Cybersecurity nei Sistemi Energetici

Regolazione e Normazione

Giovanna Dondossola

[RSE n. 22009950 - 2022/04/21]

Percorso legislativo/regolatorio

- Riferimenti Europei
  - NIS EU 2016/1148
  - EU 2019/881
  - NIS 2.0
  - Network Code on Cyber Security
  - Standard Internazionali
- Riferimenti Italiani
  - DL 2018/65
  - DL 2019/105 e DPCM attuativi
  - Norme Italiane

Direttiva (UE) 2016/1148 /1

- **Art. 5** criteri per l'identificazione degli **operatori di servizi essenziali**
  a) un soggetto fornisce un servizio che è essenziale per il **mantenimento di attività sociali e/o economiche fondamentali**
  b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi
  c) un incidente avrebbe **effetti negativi rilevanti** sulla fornitura di tale servizio
- **All. II Settori**
  1. **Energia: Energia elettrica, Petrolio, Gas**
  2. Trasporti: aereo, ferroviario, vie d'acqua, su strada
  3. Bancario
  4. Mercati finanziari
  5. Sanitario
  6. Acqua potabile
  7. **Infrastrutture digitali: IXP, DNS, TLD**

Direttiva (UE) 2016/1148 /2

- **Art. 6** Effetti negativi rilevanti – fattori intersettoriali
  a) il **numero di utenti** che dipendono dal servizio fornito dal soggetto interessato;
  b) la **dipendenza di altri settori** di cui all'allegato II dal servizio fornito da tale soggetto
  c) l'impatto che gli incidenti potrebbero avere, in termini di **entità** e di **durata**, sulle attività economiche e sociali o sulla pubblica sicurezza
  d) la **quota di mercato** di detto soggetto
  e) la **diffusione geografica** relativamente all'area che potrebbe essere interessata da un incidente
  f) l'**importanza del soggetto** per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio

Direttiva (UE) 2016/1148 /3

- **Art. 9** Gruppi di intervento per la sicurezza informatica in caso di incidente (**CSIRT**)
  1. Ogni Stato membro designa uno o più CSIRT, che abbia il compito di trattare gli incidenti e i rischi secondo una procedura ben definita. È possibile creare un CSIRT all'interno dell'autorità competente

Direttiva (UE) 2016/1148 /4

CAPO IV

SICUREZZA DELLA RETE E DEI SISTEMI INFORMATIVI DEGLI OPERATORI DI SERVIZI ESSENZIALI

Articolo 14

Obblighi in materia di sicurezza e notifica degli incidenti

Direttiva (UE) 2016/1148 – art. 14 /5

1. Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino **misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi** posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni. Tenuto conto delle **conoscenze più aggiornate in materia**, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente

2. Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure adeguate per **prevenire e minimizzare l'impatto** di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di **assicurare la continuità** di tali servizi

Direttiva (UE) 2016/1148 – art. 14 /6

3. Gli Stati membri provvedono affinché gli operatori di servizi essenziali **notifichino senza indebito ritardo** all'autorità competente o al **CSIRT** gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati. Le notifiche includono le informazioni che consentono all'autorità competente o al CSIRT di determinare qualsiasi **impatto transfrontaliero** dell'incidente. La notifica non espone la parte che la effettua a una maggiore responsabilità

4. Per determinare la rilevanza dell'impatto di un incidente si tiene conto in particolare dei seguenti parametri: a) **il numero di utenti** interessati dalla perturbazione del servizio essenziale; b) **la durata** dell'incidente; c) **la diffusione geografica** relativamente all'area interessata dall'incidente

Direttiva (UE) 2016/1148 – art. 14 /7

5. Sulla base delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, **l'autorità competente o il CSIRT informa l'altro o gli altri Stati membri interessati se l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali in quello Stato membro**. A tal fine l'autorità competente o il CSIRT preserva, conformemente al diritto dell'Unione o alla legislazione nazionale conforme al diritto dell'Unione, la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali, nonché la riservatezza delle informazioni fornite nella sua notifica. **Ove le circostanze lo consentano, l'autorità competente o il CSIRT fornisce all'operatore di servizi essenziali che effettua la notifica di incidente le pertinenti informazioni relative al seguito della notifica stessa, come le informazioni che possano facilitare un trattamento efficace dell'incidente.** Su richiesta dell'autorità competente o del CSIRT, il punto di contatto unico trasmette le notifiche di cui al primo comma ai punti di contatto unici degli altri Stati membri interessati

Direttiva (UE) 2016/1148 – art. 14 /8

6. Dopo aver consultato l'operatore notificante dei servizi essenziali, **l'autorità competente** o il CSIRT **può informare il pubblico** in merito ai singoli incidenti, qualora sia necessaria la sensibilizzazione del pubblico per evitare un incidente o gestire un incidente in corso

7. Le autorità competenti, agendo unitamente nell'ambito del gruppo di cooperazione, possono elaborare e adottare **orientamenti sulle circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti**, compresi i parametri per determinare la rilevanza dell'impatto di un incidente

NIS 2.0 /1

- NIS 2.0 revised Directive proposed on December 2020
- **Essential entities, electricity**
  - Electricity undertakings which carry out the function of ‘supply’
  - Distribution system operators
  - Transmission system operators
  - Producers
  - Nominated electricity market operators
  - Electricity market participants providing aggregation, demand response or energy storage services
- **Essential and important entities (e.g. manufactures)**

