ACER

European Union Agency for the Cooperation of Energy Regulators

Framework Guideline on Cybersecurity

Stefano Bracco

Energy Community - Cybersecurity Coordination Group - 5th Meeting

WebEx, 16th December 2021

Pillars of the FG

- Let’s assess the risks for the electricity sector
- Let’s prevent that risks will materialize
- Let’s be prepared for action in absence of the digital layer
- No overlap but harmonisation with the proposal and future NISv2

Introduction / General Record

- **2019:** Electricity Regulation mandates a NC on CS
- **2019:** Smart Grids Task Force – Report of the Expert Group 2 - Cybersecurity
- **2020:** Commission's stakeholder consultation
- **2020:** ENTSO-E and DSO associations informal interim report
- **28 Jan 2021:** Invitation to ACER to draft framework guideline
- **14 April 2021:** ACER and drafting team alignment webinar
- **30 Apr 2021:** FG proposal on public consultation
- **18 May 2021:** ACER and drafting team alignment webinar
- **27 May 2021:** Public FG webinar with ACER
- **4 June 2021:** ACER and drafting team alignment webinar
- **25 June:** 1st Review of the FG
- **29 June 2021:** End of public consultation
- **30 June 2021:** ACER and drafting team alignment webinar
- **22 July 2021:** FG sent by ACER to the Commission
- **23 July 2021:** EC sends the letter to ENTSOE to submit a proposal for a NC in close cooperation with EU-DSO
- **12 November 2021:** Public consultation on Network Code on Cybersecurity opens
- **10 December: 2021**: End of ENTSO-E/EU-DSO public consultation
- **14 January 2022:** Proposed draft network code delivered to ACER
- **13 June 2022**: Deadline to provide NC to the European Commission

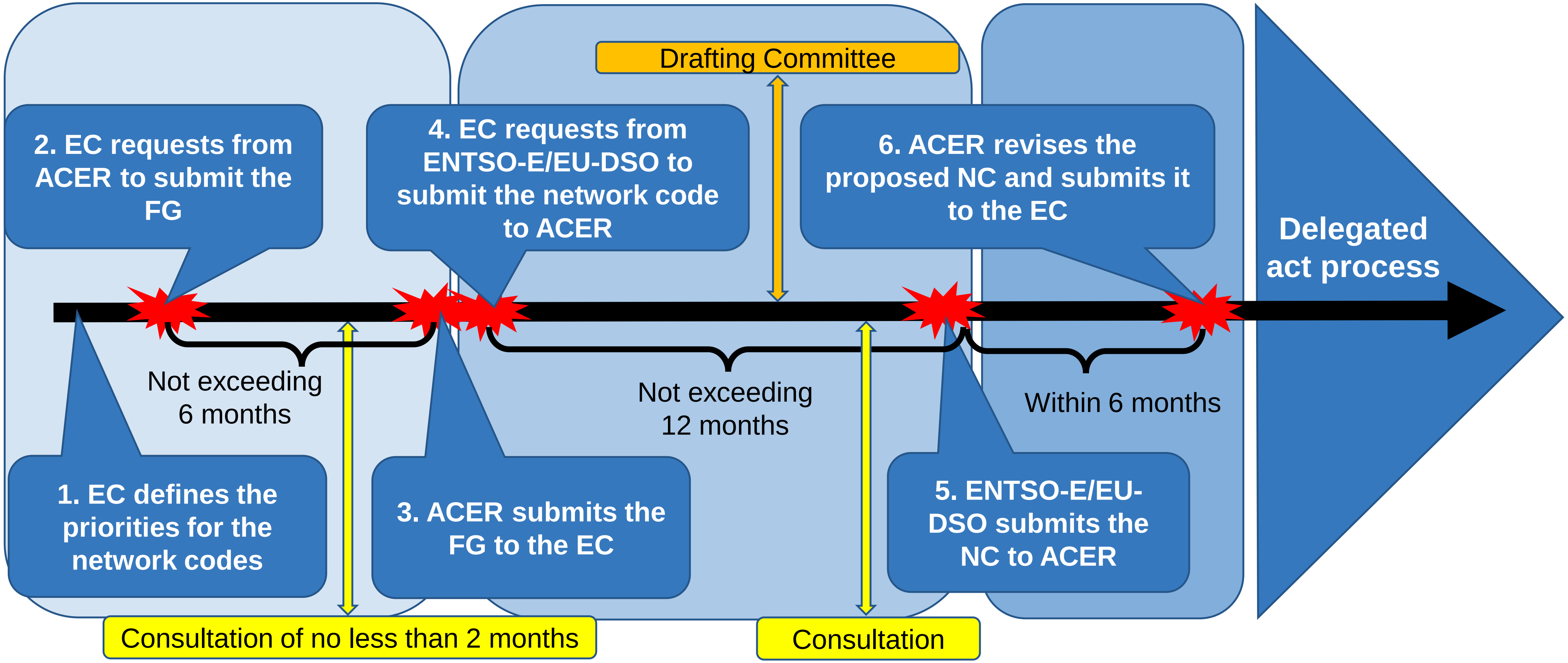
Various meetings/updates with the CS NC Drafting Team with specific scopes

