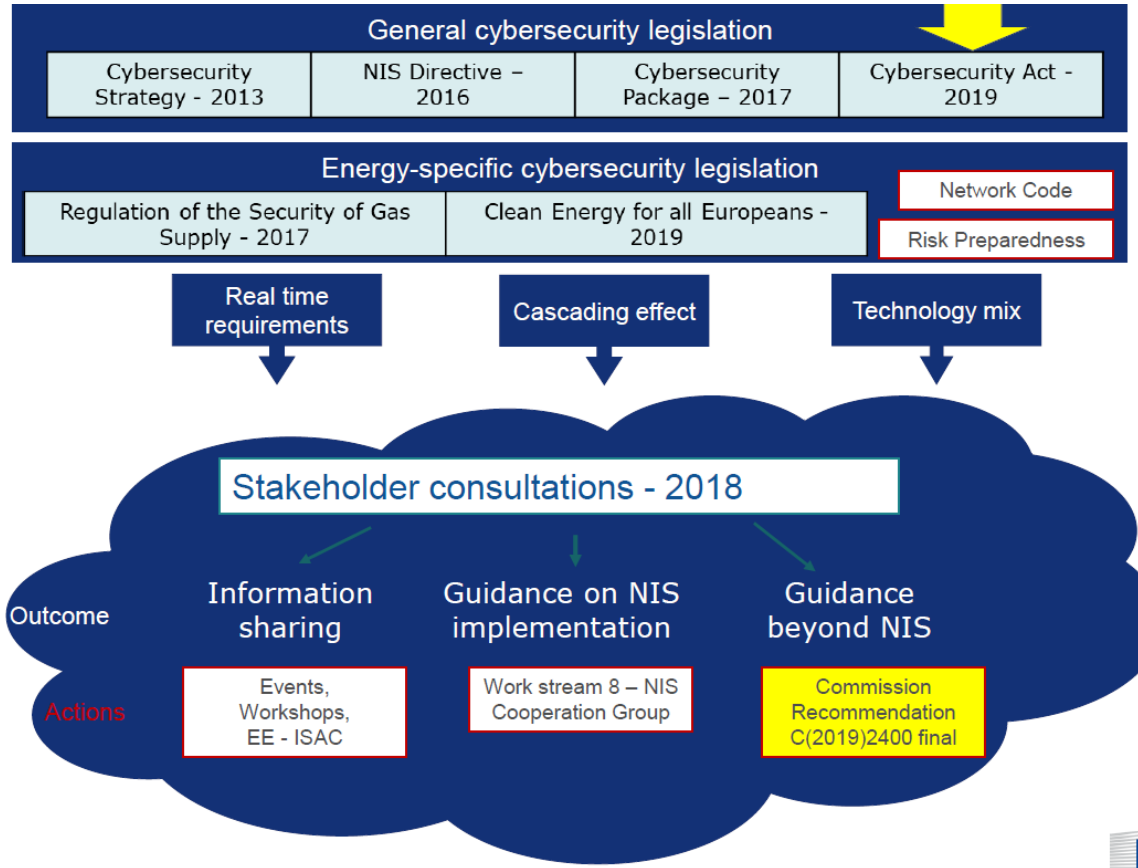
Cybersecurity Day in the Energy Community

1 June 2021

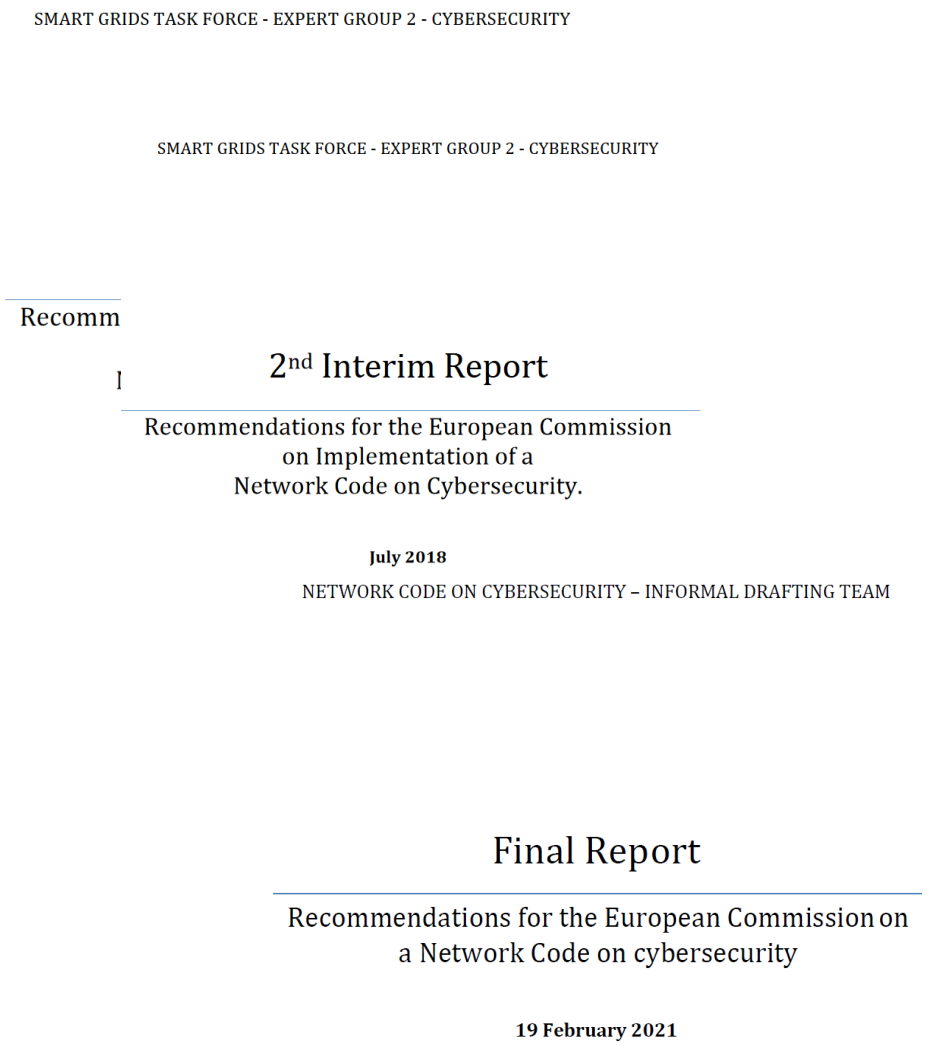
Principles for application of technical standards in energy industry