NIS 2.0 /2

- all medium-sized and large entities active in the sectors covered by the NIS2 framework would hence have to comply with the security rules put forward in the proposal
- It removes the possibility for Member States to tailor the requirements in certain cases (which had led to much fragmentation with NIS1 implementation)
- It removes the distinction made between OESs and digital DSPs, which currently fall into three categories: online marketplaces, search engines and cloud service providers
- seven key elements that all companies must address or implement as part of the measures they take, including incident response, **supply chain security**, encryption and vulnerability disclosure
- a two-stage approach to incident reporting. Affected companies have **24 hours** from when they first become aware of an incident to submit an initial report, followed by a final report no later than **one month** later

NIS 2.0 /3

- Regarding enforcement, it establishes a minimum list of administrative sanctions (up to €10 million or 2 % of the entities' total turnover worldwide, whichever is higher)

- improve the level of joint situational awareness and the collective capability to prepare and respond, by

  i) taking measures to increase the level of trust between competent authorities;

  ii) by sharing more information

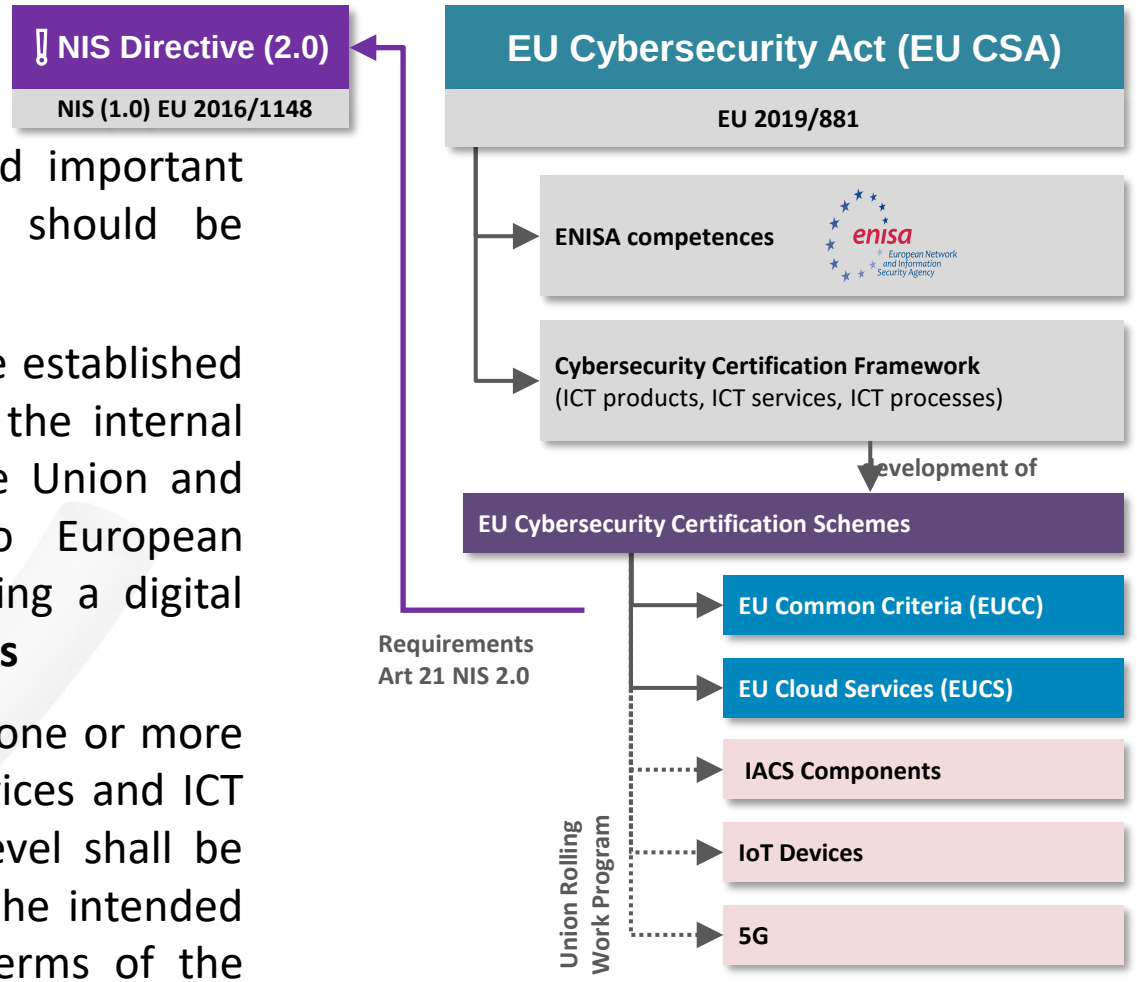
  iii) setting rules and procedures in the event of a large-scale incident or crisis. The proposed new rules improve the way the EU prevents, handles and responds to large-scale cybersecurity incidents and crises by introducing clear responsibilities, appropriate planning and more EU cooperation