+ meetings with other stakeholders

Comments on CS NC Drafting Team with specific scopes

Next steps

General timeline as set out in Article 59(2) of REGULATION (EU) 2019/943



1. EC defines the priorities for the network codes

2. EC requests from ACER to submit the FG

Not exceeding 6 months

Consultation of no less than 2 months

3. ACER submits the FG to the EC

4. EC requests from ENTSO-E/EU-DSO to submit the network code to ACER

Drafting Committee

Not exceeding 12 months

Consultation

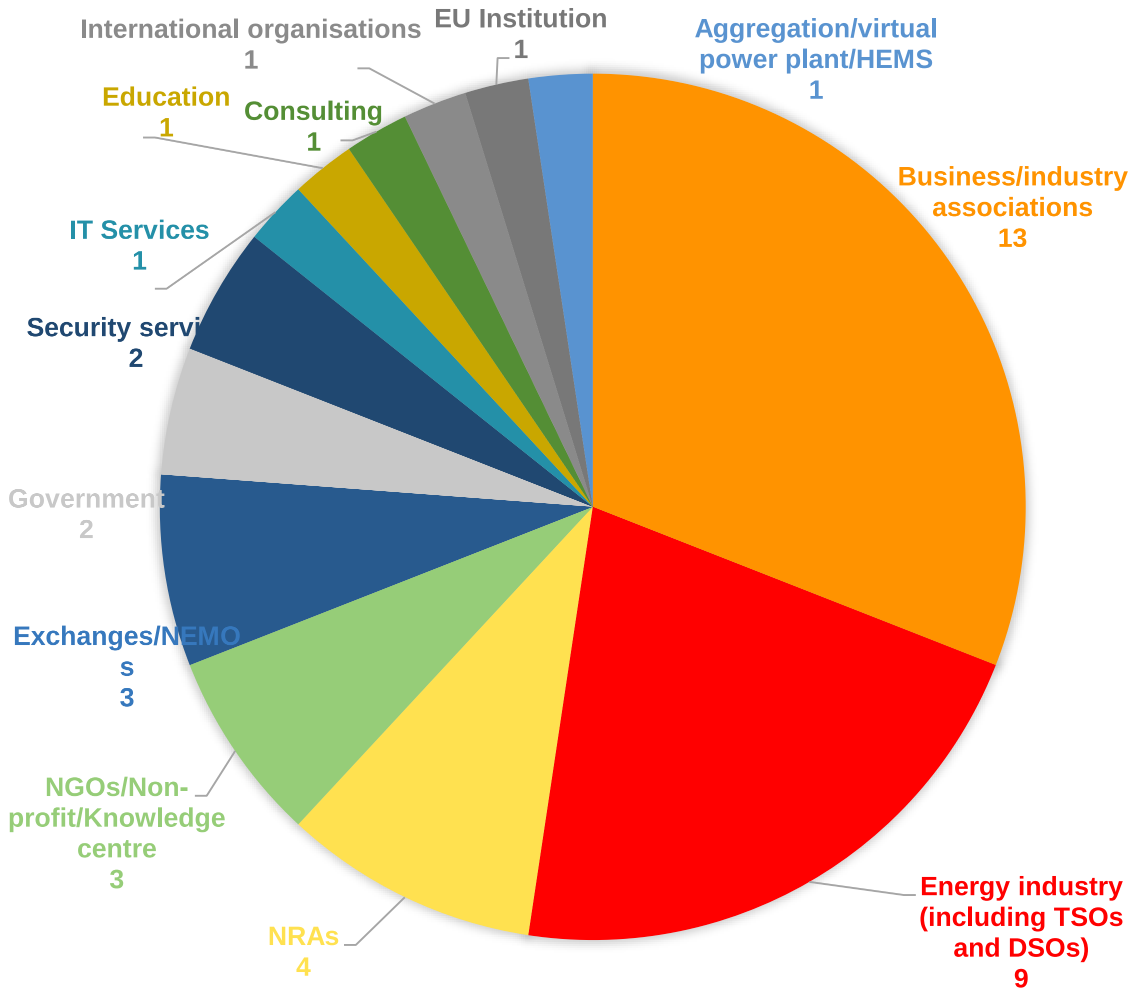
5. ENTSO-E/EU-DSO submits the NC to ACER

