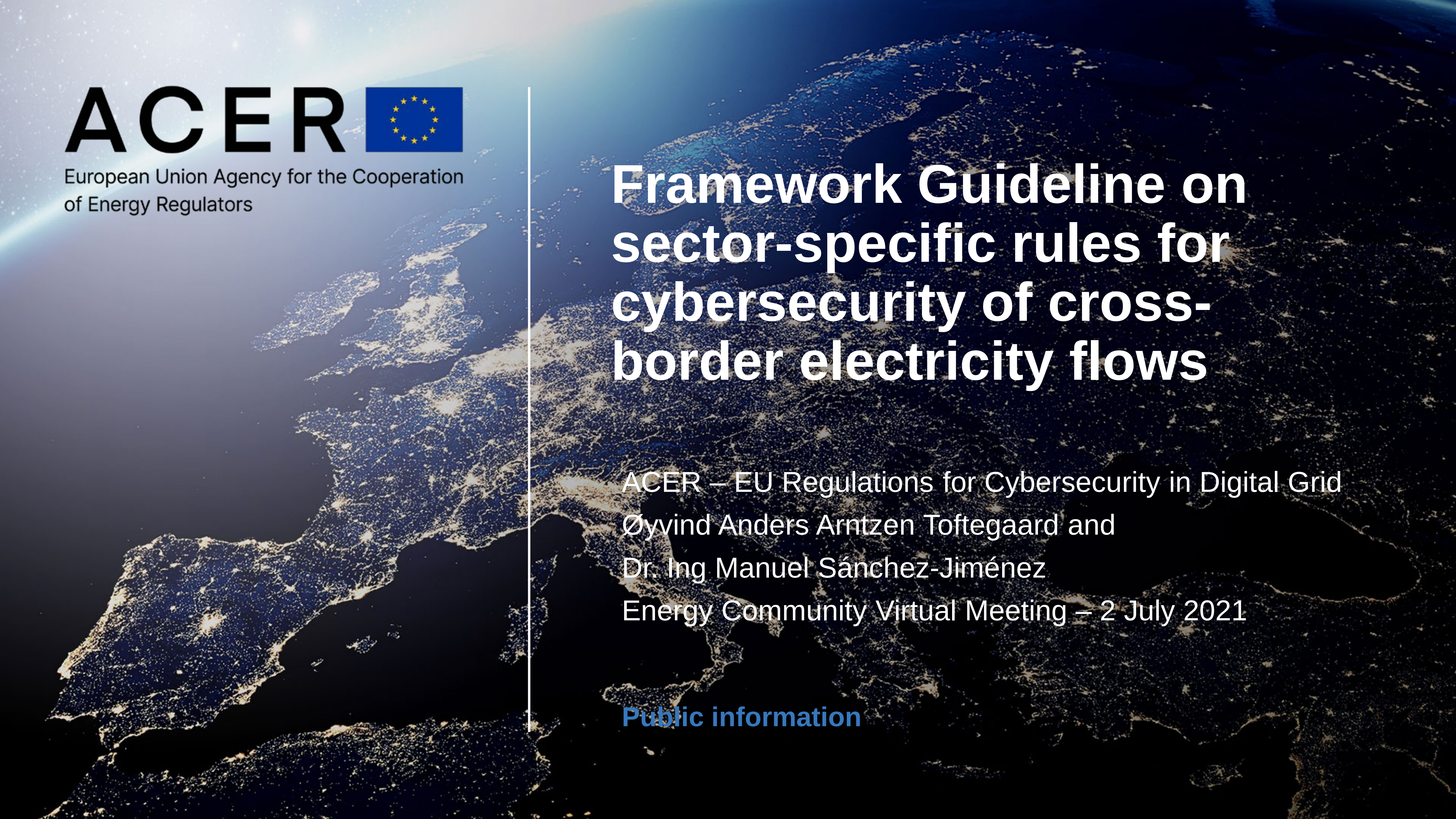


ACER

European Union Agency for the Cooperation of Energy Regulators

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

ACER – EU Regulations for Cybersecurity in Digital Grid

Øyvind Anders Arntzen Toftegaard and
Dr. Ing Manuel Sánchez-Jiménez

Energy Community Virtual Meeting – 2 July 2021

Public information

1. **Introduction**

2. **Content of the FG**

3. **Next steps**

4. **Discussions**

Introduction - Cross border electricity cyber risk

-reigai.com

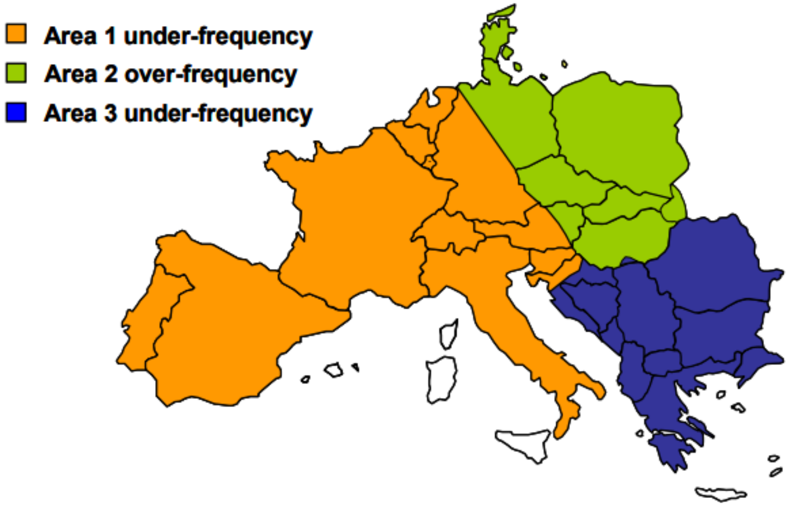
2003: Cascading effect of blackout in France and Switzerland led to blackout in Italy

-tu.no

-db.no

-dt.no

-ba.no



-entsoe.eu

2006: Cascading effects of blackout in Germany led to blackout in several European countries

Introduction – Historic timeline

- **2019:** Electricity Regulation mandates a network code on Cybersecurity
- **2019:** Smart Grid Task Force Expert Group 2 report
- **2020:** Commission’s stakeholder consultation
- **2020:** ENTSO-E/ DSO associations informal interim report
- **28 Jan 2021:** Invitation to ACER to draft framework guideline
- **30 Apr 2021:** FG proposal on public consultation
- **27 May 2021:** ACER webinar on the FG
- **29 June 2021:** End of public consultation