NIS 2.0 /4

- It establishes an EU crisis management framework, requiring Member States to adopt a plan and designate national competent authorities responsible for participating in the response to cybersecurity incidents and crises at the EU level
- It establishes an EU Cyber Crises Liaison Organisation Network (EU-CyCLONe) to support the coordinated management of EU-wide cybersecurity incidents, as well as to ensure the regular exchange of information
- It would also strengthen the role of the **NIS Cooperation Group** in making decisions and increasing cooperation between Member States. Member States would still be required to adopt a national cybersecurity strategy and to designate one or more national competent authorities to supervise compliance with the directive; and to designate CSIRTs to handle incident notifications and single points of contact (SPOC) to act as a liaison point with other Member States

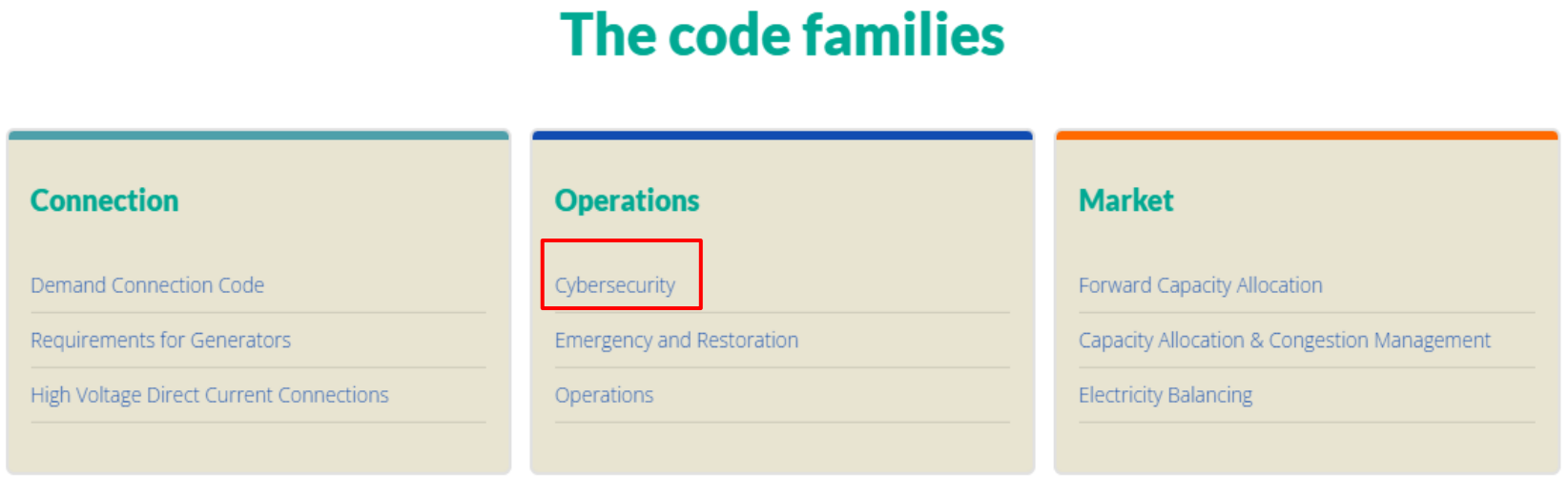
Direttiva (UE) 2019/881

- Mandate to ENISA for the definition of the European Framework of cybersecurity certification
- Articles 46-64 are related to certification
- Art. 21 The use of certification schemes by essential and important entities to ensure compliance with the NIS Directive should be mandatory
- The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a **harmonised approach** at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for **ICT products, ICT services and ICT processes**
- A European cybersecurity certification scheme may specify one or more of the following **assurance levels** for ICT products, ICT services and ICT processes: **'basic', 'substantial' or 'high'**. The assurance level shall be **commensurate with the level of the risk** associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident



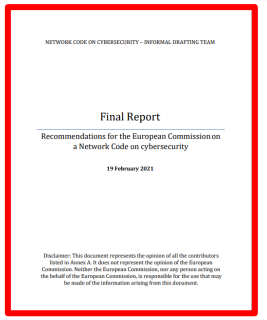
Codice di Rete Europeo /1

- Set of rules drafted by ENTSO-E and in the future EU-DSO with guidance from ACER
- Adopted by the European Commission



Codice di Rete Europeo /2

- Started in 2019
- Final informal EU-DSO and ENTSO-E report issued on February 2021
  - Aligned with NIS 2.0


NETWORK CODE ON CYBERSECURITY – INFORMAL DRAFTING TEAM

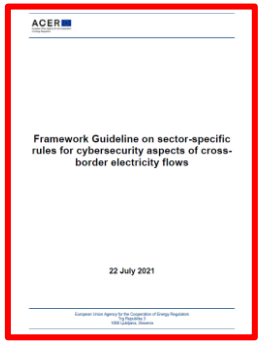
Final Report

Recommendations for the European Commission on a Network Code on cybersecurity

19 February 2021

Disclaimer: This document represents the opinion of all the contributors listed in Annex A. It does not represent the opinion of the European Commission. Neither the European Commission, nor any person acting on the behalf of the European Commission, is responsible for the use that may be made of the information arising from this document.