6. ACER revises the proposed NC and submits it to the EC

Within 6 months

Delegated act process

Introduction / Public Consultation



- Respondents in general welcome the draft FG
- 88% believe the draft FG contributes to further protecting cross border electricity flows
- 85%, consider that FG covers sufficiently the real-time requirements of energy infrastructure components, the risk of cascading effects and the mix of legacy and state-of-the-art technology
- 65% believe the draft FG still have gaps concerning the cybersecurity of cross-border electricity flows, which the FG should address

Content of the FG

1. **General Provisions**: scope, definitions, applicability and transitional measures
2. **Cybersecurity Electricity Governance**: general principles
3. **Cybersecurity Risk Assessment**: integrated approach, its governance and transitional methodology

4. **Common Electricity Cybersecurity Framework**: governance for the definition of minimum and advanced requirement, and supply chain
5. **Essential information flows, Incident and Crisis Management**
6. **Electricity Cybersecurity exercise framework**

7. **Protection of information exchanged in this network code**
8. **Monitoring, benchmarking and reporting**
9. **New systems, process and procedures**

ACER
European Union Agency for the Cooperation of Energy Regulators

Principles and entities in scope of the CSNC

Complementarity

- CSNC is more specific in description, e.g., on what entities in scope
- CSNC goes further than NIS2, e.g., on requirements to information sharing

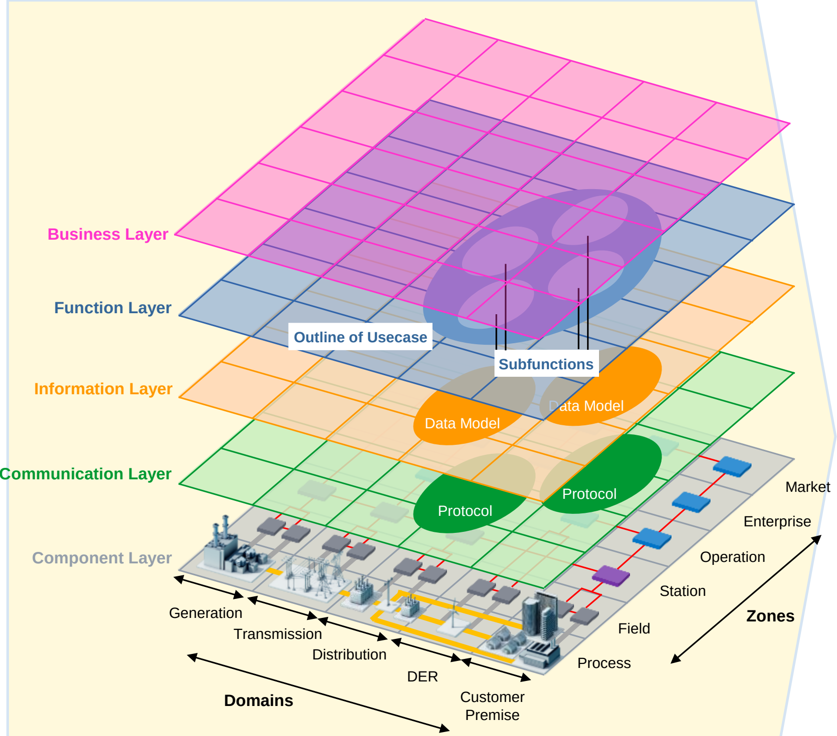
Consistency

- CSNC does not provide alternatives to requirements presented in NIS2
- CSNC is not hindering implementation of requirements presented in NIS2
- No new actors, but reinforcing their rules set up by existing EU legislation