1. Introduction
2. Content of the FG
3. Next steps
4. Discussions

Content of the FG - Scope

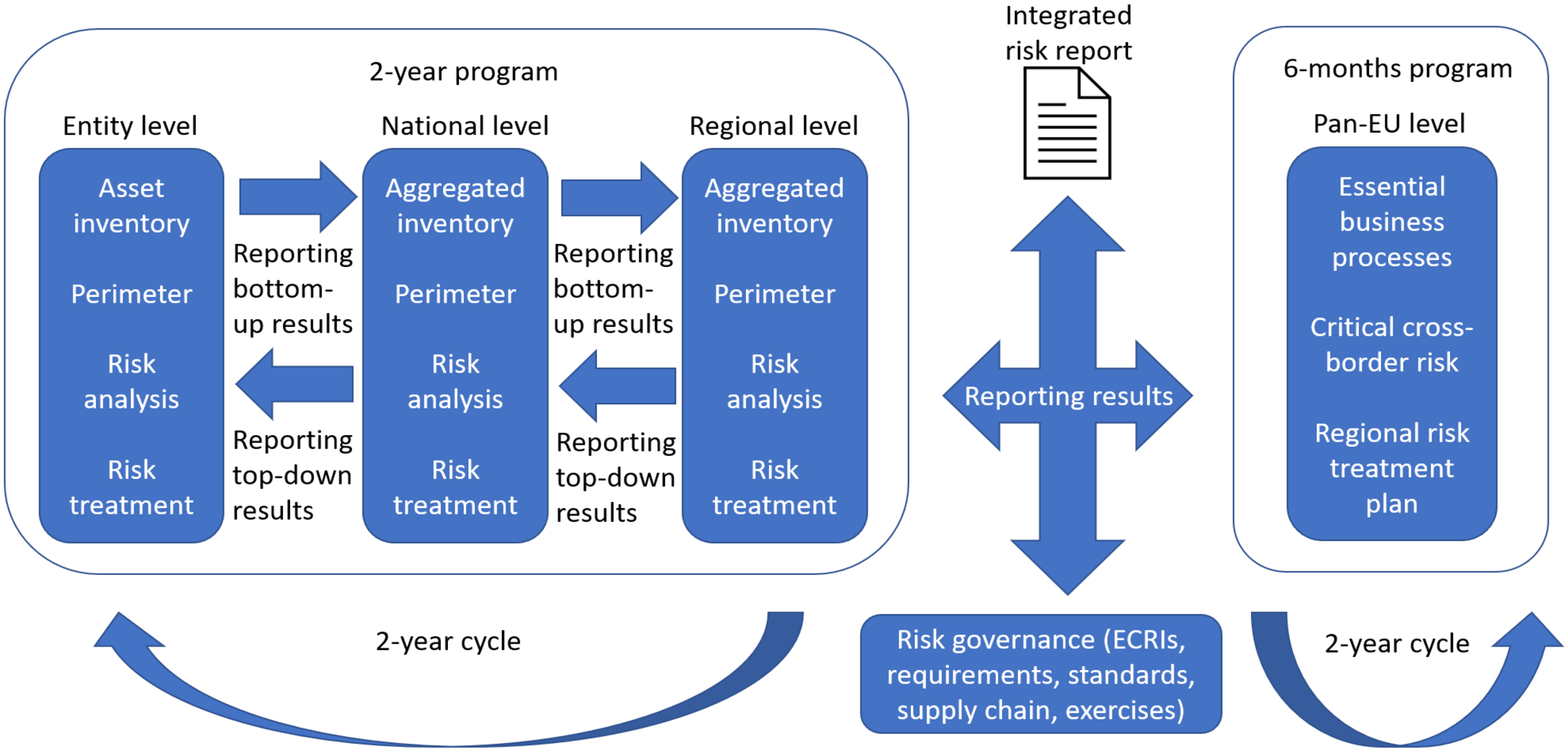
- Scope:
  - Electricity undertakings (as defined in the Electricity Directive),
  - ENTSO-E, EU-DSO, ACER, NRAs,
  - Risk Preparedness NCAs, Electricity CS NCAs, CSIRTs, SOCs,
  - RCCs, and
  - Critical Service Suppliers.

ACER European Union Agency for the Cooperation of Energy Regulators

Content of the FG – Overview of requirements

	Small and Micro Enterprises <50 Employees & <10 Mill Eur	Large Risk Electricity Entities Minimum Cybersecurity Requirements	High Risk Electricity Entities Advanced Cybersecurity Requirements
Basic cyber hygiene	Yes	Implicit	Implicit
Identification of critical products and processes		Yes	Yes
Integrated top-down bottom-up risk assessment		Yes	Yes
Evaluation of critical assets and risks		Yes	Yes
Common security framework including verification of implemented requirements		Yes	Yes
Establish SOC or engage with MSSP		Yes	Yes
Security verification of essential products			Yes
Participation in cyber exercises			Yes

Content of the FG - Cross border risk assessment



Content of the FG - Classification of entities

Apply Electricity Cybersecurity Risk-Index (ECRI) Caps to classify high-risk and large-risk electricity entities