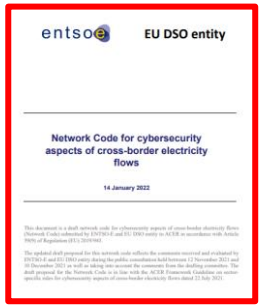
- Framework guidelines from ACER issued on July 2021


ACER

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

22 July 2021

- Legal text delivered to ACER on January 2022
- Expected to be adopted by the EC in 2023
- Full enforcement in two years


entsoe EU DSO entity

Network Code for cybersecurity aspects of cross-border electricity flows

14 January 2022

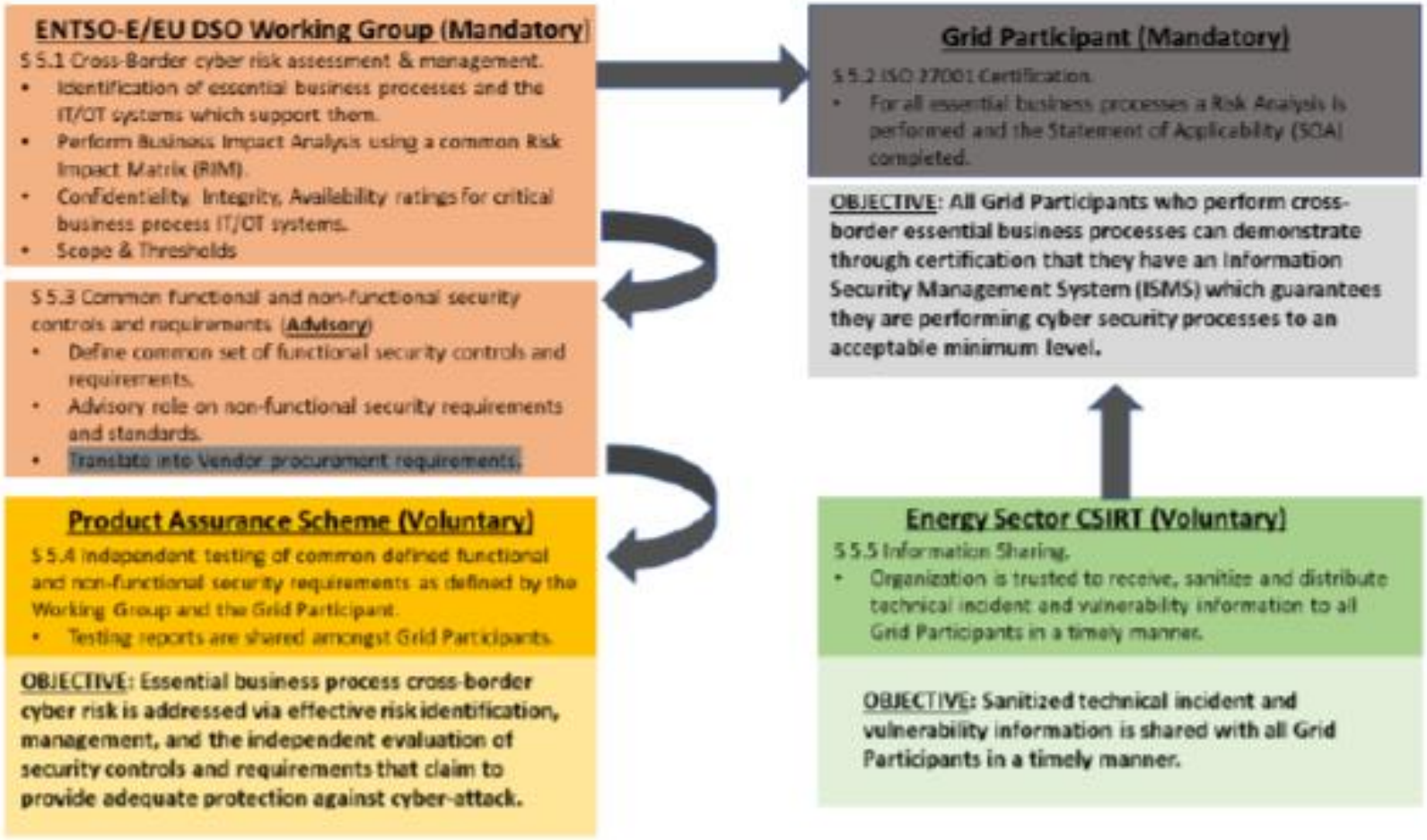
Codice di Rete Europeo /3

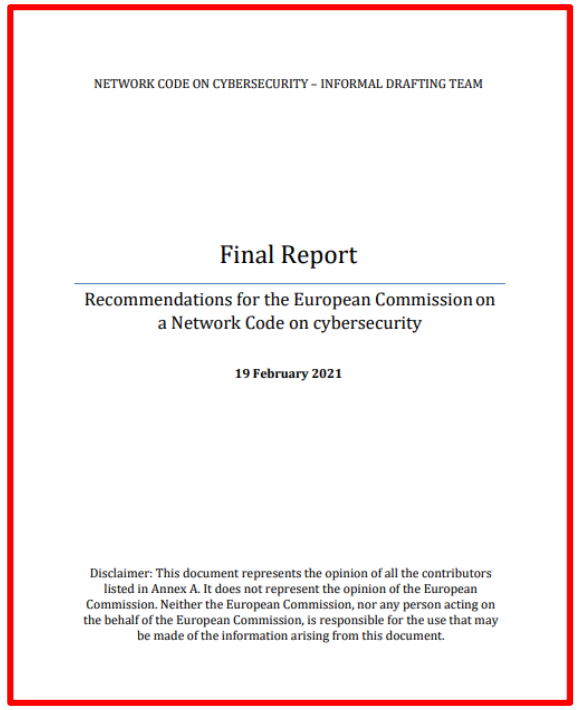
[Cybersecurity (entsoe.eu)]