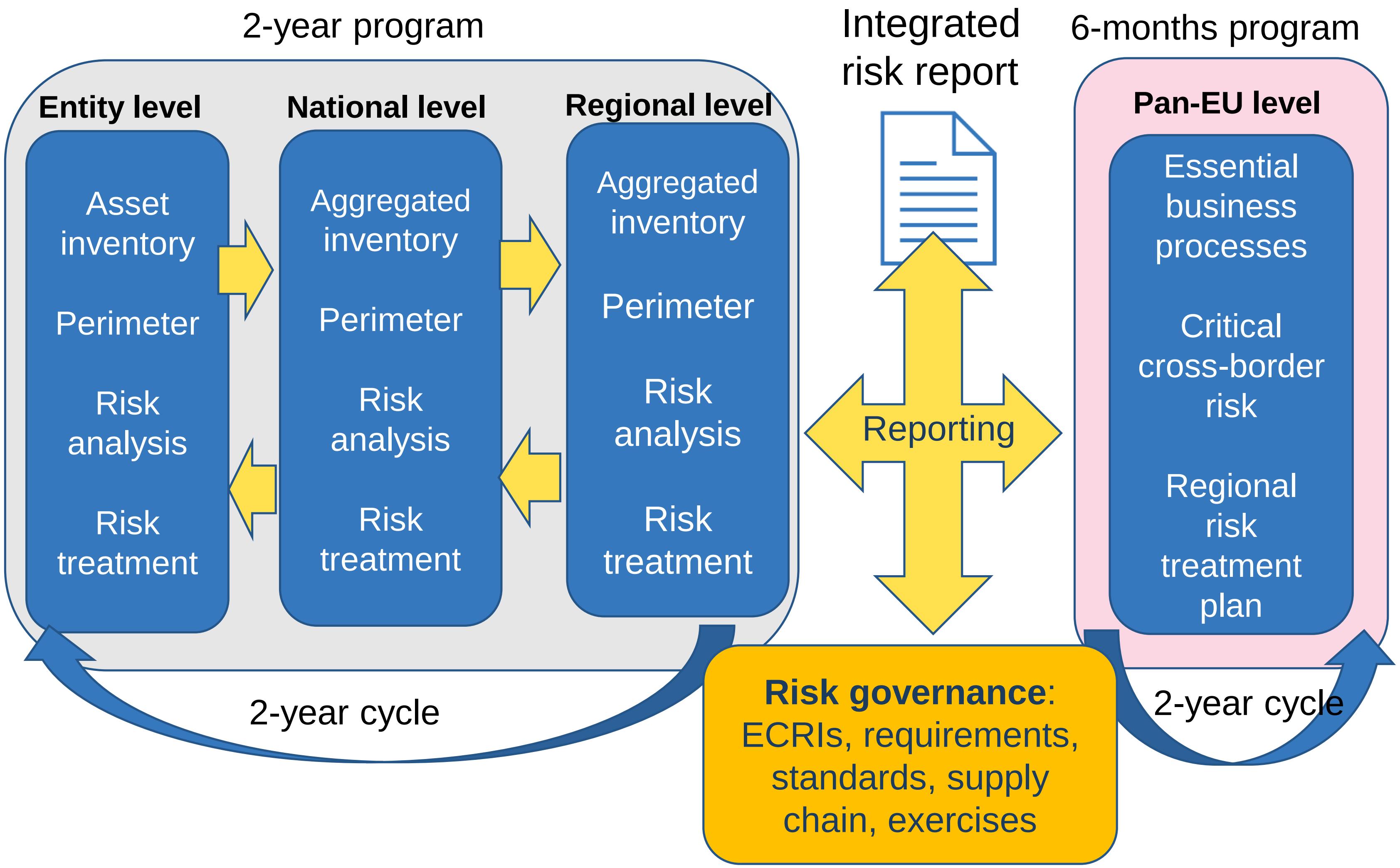
Small and micro enterprises are in principle are excluded, but the **network code must provide for the possibility of applying** it to SMEs-µEs, as well as any additional stakeholders (biannual inclusion/derogation)

#	Table 1. Entity definition
1	Electricity undertakings as defined in Article 2(57) of the Electricity Market Directive
2	NEMOs as defined in Article 2(7) and (8) of Electricity Market Regulation
3	Electricity digital market platforms as defined in this Framework Guideline
4	Critical service providers as defined in this Framework Guideline
5	Regional Coordination Centres (RCCs) established pursuant to Article 35 of the Electricity Market Regulation
6	ENTSO-E, the EU DSO entity, ACER and NRAs
7	RP-NCAs, SOCs, CS-NCAs and CSIRTs and ENISA

