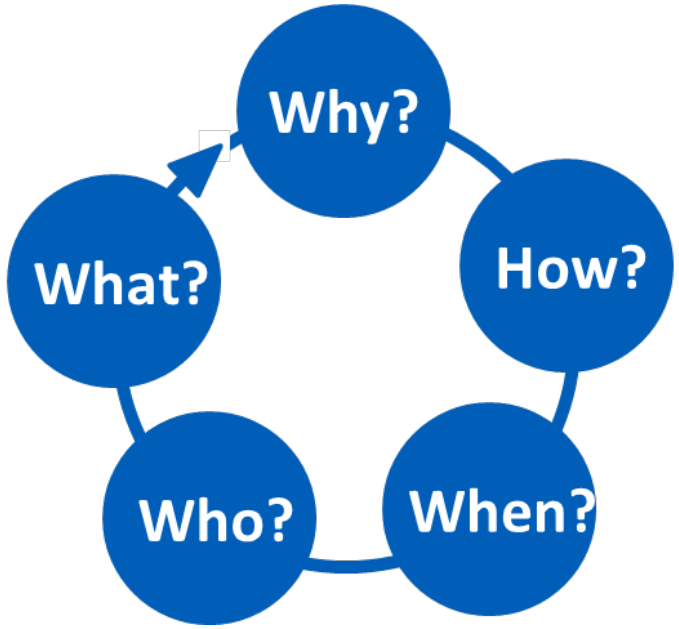
Network Code Cybersecurity – The grid operators view

Andréa FOSCHINI & Olivier CLEMENT

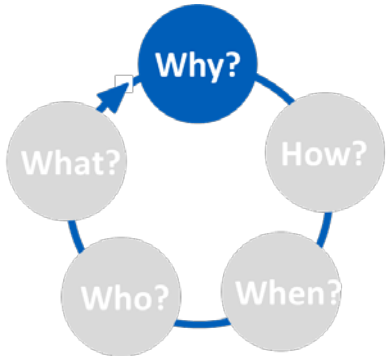
21/10/2021

The NCoCS in

5 questions



Why ?



Is the energy sector special in cybersecurity implementation?

Real-time requirements

...simply cannot be addressed by standard cyber security solutions like authentication or encryption.

Cascading effects

...can trigger black-outs in other sectors and countries.

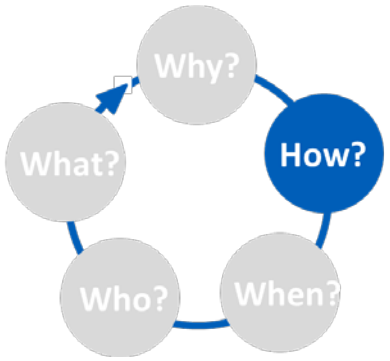
Technology mix

*...creates risks from **legacy** components designed when cyber security was not an issue, and from new **Internet-of-Things** devices not made with cyber security in mind.*

Urgency to define of a EU-wide cybersecurity regulation for the Energy Sector

1. Threat landscape/level keeps increasing
2. Different levels of maturity EU-wide
3. Guidance is needed for harmonized rules and approaches
4. Collaboration is needed – it is an European Power Grid

How ?

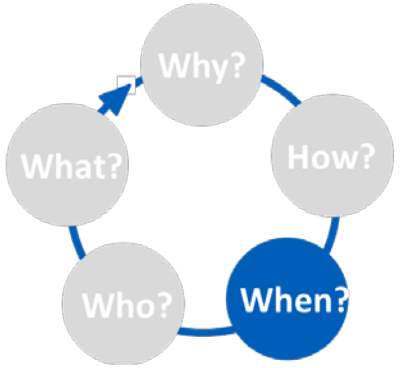


How drafting network codes follows Regulation 714/2009:

- Legally binding / Every entity within the scope will have to comply
- While they will not duplicate national regulation, national regulation have to be consistent. Hence, creating fit-for-purpose network codes is in everyone's interest.
- Stakeholder engagement is crucial*.

**Network Code on Cybersecurity is the first NC to be drafted according to the new CEP rules that explicitly require the establishment of a Drafting Committee (Article 59 para 2 lit 10 Ele-Reg.)*

When ?