NC CS drafting status

Timeline

Codice di Rete Europeo /4





NETWORK CODE ON CYBERSECURITY – INFORMAL DRAFTING TEAM

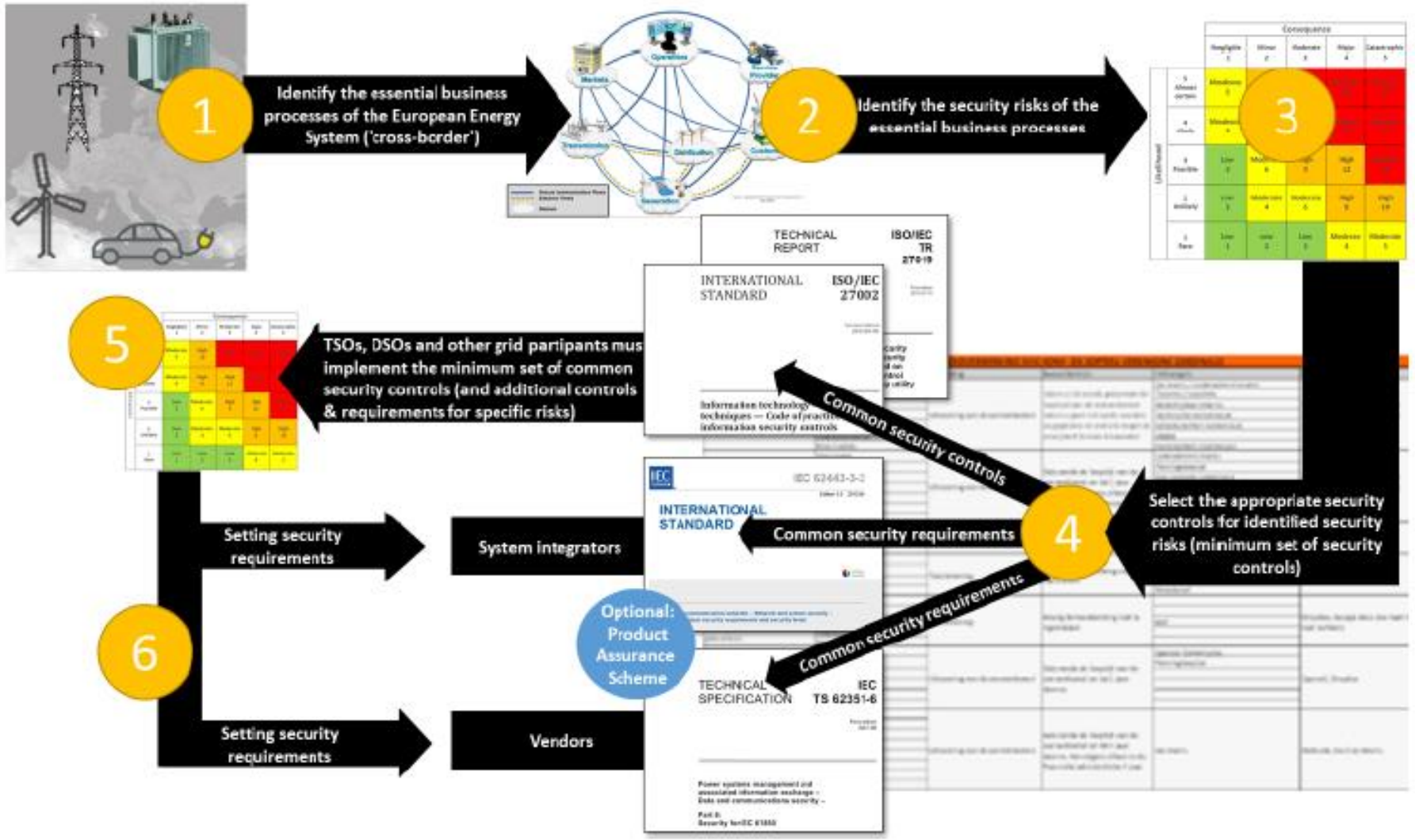
Final Report

Recommendations for the European Commission on a Network Code on cybersecurity

19 February 2021

Disclaimer: This document represents the opinion of all the contributors listed in Annex A. It does not represent the opinion of the European Commission. Neither the European Commission, nor any person acting on the behalf of the European Commission, is responsible for the use that may be made of the information arising from this document.