EU legislation evolution

LEGISLATION



SOFT MEASURES



Smartgrids TaskForce

1. *As the energy system becomes more integrated, having a common mandatory standard is the only way* ***to assure a common minimum level of cybersecurity across all European grid participants****.*

2. ***The ISO/IEC 27001 provides such a common standard for an ISMS for aligned risk management****.*

3. *Conformance to ISO/IEC 27001 has been generally accepted by the associations of the TSOs and DSOs, although it must be recognised that* ***some organisations do not agree****.*

4. ***Other common standards are a valid alternative approach,*** *if they provide a validated mapping with ISO/IEC 27001 domains/controls and are independently verified and audited in a harmonized way.*

Final Report

Recommendations for the European Commission on a Network Code on cybersecurity

19 February 2021

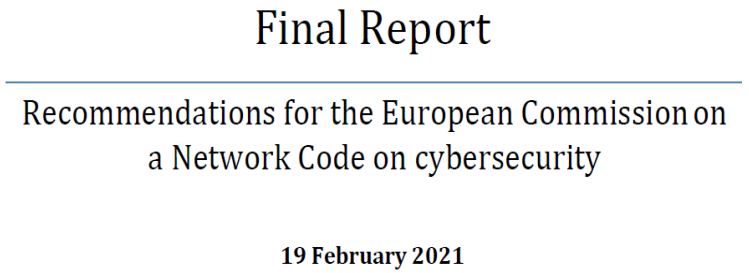
TSO's & DSO's raised questions concerning:

1. *Should equivalent certifications be recognised since some TSOs have already invested in alternative certification schemes,*

2. *Will **costs increase** substantially if **compliance** to standards are demanded,*

3. *ISO/IEC 27001 only demonstrates that a control has been implemented, not its maturity.*

4. *Identification of suitable and adequate **security controls** which should ideally be based on internationally recognised standards like ISO/IEC 27001 Annex A, ISO/IEC 27002 and **ISO/IEC 27019, ISA/IEC 62443 series, IEC 62351 series, IEC 60870**, or **alternatively popular US security standards** like NERC and NIST may be considered **which are already being used by some TSOs and DSOs**.*



Network Code on Cybersecurity - ACER

ACER

Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

(Draft)

PC_2021_E_04
30 April 2021

Table 1: Entities to whom the network code shall apply

#	Entity definition
1.	Electricity undertakings referred to in paragraph (57) of Article 2 of the Electricity Market Directive
2.	ENTSO-E, the EU-DSO Entity, ACER and NRAs
3.	National Competent Authorities for Risk Preparedness, SOCs, National Competent Authorities for cybersecurity in Energy and CSIRTs
4.	Regional Coordination Centres referred to in Article 35 of the Electricity Market Regulation
5.	Essential Service suppliers as defined in this Framework Guideline

Classification of entities subject to the network code by Electricity Cybersecurity Risk Index (ECRI)