Integrated top-down and bottom-up approach



SGAM, Smart Grids Architecture Model.
©CEN-CENELEC-ETSI 2015



2-year program

Entity level

- Asset inventory
- Perimeter
- Risk analysis
- Risk treatment

National level

- Aggregated inventory
- Perimeter
- Risk analysis
- Risk treatment

Regional level

- Aggregated inventory
- Perimeter
- Risk analysis
- Risk treatment

2-year cycle

Integrated risk report

Reporting

6-months program

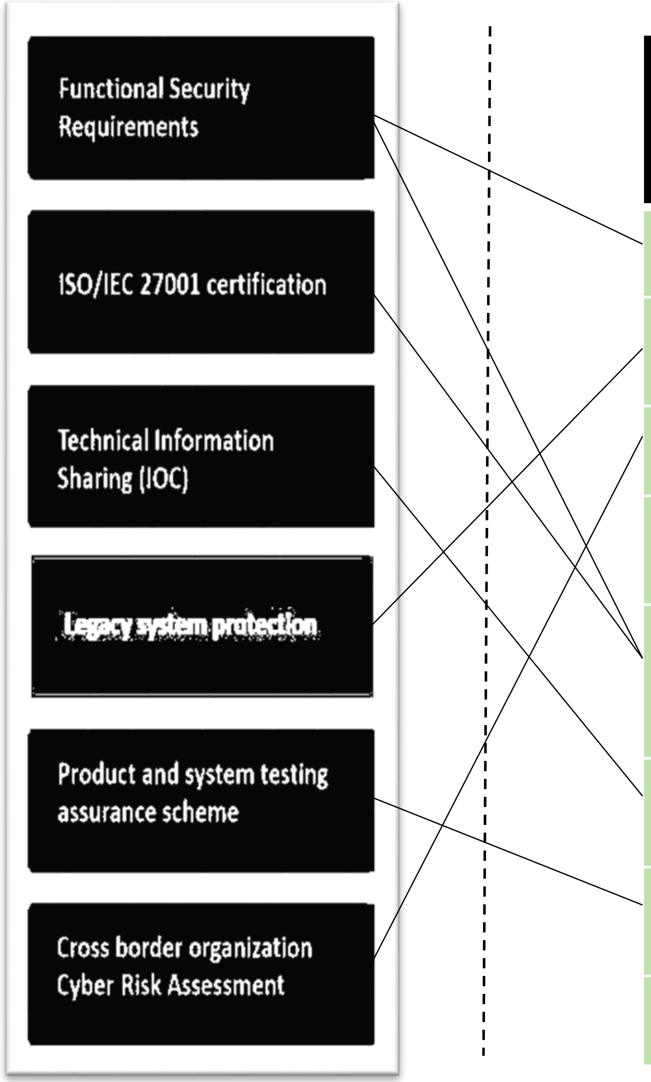
Pan-EU level

- Essential business processes
- Critical cross-border risk
- Regional risk treatment plan