Codice di Rete Europeo /6



Standard internazionali /1

IEC SyC Smart Energy – Cyber Security Task Force

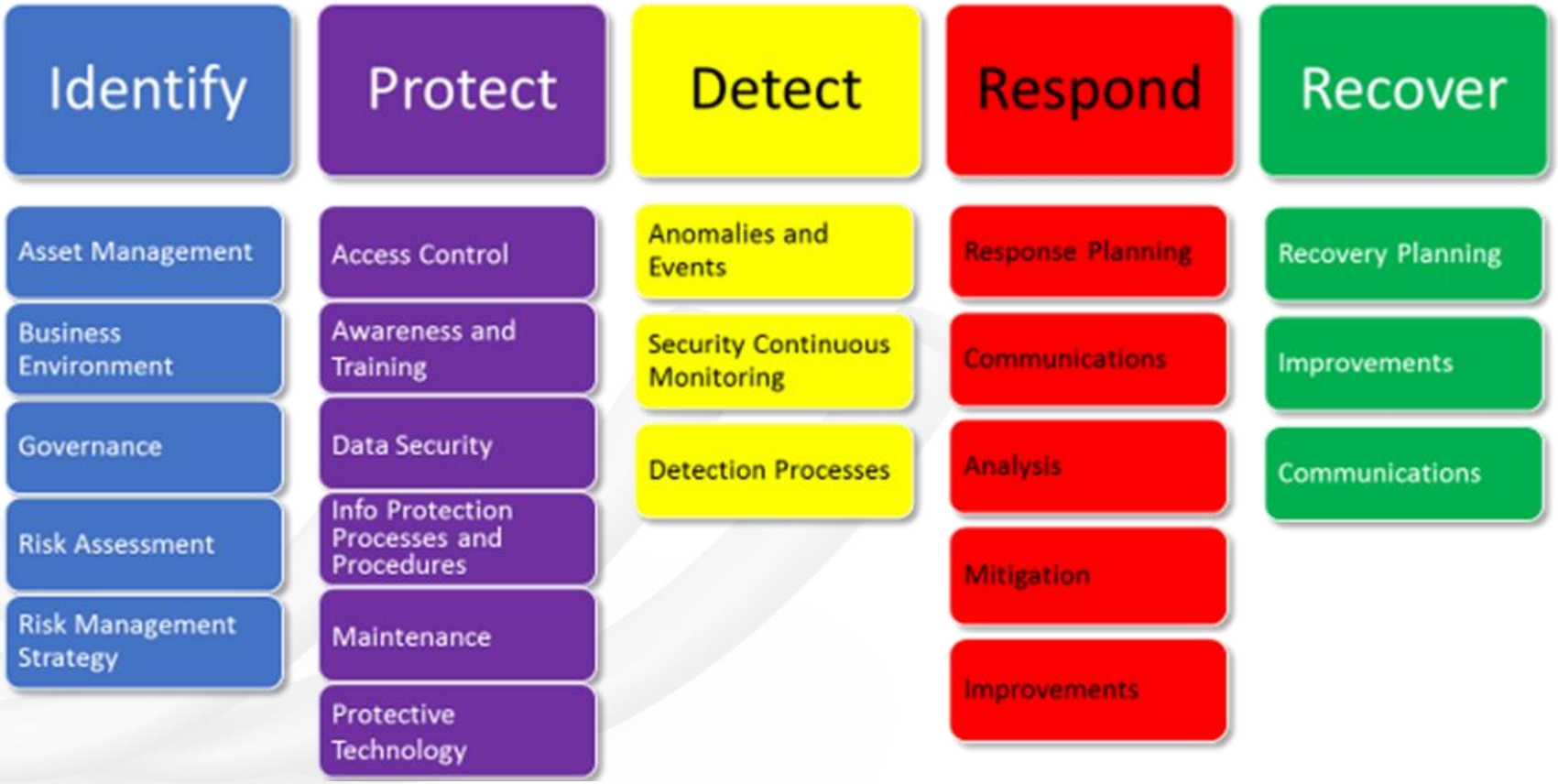
Cyber Security Standards and Guidelines that Apply to Smart Energy Operational Environments

Area (Focus)	Organizational (What)	Technical (How)	Process towards Compliance
General IT Security Reflecting Business Requirements	ISO/IEC 27001 Security Requirements ISO/IEC 27005, NIST SP800-39, ISO 31000 Risk Assessment NIST Cyber Security Framework ISO/IEC 27002, 27019 Security controls	Internet Standards Directory svcs X500 LDAP RFC 4511 PKI, X509 OCSP RFC 6960 GDOI RFC 6407 EST RFC 7030 SCEP ... IPSec RFC 1827 TLS RFC 5246 SNMP RFC 3418 Syslog RFC 5424 OAuth RFC 6749 Cloud Services XML ...	ISO/IEC 27001 Certification (ISO/IEC 27002/27019) ISO 22301 Business Continuity Cybersecurity Capability Maturity Model (C2M2) *(for determining the degree of compliance)*
Energy Systems Operational Environments (Organizational and Procedural Security Controls)	NISTIR 7628 Smart Grid security controls IEC 62443-2-3, 2-4, & 4-1 Security programs	IEC 62351 IEC 62351-3 to 6 Security for protocols IEC 62351-7 Network & Sys Mgmt (SNMP) IEC 62351-8 Access control (RBAC) IEC 62351-9 Key management IEC 62351-10 Security Architecture IEC 62351-11 Security for XML Files IEC 62351-14 Security logging IEC/TR 62351-90-2 Deep packet inspection	IECEE CMC TF Cybersecurity for IEC 62443 2-4, 4-1 *(in progress)*
Energy Systems Operational Technologies (Technical Security Controls and Techniques)	IEC 62443-3-3 System security controls IEC/TR 62351-12 Resilience of power systems with DER IEC 62443-4-2 Security for products	IEC 62325-503 Energy Market Security	IECEE CMC TF Cybersecurity for IEC 62443 3-3, 4-2 *(in progress)* IEEE 1686 Conformance *(future)* IEC 62351-100-xx Conformance *(in progress)*

Standard internazionali /2

Standard internazionali /3

Functions and categories



Legislazione italiana /1

- Il **decreto-legge n. 65**, entrato in vigore il 24 Giugno 2018, costituisce l'attuazione italiana della Direttiva europea NIS (EU 2016/1148)