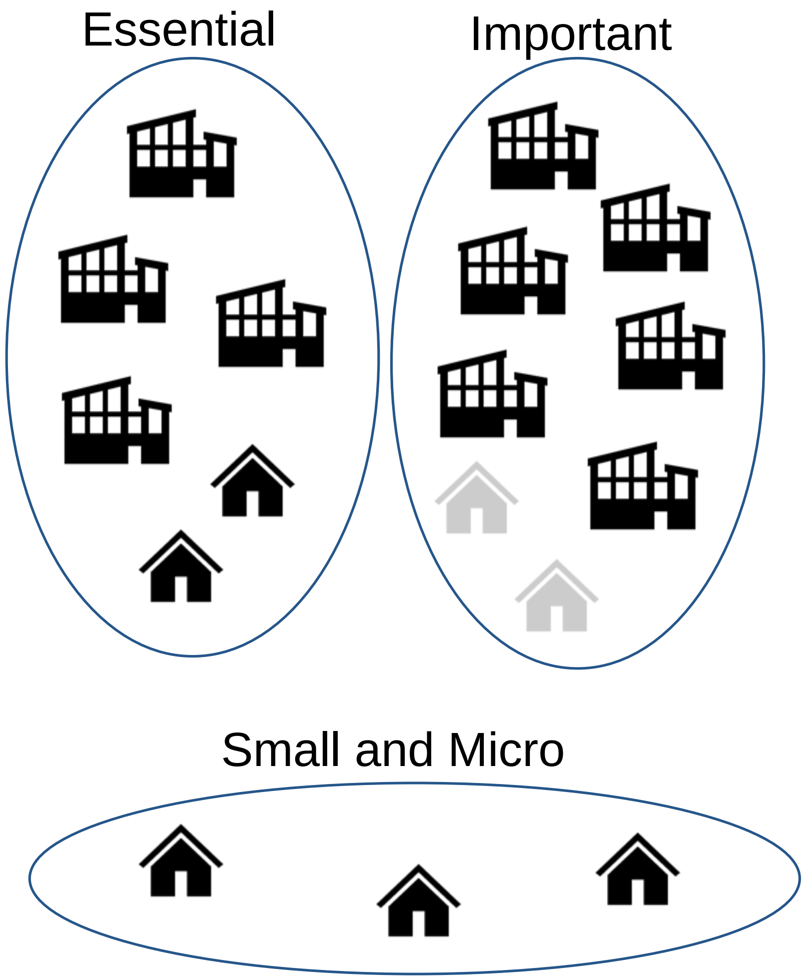
- ECRI score based on information asset inventory and risk assessment

Transitional measures for the classification of entities

- Transitional list of high-risk and large-risk electricity entities

Small and Micro enterprises may be classified too

- Primary as high-risk electricity entities



Content of the FG - Common cybersecurity framework

The implementation of the security requirements shall be verifiable

1.

Or Other Certifiable Standard

2.

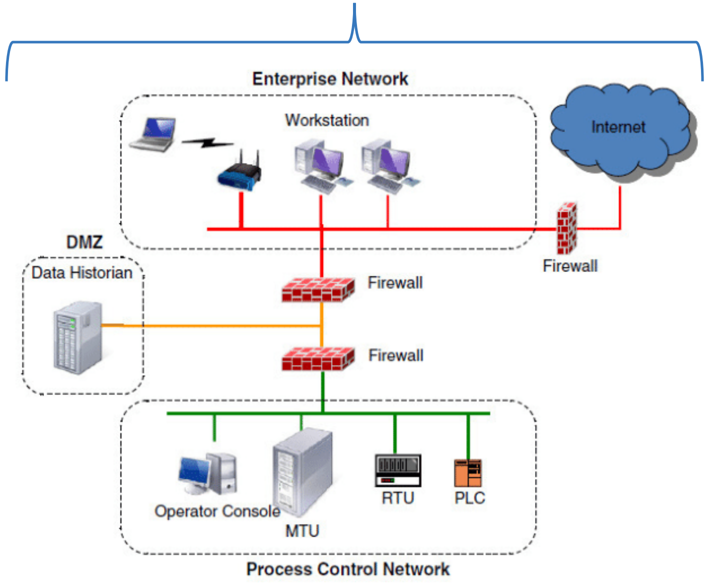
Peer Review

3.