2-year cycle

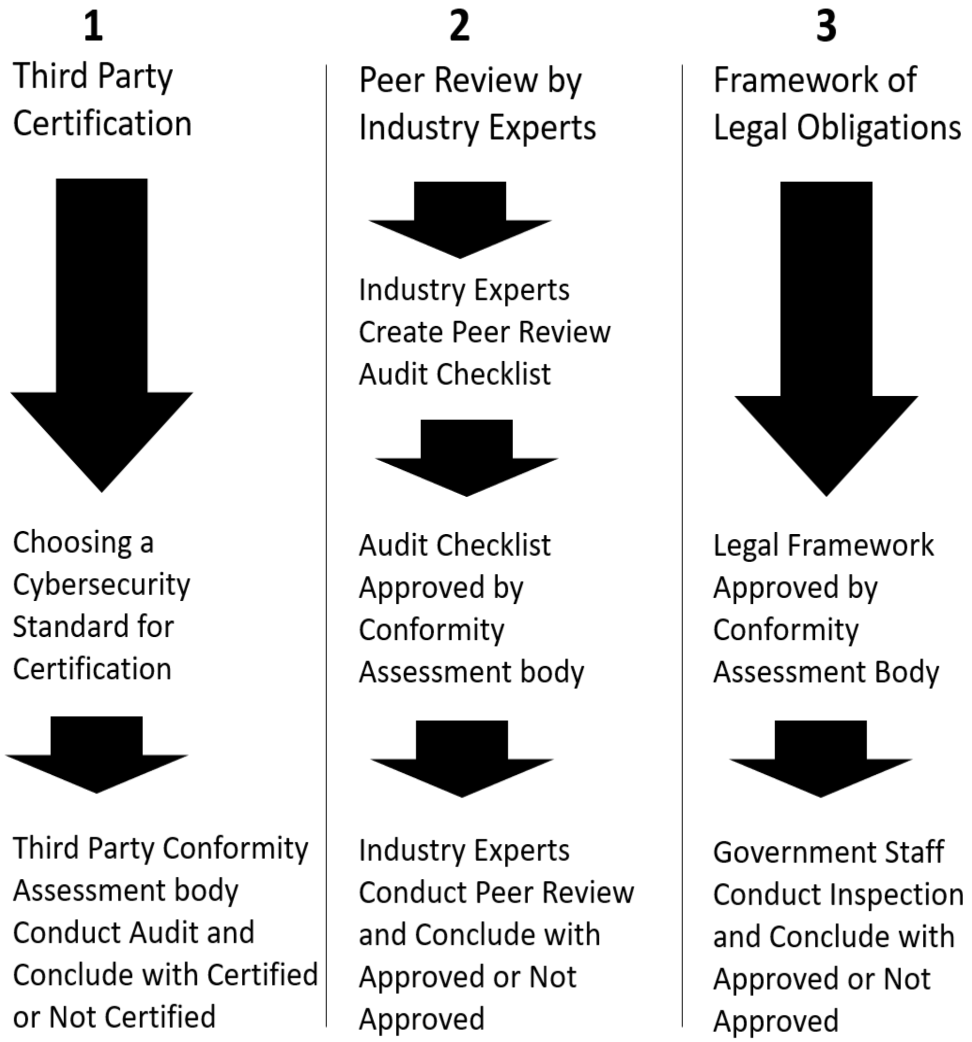
Risk governance: ECRIs, requirements, standards, supply chain, exercises

Main content of the Framework Guideline


Functional Security Requirements
ISO/IEC 27001 certification
Technical Information Sharing (IOC)
Legacy system protection
Product and system testing assurance scheme
Cross border organization Cyber Risk Assessment

Framework Guideline	Small and Micro Enterprises <50 Employees & <10 Mill Eur	High-risk entities Minimum Security Requirements	Critical-risk entities Advanced Security Requirements
Basic cyber hygiene	Yes	Implicit	Implicit
Identification of critical products and processes		Yes	Yes
Integrated risk assessment		Yes	Yes
Evaluation of critical assets and risks		Yes	Yes
Common security framework including verification of implemented requirements		Yes	Yes
A SOC network for information sharing and incident handling		Yes	Yes
Security certification of essential products			Yes
Participation in cyber exercises			Yes

Common electricity cybersecurity framework Three tracks for verification of compliance.



1
Third Party Certification

Choosing a Cybersecurity Standard for Certification

Third Party Conformity Assessment body Conduct Audit and Conclude with Certified or Not Certified

2
Peer Review by Industry Experts

Industry Experts Create Peer Review Audit Checklist

Audit Checklist Approved by Conformity Assessment body

Industry Experts Conduct Peer Review and Conclude with Approved or Not Approved

3
Framework of Legal Obligations

Legal Framework Approved by Conformity Assessment Body

Government Staff Conduct Inspection and Conclude with Approved or Not Approved

- **Verification through third party certification or statement of applicability:** Standards covering cybersecurity requirements may be used for verification through certification or a statement of applicability from a conformity assessment body.
- **Verified peer review process:** Industry experts on electricity cybersecurity may establish a template of controls covering cybersecurity requirements. The process shall be overlooked by NRAs and/or CS-NCAs and the frequency of reviews shall be reported to ACER.
- **Verified framework of legal obligations:** National legal obligations that impose to entities the implementation of cybersecurity requirements equivalent to the common electricity cybersecurity framework shall be listed in the ERSMM and may be used for verification through inspection and supervision by authorities in the Member States.