Timeline

2019

- Scoping paper — EC
- Informal agreement on work plan — EC, EU-DSO, ACER, ENTSO-E

2020

- Priority list — EC (12 months)
- official letter to start informal work — EC
- Informal drafting and consultation — EC, EU-DSO, ACER, ENTSO-E

NETWORK CODE ON CYBERSECURITY – INFORMAL DRAFTING TEAM

Final Report

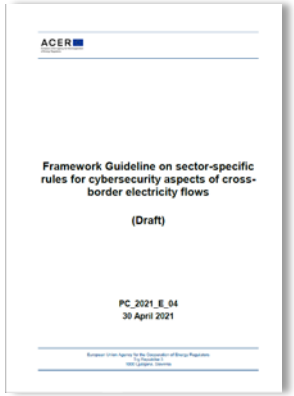
Recommendations for the European Commission on a Network Code on cybersecurity

19 February 2021

The mission of the informal drafting team is to prepare the ground for a future Network Code on cybersecurity for the electricity sector.

2021

- Final informal draft — EU-DSO, ENTSO-E
- EU-DSO established — EU-DSO
- Framework guidelines — ACER (2 months)
- official drafting network code — EU-DSO, ENTSO-E (3 months)
- Agency review — ACER (2 months)


ACER

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

(Draft)

PC_2021_E_04
30 April 2021

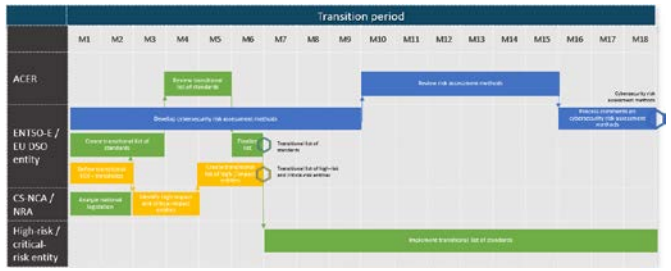
2022

- Impact assessment — EC
- Procedure to adopt delegated act — EC

2023

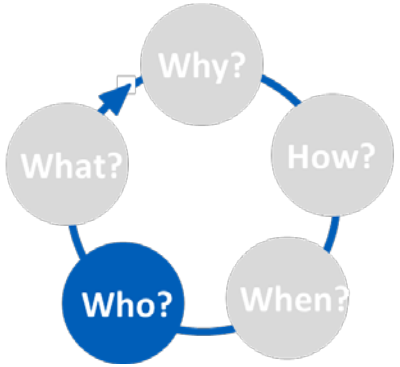
Implementation of the Network Code on Cybersecurity

TRANSITION PERIOD (18 MONTHS)



Full Enforcement

Who ?

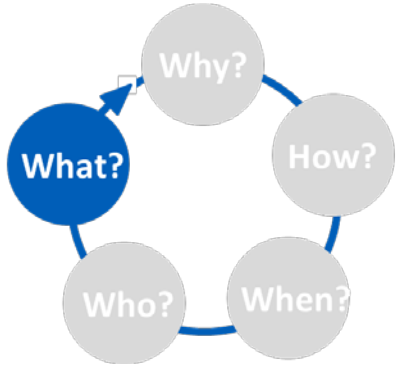


#	Table 1. Entity definition
1	Electricity undertakings as defined in Article 2(57) of the Electricity Market Directive
2	NEMOs as defined in Article 2(7) and (8) of Electricity Market Regulation
3	Electricity digital market platforms as defined in this Framework Guideline
4	Critical service providers 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

From the definition in the Framework Guidelines…

… to the «word cloud» of the Legal Text

What ?