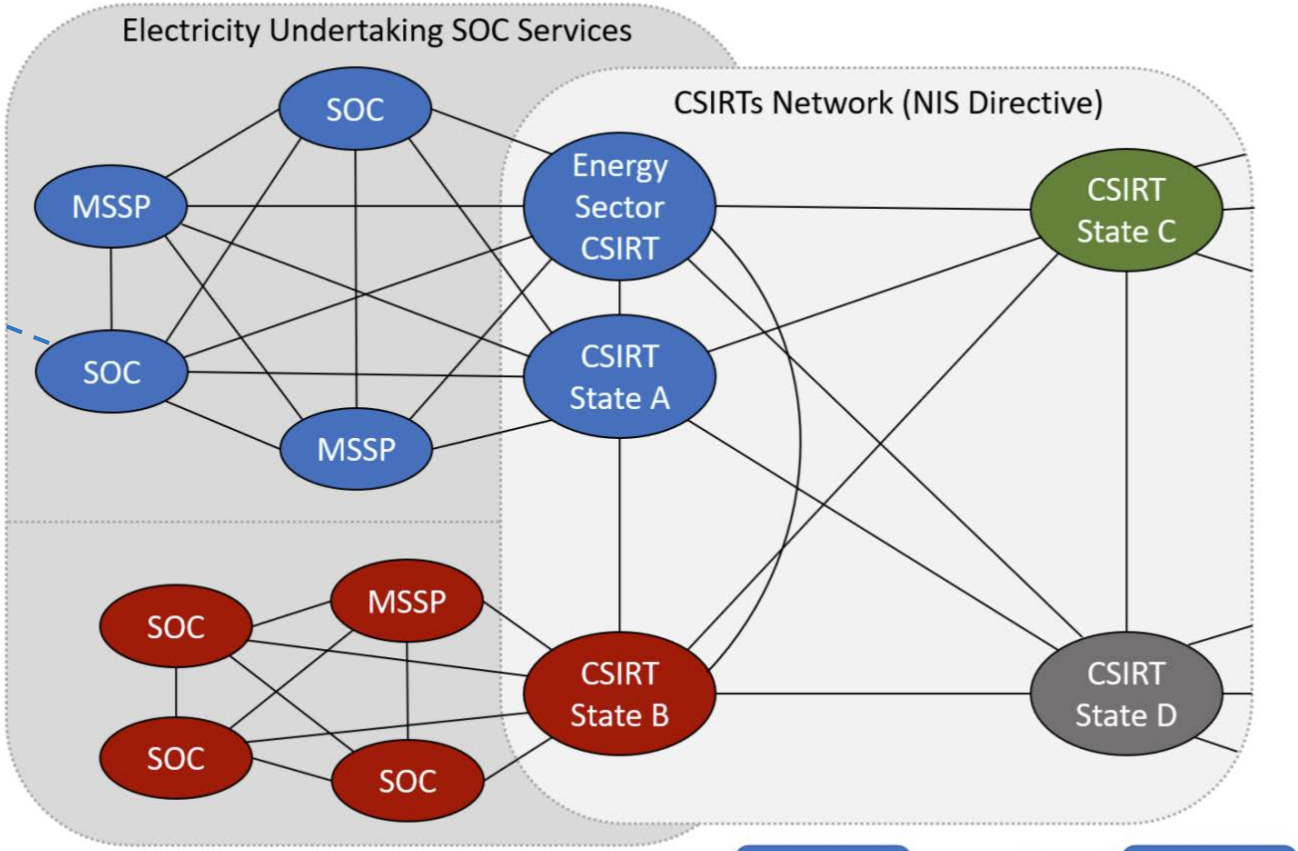
Approved National Government Schemes

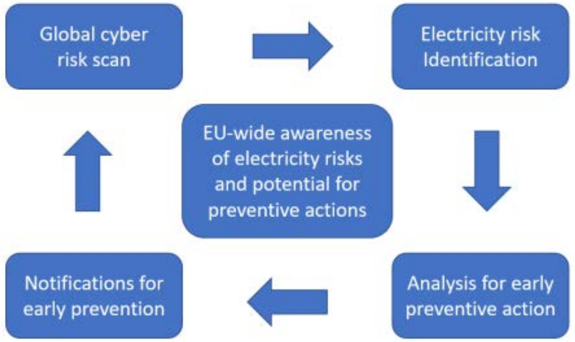
Content of the FG: Information sharing, incident and crisis management

-mdscs.sa



Rysavy, Ondrej & Rab, Jaroslav & Sveda, Miroslav. (2013)




Global cyber risk scan
Electricity risk Identification
EU-wide awareness of electricity risks and potential for preventive actions
Analysis for early preventive action
Notifications for early prevention

Content of the FG - Participation in cyber exercises

-tussa.no

-bladet.no

Content of the FG - Information protection scheme

An information protection scheme shall be established for protection of information exchanged in the context of the Network Code, including:

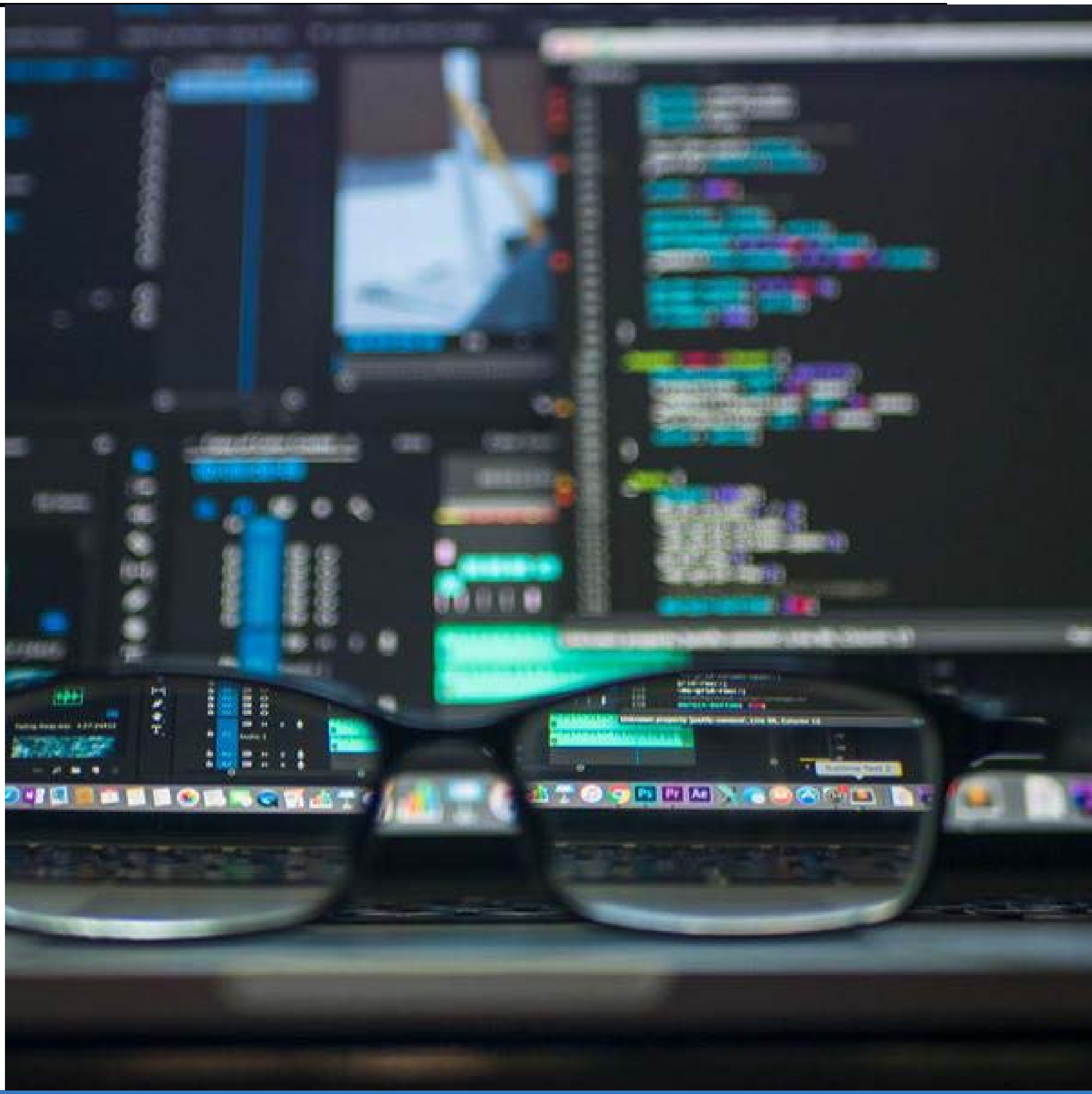
- **An information classification scheme**
- **General information protection rules**

Content of the FG - Monitoring, benchmarking and reporting

- **Monitoring effectivity of security requirements**
  By ACER, ENTSO-E and EU-DSO