- Un primo fondamentale provvedimento stabilito dal decreto n.65 è relativo all'identificazione degli **operatori** classificati come fornitori **di servizi essenziali**, quali quelli energetici, soggetti agli **obblighi** in materia di sicurezza e notifica degli incidenti indicati dall'**Art. 14**, e alle relative **sanzioni amministrative** in caso di inadempienza di cui all' **Art. 21**

- L' Art.21 stabilisce che gli operatori dei servizi essenziali che risultano inadempienti agli oblighi stabiliti dalla legge nazionale sono soggetti a sanzioni pecuniarie che, a seconda dei casi, variano da € 12,000 a € 150,000

Legislazione italiana /2

- Il **decreto-legge n. 105**, approvato il 21 Settembre 2019 dal Consiglio dei Ministri, modificato e convertito dal **decreto per la legge di conversione n.133** entrato in vigore il 21 Novembre 2019, introduce disposizioni urgenti in materia di *perimetro di sicurezza nazionale cibernetica*
- Il perimetro riguarda tutte le ***infrastrutture critiche, private e pubbliche aventi una sede nel territorio nazionale***, che assicurano un ***servizio essenziale per le attività civili, sociali o economiche fondamentali per la nazione***, e che per la fornitura di tale servizio si avvalgono di *reti, sistemi informativi e servizi informatici* dal cui malfunzionamento o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale
- L' **Art.1** stabilisce che entro quattro mesi dall'entrata in vigore della legge di conversione è richiesta l'***individuazione delle amministrazioni, degli enti e degli operatori*** inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto degli obblighi stabiliti dalla legge

Legislazione italiana /3

- L' **Art.1** stabilisce che **entro dieci mesi** dall'entrata in vigore della legge di conversione il Ministero dello Sviluppo Economico definisce ***le procedure*** che i soggetti privati del settore energia devono seguire **per la *notifica degli incidenti cyber al gruppo di intervento per la sicurezza informatica (CSIRT)*** già prevista dal D.L. n.65
- Vengono inoltre stabilite le ***misure organizzative, di gestione del rischio e di mitigazione e gestione degli incidenti*** che garantiscono elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici ***tenendo conto degli standard definiti a livello internazionale ed europeo***

Legislazione italiana /4

- ***I soggetti individuati che intendono approvvigionarsi di beni, sistemi e servizi ICT devono darne comunicazione al CVCN, unitamente alla valutazione del rischio associato all'oggetto della fornitura in relazione all'ambito di impiego***
- **Entro al massimo sessanta giorni** dalla comunicazione, ***il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software*** da effettuare in collaborazione con i soggetti individuati secondo un approccio gradualmente crescente nelle verifiche di sicurezza
- Tali condizioni e test di hardware e software ***condizionano i relativi bandi di gara e contratti*** al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN
- ***L'onere dell'effettuazione delle attività di test risulta a carico dei soggetti inclusi nel perimetro di sicurezza nazionale***

Legislazione italiana /5

- **Il CVCN assume il compito di *elaborare le misure di sicurezza che riguardano l'affidamento di forniture di beni, sistemi e servizi ICT, definisce le metodologie di verifica e di test, effettua le verifiche avvalendosi di laboratori accreditati dallo stesso CVCN, se necessario elabora ed adotta nuovi schemi di certificazione cibernetica tenendo contro degli standard definiti a livello internazionale ed europeo***

- Il mancato adempimento da parte dei soggetti inclusi nel perimetro degli obblighi previsti dalla legge comporta **sanzioni amministrative e pecuniarie fino a 1.8 Meuro**

Legislazione italiana /6

- Misure preventive e di risposta agli attacchi cyber che coinvolgono il piano legale, tecnologico e organizzativo
- Misure preventive
  - misure di sicurezza
  - screening tecnologico CVCN
  - ispezioni e sanzioni
  - istituzione della figura del security manager aziendale
- Misure di risposta
  - La notifica deve avvenire **entro 6 ore dal primo incidente** ad uno degli asset del perimetro
  - **La Presidenza del Consiglio ha la facoltà di intervenire in merito ai dispositivi compromessi**

Legislazione italiana /7

- DPCM n. 131 30/07/2020
  - **Regolamento in materia di perimetro di sicurezza nazionale cibernetica**
  - Criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro
  - Criteri che i soggetti inclusi devono adottare per la predisposizione dell'elenco delle reti, dei sistemi e dei servizi, loro architettura e componentistica
- DPR n. 54 5/02/2021
  - **Regolamento CVCN**
  - Procedure, modalità e termini di funzionamento del CVCN
  - Criteri tecnici per l'individuazione delle categorie e dell'elenco dei beni, dei sistemi e dei servizi a cui si applica la procedura di valutazione
  - Procedure, modalità e termini con cui le autorità competenti effettuano le verifiche e le ispezioni per l'accertamento del rispetto degli obblighi stabiliti dal DL 105
- DPCM n.81 14/04/2021
  - **Regolamento in materia di notifiche degli incidenti** aventi impatto su reti, sistemi informativi e servizi informatici

Legislazione italiana /8

- DPCM n.82 14/06/2021
  - **Disposizioni urgenti in materia di cybersicurezza**, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale
  - Istituzione dell'**Agenzia per la Cybersicurezza Nazionale** (ACN)