Essential
electricity undertakings

Important
electricity undertakings

Network Code on Cybersecurity - ACER

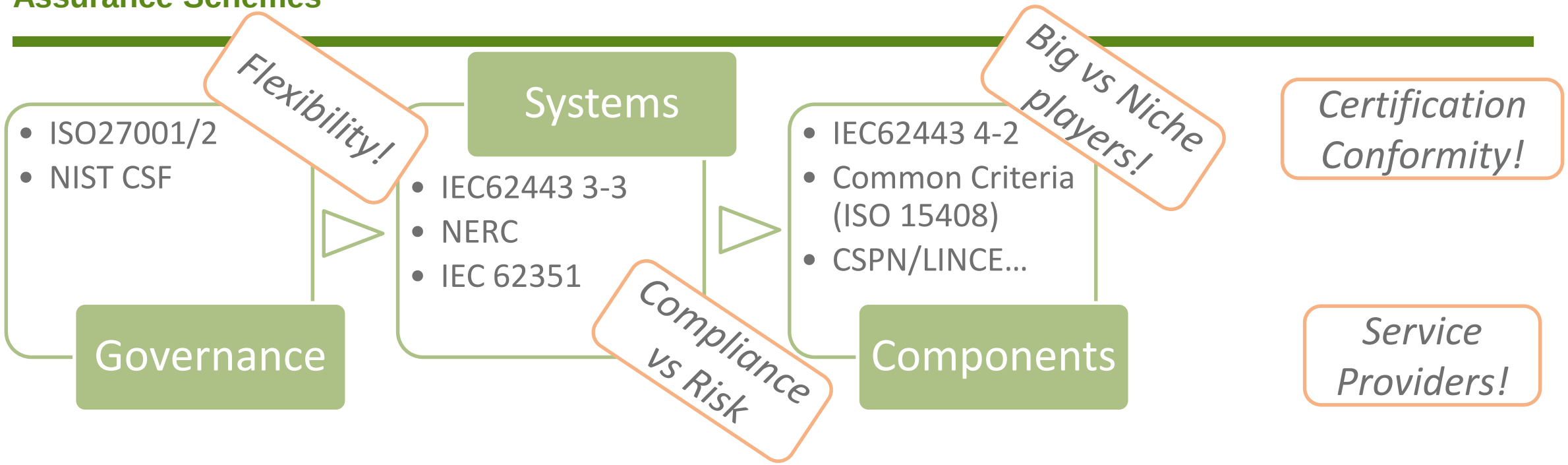
Common Electricity Cybersecurity Framework

*the **network code shall ask** ENTSO-E and the EU-DSO Entity, assisted by ACER and ENISA, **to provide an electricity principles/standards mapping matrix** (EPSMM)*

*The **network code may entrust ENISA**, assisted by ACER and by the Joint Research Centre of the European Commission, **with the development of a European Cybersecurity Electricity Maturity Model** (ECEMM)*

	Cybersecurity areas	Small and Micro Enterprises[17]	Minimum Requirements (Important electricity undertakings)	Advanced Requirements (Essential electricity undertakings)
1	Basic Cybersecurity Hygiene requirements (see last paragraph of Chapter 1.3)	✓	✓*	✓*
2	Obligation to compile an asset inventory and to define the internal electricity cybersecurity perimeter		✓	✓
3	The assets potential impact on cross-border electricity flows shall be described in the inventory.			✓
4	Obligation to perform a cybersecurity risk assessment, including the evaluation of the cybersecurity maturity of the implemented measures/controls to manage risks at point 2 of this table.		✓	✓
5	Take part to a cross-border cybersecurity Risk assessment for electricity cross-border flows, including the evaluation of the cybersecurity maturity of the implemented measures/controls to manage risks identified at point 2 of this table.			✓
6	Obligation to implement measures and controls to mitigate risks, based on the minimum set of cybersecurity principles/standards to manage risks at point 4 of this table.		✓	✓
7	Obligation to apply common Functional and Non-functional requirements to all inventory assets		✓	✓
8	Prioritize application of common Functional and Non-functional requirements to assets that take part to cross-border electricity flows.			✓
9	Obligation to take part and contribute to the information sharing and dissemination system for the electricity cybersecurity cross-border flows and monitoring, benchmarking and additional reporting obligations.		✓	✓
10	Obligation to establish incident handling procedures.		✓	✓
11	Obligation to set procedures in case of a disruption to cross-border electricity flows.			✓
12	Obligation to take part to the Crisis Management System (CyCLONe)		✓	✓
13	Obligations on the Supply Chain Security and on the Certification of Components taking part to the operations of cross-border electricity flows.			✓
14	Participation in electricity cybersecurity exercises (see chapter 6).			✓

Assurance Schemes



Product Assurance Scheme

Governance

Enabling innovation

Mandatory vulnerability handling

Requirements to evaluate against

Requirements defined top-down by risk owners

Requirements cover secure development

Evaluation methods

Thorough, independent evaluation

WEF contribution

1. ***Utilities should selectively adopt provisions from various standards and frameworks where appropriate..***

2. ***Regulators should avoid making these standards compulsory in their entirety*** and instead use them and other cybersecurity frameworks as useful tools when designing a cybersecurity programme for specific operational aspects.

3. ***Utilities should follow reference architectures and product-specific implementation guidance, where relevant, when deploying or updating their systems.***

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

Cyber Resilience in the Electricity Industry:

Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors

In collaboration with Accenture and the Electricity Industry Community

July 2020

FIGURE 4. REVIEWED STANDARDS AND FRAMEWORKS