- **Benchmarking with focus on cost-efficiency**
  By ACER supported by NRAs

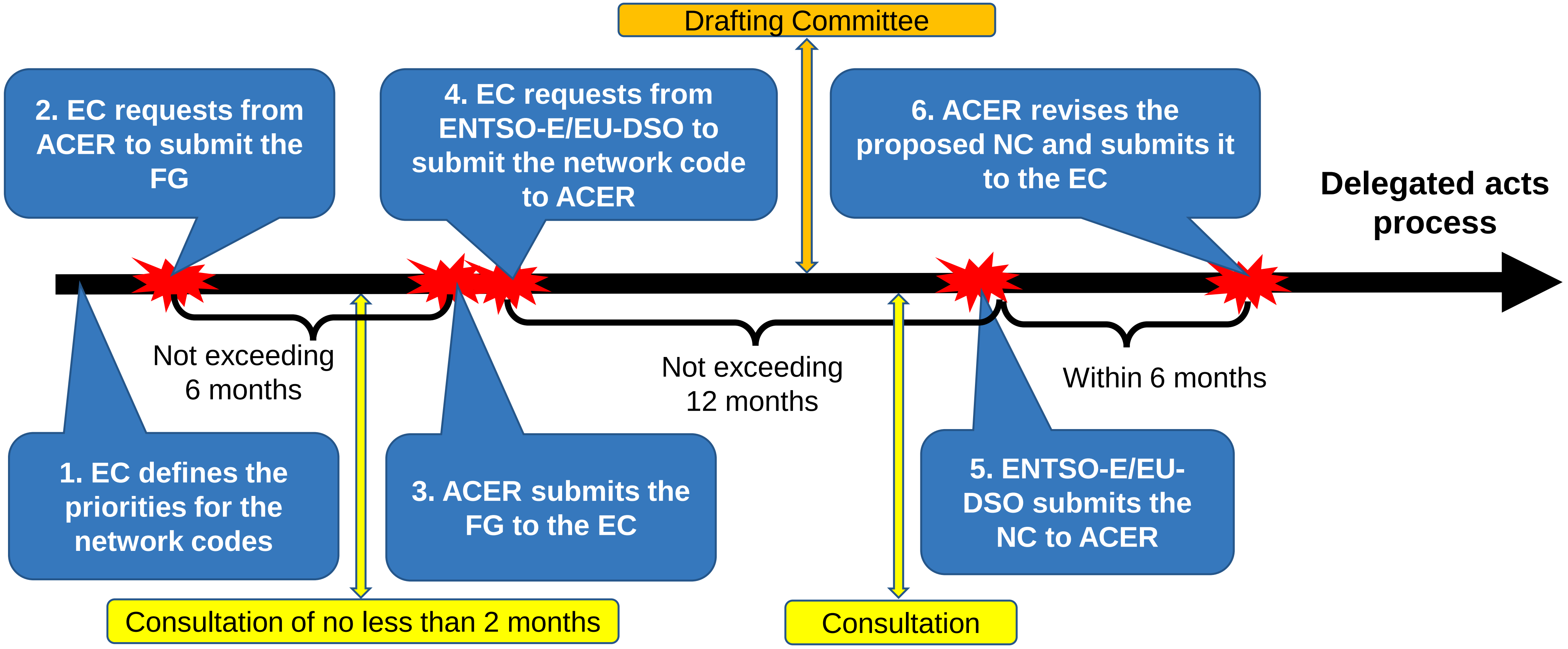
- **Reporting on security status and trends**
  By ENTSO-E, EU-DSO and stakeholders



1. Introduction
2. Content of the FG
3. **Next steps**
4. Discussions

Next steps – Time schedule

- **General timeline as set out in Article 59 of [REGULATION (EU) 2019/943]**



Drafting Committee

2. EC requests from ACER to submit the FG

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

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

Delegated acts process

Not exceeding 6 months

Not exceeding 12 months

Within 6 months

1. EC defines the priorities for the network codes

3. ACER submits the FG to the EC

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

Consultation of no less than 2 months

Consultation

Summary

- **We need sector specific cybersecurity legislation to prevent cross border cybersecurity risk**
- **The FG will provide guidance to ENTSO-E and EU-DSO entity for the drafting process**
- **The FG proposes mainly**
  - **Cybersecurity requirements for a wide scope of organisations**
  - **Cross border electricity cybersecurity risk assessment**
  - **A system for common cybersecurity requirements and its verification**
  - **A system for information sharing, incident- and crisis management**
  - **Advanced requirements in form of product verification and cyber exercises**
- **We are now evaluating responses after the public consultation and drafting a final deliverable**

1. Introduction
2. Content of the FG
3. Next steps
4. **Discussions**

Øyvind Arntzen Toftegaard
arntzoy@acer.europa.eu

Dr. Ing Manuel Sánchez-Jiménez