I. General provisions (monitoring & Benchmarking)

II. Governance for cybersecurity risk Management

III. Risk management at Union and regional level

IV. Common electricity cybersecurity Framework

V. Risk analysis at Member State Level

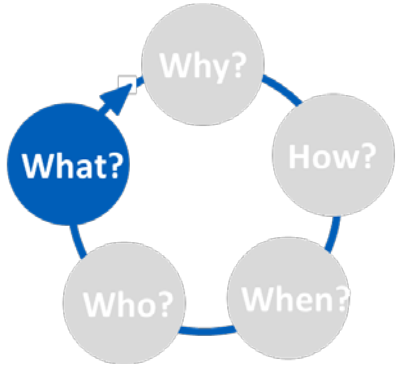
VI. Risk management at entity level

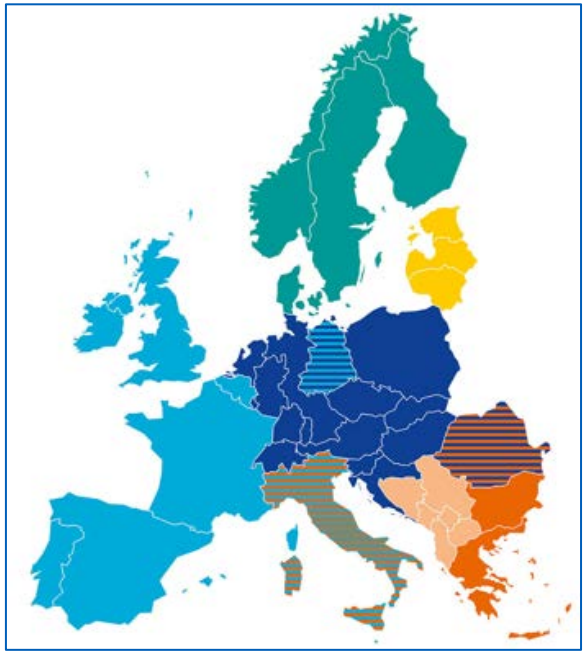
VII. Harmonising product and system requirements and verification

VIII. Essential information flows and Crisis Management

IX. Electricity cybersecurity exercise framework

III – Risk management at Union & regional level





Impact Assessment

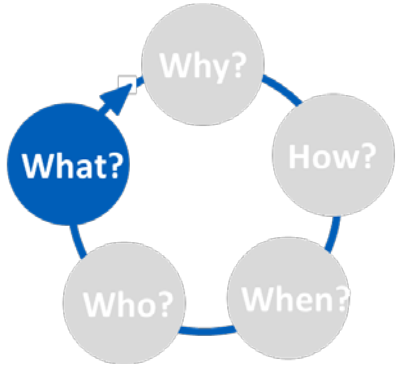
- *Selection of Entity's business process that are high/critical impact at Pan-European level*
- *Definition of treshold for high/ critical impact*
- *Harmonized Risk Matrix*

Regional Cybersecurity Risk Assessment

- *Assessment of Cybersecurity risks on cross-border electricity flows*
- *Regional cybersecurity risk treatment, with minimum cybersecurty controls for mitigation*
- *Residual Risk acceptance*

Risk Assessment Report

IV – Common electricity cybersecurity framework



During Implementation Phase of NCoCS, a Common Electricity Cybersecurity Framework will be developed to enlist minimum cybersecurity that entities will adopt during Risk Treatment phase.

Current draft of NCoCS articulates the framework in four parts:

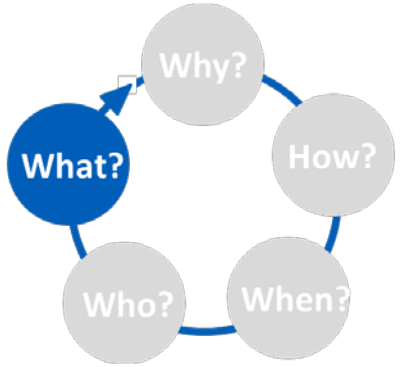
1. **Cyber Hygiene requirements**, applicable to all entities within the scope of the Network Code. Developed *in line with ENISA guidelines*.

2. **Minimum Cybersecurity Controls**, applicable to **all high-impact entities**

3. **Advanced Cybersecurity Controls**, applicable to **all critical-impact entities**

4. Electricity Controls to Standards **Mapping Matrix**, a tool that provides mapping of the Framework requirements and controls against main *International Standards and National Legislative Frameworks* for cybersecurity

V – Risk analysis at member state level



Identification of high and critical impact entities

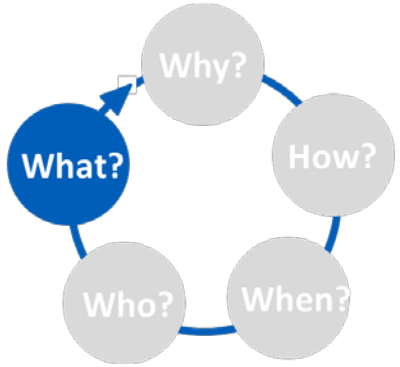
- *Definition of criteria for high and critical impact entities aligned with Electricity Cybersecurity Impact Indices*
- *Identification of high and critical impact entities*