- DPCM 15/06/2021
  - Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica

Legislazione italiana DPCM n. 82 /15

- Art. 7 - **Funzioni dell'Agenzia per la cybersicurezza nazionale**

1. L'Agenzia:

a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, il **coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale** e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento **dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore**;

b) predispone la strategia nazionale di cybersicurezza

c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza

d) è **Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS**, a tutela dell'unità giuridica dell'ordinamento, ed è **competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto**

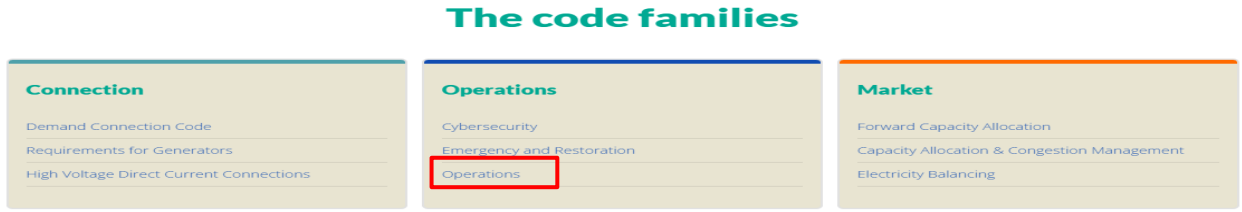
e) è **Autorità nazionale di certificazione della cybersicurezza** secondo quanto specificato dal Parlamento europeo e del Consiglio, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative **all'accertamento delle violazioni e all'irrogazione delle sanzioni**

f) assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico

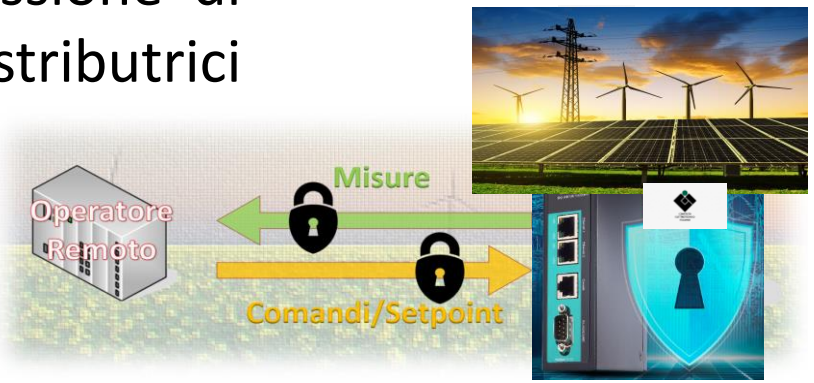
h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica

4. **Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia**

Normativa italiana



- CEI 0-16 «Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT e MT delle imprese distributrici di energia elettrica»
  - Allegato O – Controllore Centrale di Impianto
  - Allegato T – Modello dati e **cybersecurity**
    - Recepiscono lo standard IEC 61850 e IEC 62351



- CEI 0-21 «Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti BT delle imprese distributrici di energia elettrica»
  - PAS Allegato X – Controllore Infrastruttura di Ricarica Veicoli Elettrici

Riferimenti /1

1. NIS Directive EU 2016/1148 https://eur-lex.europa.eu/eli/dir/2016/1148/oj
2. CEN-CENELEC-ETSI Smart Energy Grid – Coordination Group, Cyber Security & Privacy, Dec 2016, https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/smart-grids-and-meters/smart-grids/
3. the Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector from Energy Expert Cyber Security Platform (2017) https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
4. the European Commission Recommendation C(2019)2400 on cybersecurity in the energy sector https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf
5. the Cybersecurity Act Regulation (EU 2019/881) https://eur-lex.europa.eu/eli/reg/2019/881/oj
6. Clean Energy for all Europeans Package, European Union 2019
7. ENISA CYBERSECURITY CERTIFICATION (2020) Cybersecurity Certification: EUCC Candidate Scheme — ENISA (europa.eu)
8. Evaluating the prudency of cybersecurity investments: Guidelines for Energy Regulators, National Association of Regulatory Utility Commissioners (NARUC), May 2020

Riferimenti /2

9. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, December 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0823&from=EN Cybersecurity Act Regulation (EU 2019/881) https://eur-lex.europa.eu/eli/reg/2019/881/oj
10. ENTSO-E / EU DSO, «Recommendations for the European Commission on a Network Code on Cybersecurity», Final Report,19 February 2021
11. ACER, Framework Guideline on sector-specific rules for cybersecurity aspects of crossborder electricity flows, July 2021, https://documents.acer.europa.eu/Official_documents/Acts_of_the_Agency/Framework_Guidelines/Framework%20Guidelines/Framework%20Guideline%20on%20Sector-Specific%20Rules%20for%20Cybersecurity%20Aspects%20of%20Cross-Border%20Electricity%20Flows_210722.pdf
12. NIST Cybersecurity Framework Version 1.1, Aprile 2018, https://www.nist.gov/cyberframework/framework
13. IEC Technology Report, “Cyber security and resilience guidelines for the smart energy operational environment”, 2019

Riferimenti /3

14. Norma CEI 0-16, “Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT e MT delle imprese distributrici di energia elettrica”, 2020
15. DossieRSE, «Cyber Security nella transizione energetica e digitale», Dicembre 2019, https://www.dossierse.it/