Chapter 4 - Common Cybersecurity Framework Deliverables

Deliverable	Responsibility
1. A Common Electricity Cybersecurity Framework, including: **-A minimum set of cybersecurity requirements** **-A set of advanced cybersecurity requirements**	Jointly established by ENTSO-E and the EU DSO entity, to be submitted to ENISA for their opinion and then ACER for their opinion
2. An Electricity Requirements/Standards Mapping Matrix (ERSMM)	ENTSO-E and the EU DSO entity, advised by ACER and ENISA
3. A transitional list of national regulations of electricity cybersecurity and EU/International standards	ENTSO-E and the EU DSO entity, advised by ENISA and ACER and with the assistance of the NRAs and the CS-NCAs
4. A list of the temporary derogations from the minimum and advanced cybersecurity requirements	ENTSO-E and the EU DSO entity
5. Procurement templates and procurement protocols	To be defined by the network code
6. A sector-specific guideline on EU products/services/systems certification schemes	ENTSO-E and the EU-DSO entity, in cooperation with ENISA
7. Monitoring of cost-efficiency of the cybersecurity verification schemes	ACER and ENISA
8. Rules to require confidentiality and traceability of information exchanges between the critical-risk / high-risk entities and all actors in the supply chain	ENTSO-E and the EU DSO entity
9. Rules for the roll-out of new systems that may be classified as critical systems for cross-border electricity flows or for the systems that take part to the execution of any critical process in the scope of cross border electricity flows	
10. Rules for the integration of cybersecurity requirements into tender specifications, life-time support, limiting supply chain tracking and promote secure termination	

ACER
European Union Agency for the Cooperation
of Energy Regulators

Chapter 4 - Common Cybersecurity Framework
Content and revision

- **A choice of strategy to verify a common cybersecurity framework including the use of certifiable or verifiable standards, government inspections and peer accreditation processes**
- **The text regarding a common cybersecurity framework is clarified with regards to what requirements the entities shall be subject to**

Chapter 5 - Essential information flows, Incident and Crisis Management. Content and revision

Deliverable	Responsibility
1. An illustration of the information sharing network by mapping different information sharing initiatives and their connections	ENISA
2. A track record of events such as incidents, crises and vulnerabilities that have been reported in the international information sharing network	~~CERT-EU~~, may, with support from ENISA
3. A report on the effectiveness of the Electricity Cybersecurity Early Warning System (ECEWS)	ENISA
4. Criteria to determine if an identified cybersecurity Incident is a Reportable Cyber Security Incident	ENTSO-E and the EU DSO entity
5. Rules for how cross-border cybersecurity crisis shall be managed	
6. Minimum content of crisis management plans, BCP and recovery plans	

- **CSIRTs on Member State level have been given the possibility to withhold information and request advice from ACER and ENISA in cases where dissemination at the EU level is considered a risk**
- **CSIRTs on Member State level may define processes and technologies and ensure daily operations of the information sharing network**

ACER

European Union Agency for the Cooperation of Energy Regulators

Chapter 6 - Electricity cybersecurity exercises Content and revision

1. **A mandatory internal cybersecurity exercise for all critical-risk entities**
2. **For each Member State, a national cybersecurity exercise of all national critical-risk entities of the considered Member State, in substitution of point 1**
3. **A mandatory regional or cross-regional cybersecurity exercise**

Deliverable	Responsibility
1. A multi-year programme of electricity cybersecurity exercises	ENTSO-E and the EU DSO entity
2. A voluntary cybersecurity simulation testbed	

- **A reduction in frequency of internal exercises from two to three years has been introduced**

ACER
European Union Agency for the Cooperation of Energy Regulators

Chapter 7 - Protection of information exchanged in the context of this network code