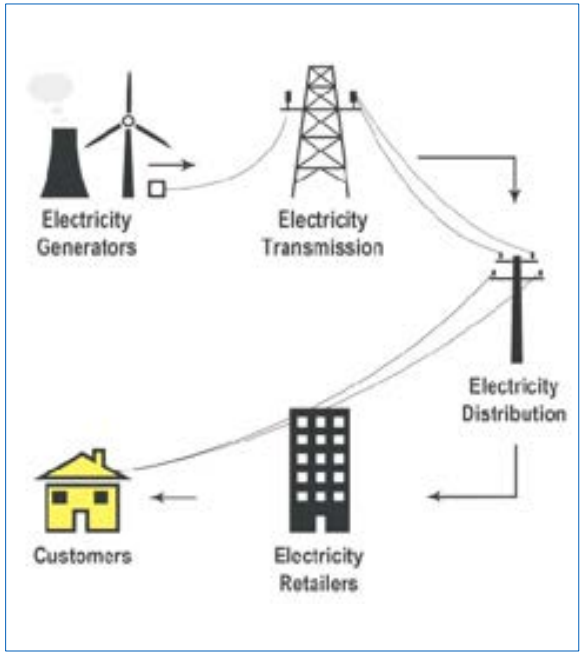
National Cybersecurity Risk Assessment

- *Member state level cybersecurity risk analysis*
- *Evaluation of likelihood of insisting threats*
- *Definition of a verification scheme to audit the implementation of national legislative framework included in ECSMM*

Member State Cybersecurity Risk Analysis Report

VI – Risk analysis at entity level





Cybersecurity Risk Management

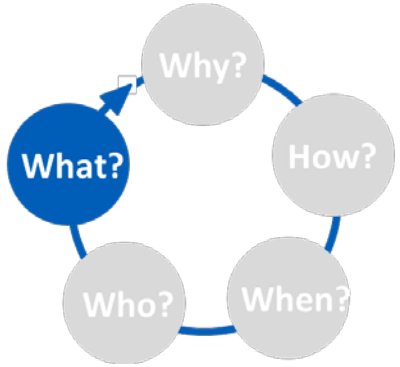
- *Context establishement with identification of the perimeter of high and critical impact assets (supply chain included)*
- *Cyber risk assessment*
- *Cyber risk treatment, with risk-based application of common electricity cybersecurity framework*
- *Acceptance of residual cyber risk*

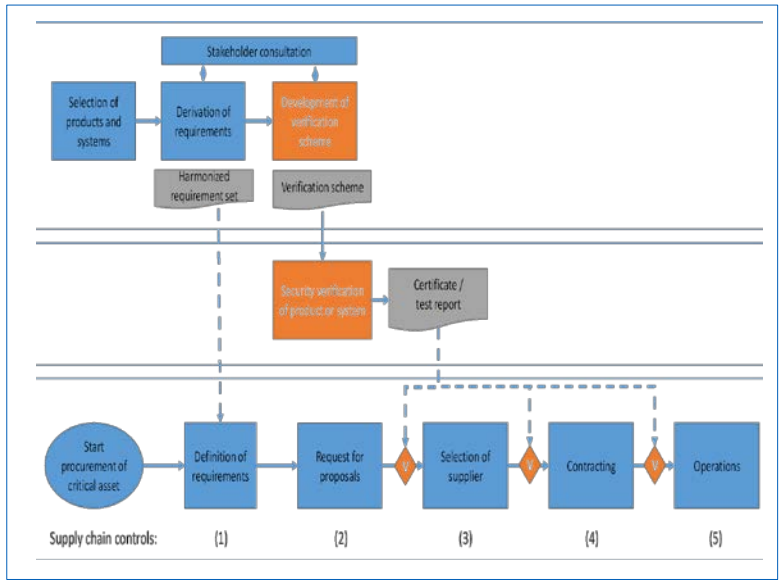
Cybersecurity Management System and Reporting

- *Each high and critical impact entity shall establish a cybersecurity management system based on an international standard*
- *Define and establish policies, processes and adequate resources to efficiently operate of the system.*
- *Provide evidence of compliance to the common electricity cybersecurity framework*

Entity Level Cybersecurity Risk Assessment Report

VII - Supply chain



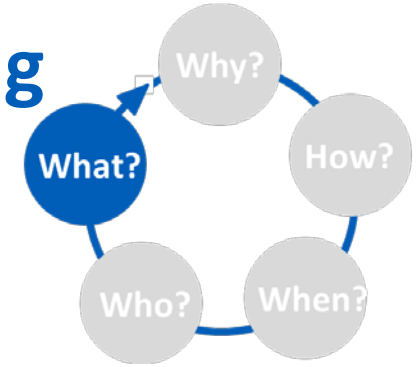


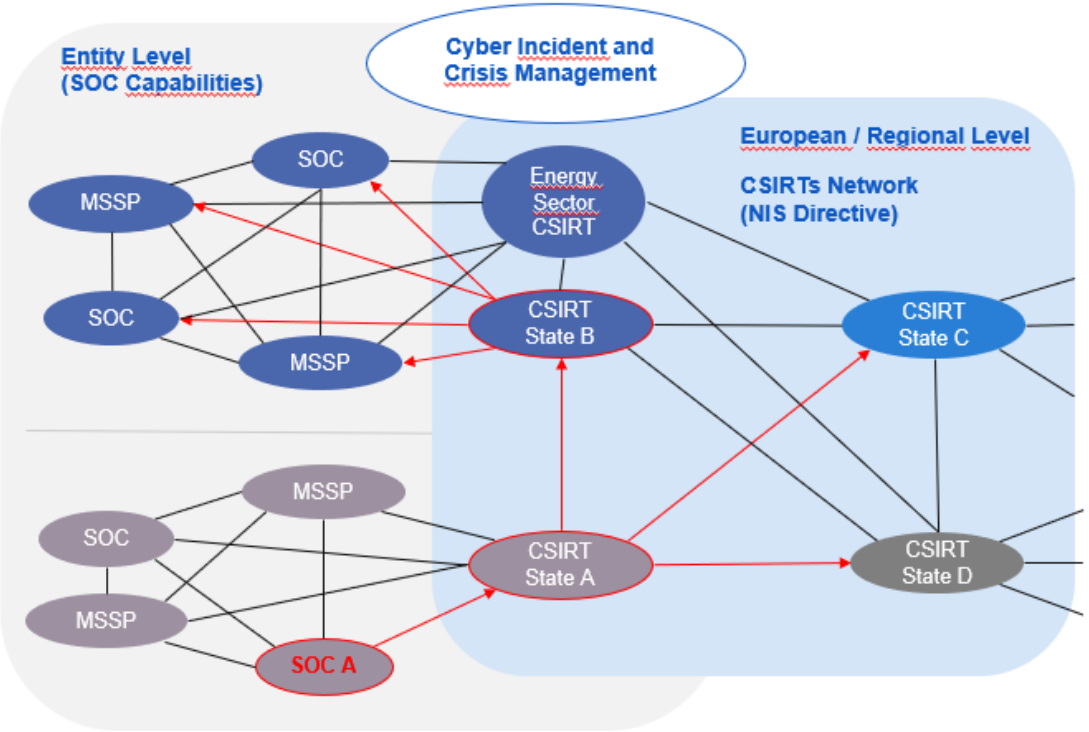
Harmonised Cybersecurity requirements sets → **Verification Methods**

- *Reference architecture*
- *Harmonised cybersecurity requirement sets for ICT products, ICT services and ICT processes*

- *Eu cybersecurity certification scheme*
- *Sector –specific guideline*
- *Penetration testing*

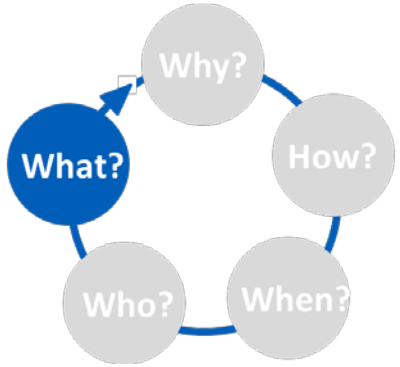
VIII - Incident & crisis management, information sharing