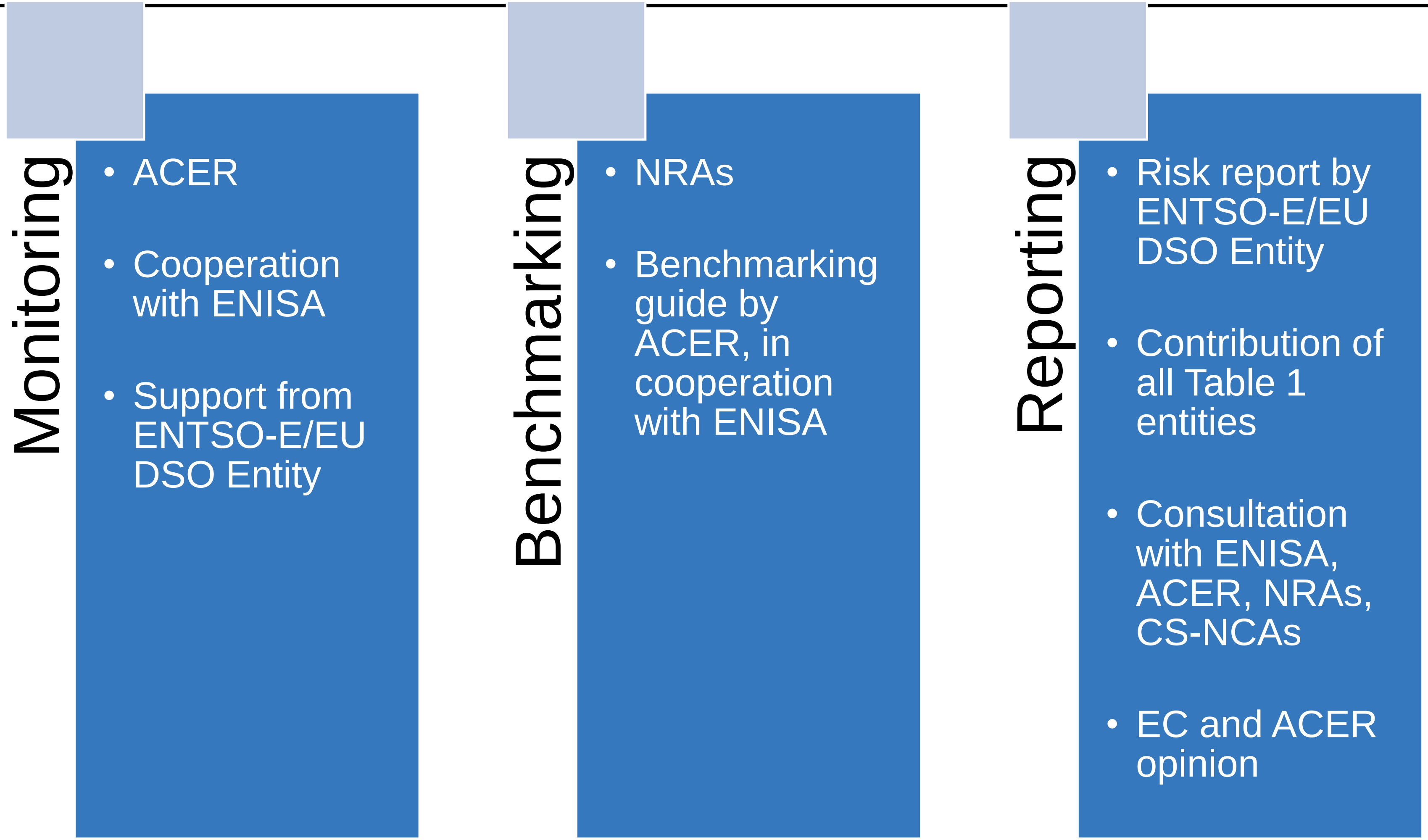
- **All information shall be protected:**

classification level applied by originator and following a number of principles

- **ENTSO-E and the EU DSO entity responsible for defining the rules for the classification and protection of information**

- **NRAs decide on litigation over information classification, processing or exchange**

Chapter 8 - Monitoring, benchmarking and reporting



Monitoring

- ACER
- Cooperation with ENISA
- Support from ENTSO-E/EU DSO Entity

Benchmarking

- NRAs
- Benchmarking guide by ACER, in cooperation with ENISA

Reporting

- Risk report by ENTSO-E/EU DSO Entity
- Contribution of all Table 1 entities
- Consultation with ENISA, ACER, NRAs, CS-NCAs
- EC and ACER opinion

ACER
European Union Agency for the Cooperation
of Energy Regulators

Chapter 9 - New systems, processes and procedures

- **All new systems, processes and procedures shall be acquired, designed, configured and maintained embedding principles such as, but not limited to, security in-depth and security by design.**

- **The network code shall promote the safe digitalisation of the electricity sector.**

Stefano Bracco

ACER

European Union Agency for the Cooperation
of Energy Regulators

info@acer.europa.eu
acer.europa.eu

@eu_acer
linkedin.com/company/EU-ACER/