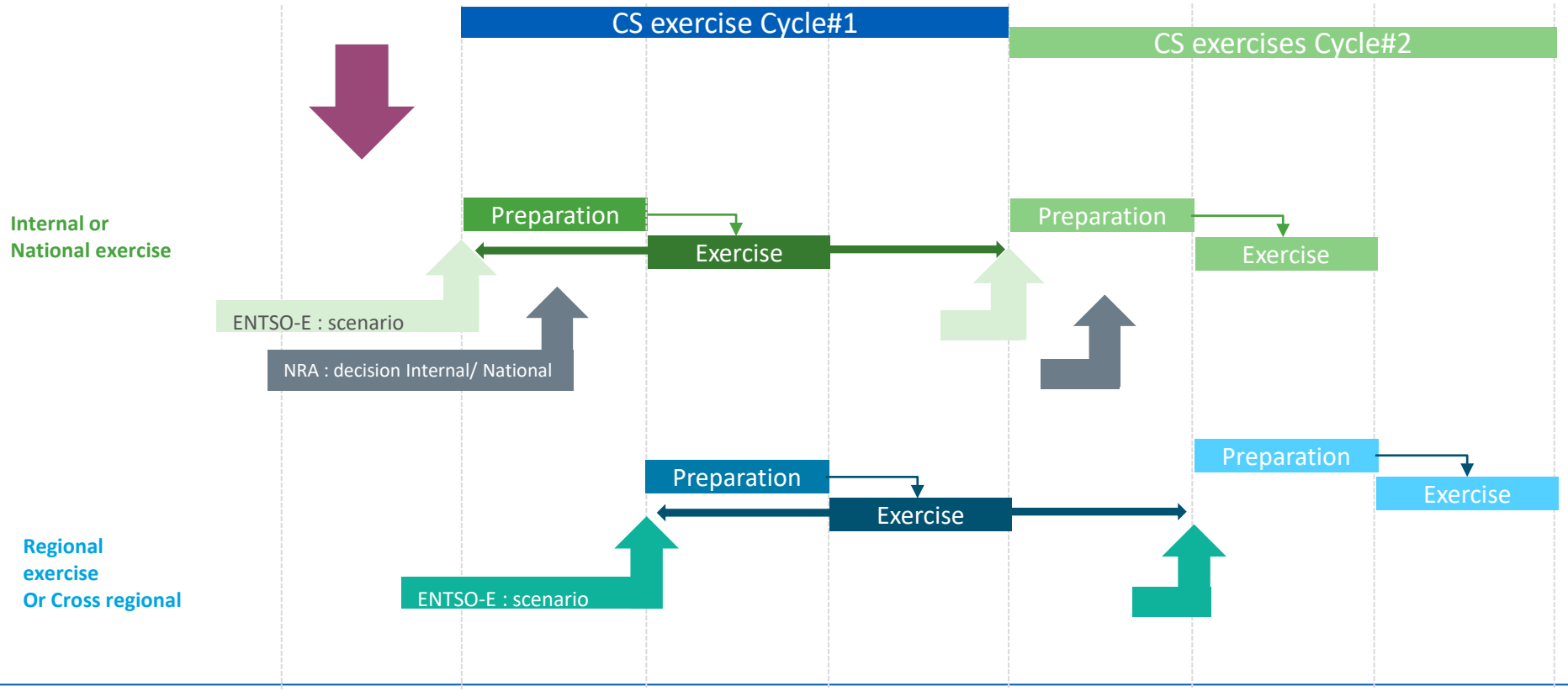


Information sharing	Incident & Crisis Management	ECEWC
• *SOC* • *Reportable CS Incident* *0 days vulnerabilities* *Threats* • *Common tools*	• *ad'hoc coordination Group* • *Electric crisis with Cybersecurity root cause* • *relevant authority support*	*Electricity Cybersecurity Early Warning Capabilities* • *Collect, assess, identify, notify/alert* • *ENISA*

IX - Cybersecurity exercises



Critical-impact electricity entities → **2 exercises every 3 years**



Conclusion, 2 words:

Opportunity
Threats