NETWORK CODE ON CYBERSECURITY – INFORMAL DRAFTING TEAM

Final Report

Recommendations for the European Commission on a Network Code on cybersecurity

19 February 2021

1 Table of Contents

2 Terms and Definitions

Accreditation
Certification bodies issue certificates and must get a license to conduct certification audits. Hence, certification bodies secure their licenses through accreditation.

Accredited Certification
Accredited certification is a written assurance provided by a third party that has been formally recognised by an accreditation body. The accredited certification assures a comparable trustworthy certification for all Grid Participants and thus a certified minimum-security baseline level. All accreditation standards include the principles of quality management systems, such as those found in the well-recognised standards.

Certification
The Certification is the procedure by which a third party gives written assurance that a product, process, system, or person has met the specified requirements.

Essential business process
Any business process performed by grid and market participants and supported by IT/OT systems and infrastructure which if successfully cyber attacked would cause serious cross-border problems to the safety, security, reliability, and proper functioning of the European electricity grid.

Grid and market participant
As defined by the NIS 2.0 ANNEX I - ESSENTIAL ENTITIES: SECTORS, SUBSECTORS AND TYPES OF ENTITIES. Sector. Subsector. Type of entity. 1. Energy. (a) Electricity.

- *Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944*
- *Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944*
- *Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944*
- *Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU) 2019/943*
- *Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944*
- Plus, any company or organization which performs services (such as generation, transmission, distribution, market related etc.) contributing to the overall safety, security, reliability, and proper functioning of the European electricity grid.

Note: the term “Significant Grid User” is also defined in some Network Codes. Significant Grid User (SGU) in the terminology used in the European Union Internal Electricity Market is the existing and new Power Generating Facility and Demand Facility deemed by the Transmission System Operator (TSO) as significant because of their impact on the transmission system in terms of the security of supply including provision of ancillary services. Significant Grid Users are assigned tasks important for the functioning of the EU Internal Electricity Market. According to Article 4(2)(c) of the Emergency and Restoration Network Code (Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration - NC ER) each TSO is required to submit to the relevant regulatory authority for approval the list of SGUs responsible for implementing on their

installations the measures that result from mandatory requirements set out in the connection network codes

CSIRT
Computer Security Incident Response Team.

ICS/SCADA
Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems.

Information Security Management System (ISMS)

An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive and confidential data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

Operation Security

Means the transmission system's capability to retain a normal state or to return to a normal state as soon as possible, and which is characterised by operational security limits (Regulation 2017/1485).

OT
Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. OT is common in Industrial Control Systems (ICS) such as a SCADA System and substation automation.

Security Control

A measure taken by a grid participant to mitigate a security risk (usually within an information security management system). Examples of control sets are ISO/IEC 27002, 27019 or IEC 62443-2-1.

Security Requirement

A function or quality that a product, service or process needs to have to implement a security control. The requirements are used to communicate to suppliers (manufacturers, service providers, internal departments) what the grid participant needs, to be able to implement the security controls they have selected. Examples of requirement sets are the BDEW whitepaper or IEC 62443 parts 2-4, 3-3, 4-1 and 4-2.

3 Introduction

The "Clean Energy for all Europeans" legislative package acknowledges the importance of cybersecurity for the electricity sector, and the need to duly assess cyber-risks and their possible impact on the security of supply. In particular, the new 'Electricity Regulation[1]' includes sector-specific rules for cyber security aspects of cross-border electricity flows among the areas on which the Commission may establish a Network Code. The European electricity grid is becoming more interconnected and interdependent due to a transition towards more renewable energy generation through decentralised energy generation and demand, for example, electric vehicle (EV) charging points and solar and wind farms. It therefore becomes more important to defend this critical infrastructure against cyber-attacks. To ensure that cybersecurity risks are mitigated through the European electricity grid, the European commission has asked the TSO and DSO community to provide recommendations on a network code on cybersecurity.

Network codes are a set of rules drafted by ENTSO-E and in the future EU-DSO, with guidance from the Agency for the Cooperation of Energy Regulators (ACER), to facilitate the harmonisation, integration and efficiency of the European electricity market which are then adopted by the European Commission. There are currently eight approved electricity Network Codes and guidelines[2]:

- Demand Connection https://www.entsoe.eu/network_codes/dcc/
- High Voltage Direct Current https://www.entsoe.eu/network_codes/hvdc/
- Requirements for Generators https://www.entsoe.eu/network_codes/rfg/
- Emergency and Restoration https://www.entsoe.eu/network_codes/er/
- System Operations Guidelines https://www.entsoe.eu/network_codes/sys-ops/
- Capacity Allocation and Congestion Management https://www.entsoe.eu/network_codes/cacm/
- Electricity Balancing https://www.entsoe.eu/network_codes/eb/
- Forward Capacity Allocation https://www.entsoe.eu/network_codes/fca/

This proposed Network Code on cybersecurity will break new ground, since it will be the first time that both the TSO and DSO communities are collaborating on the drafting, preparation and definition of a Network Code. Decentralised energy systems are connecting many new stakeholders and digitals systems to the European electricity grid resulting in an ever-increasing cyber-attack surface. Since most of these resources are connected to distribution grids, the role of the DSOs has now become more prominent from an overall system balancing perspective. The collaboration between TSOs and DSOs should follow the same approach developed by the Systems Operations Guidelines (SOGL) where a regional or European level of coordination is added to an otherwise National approach to operational security.

[1] Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity
[2] https://fsr.eui.eu/network-codes-versus-guidelines/

In the opinion of the informal drafting team, the purpose of the Network Code for cybersecurity should be to satisfy the following five specific objectives:

Objective 1: Essential business process cross-border cyber risk is addressed via effective risk identification and management.

Objective 2: All grid participants who come into scope because they perform essential business processes can demonstrate through certification that they have an Information Security Management System (ISMS) which guarantees they are performing cybersecurity processes to an acceptable minimum level.

Objective 3: Recommend and advise upon common security controls (implementation) and security requirements (for procurement) to be adopted by all grid participants thus applying the same level of protection to the same cross-border essential business process.

Objective 4: Make it easy for TSOs and DSOs to purchase products that meet the common security requirements in a cost-effective way through a product assurance scheme.

Objective 5: Sanitized technical incident and vulnerability information is shared with all grid participants in a timely manner.

To be acceptable by all grid participants, the proposed Network Code on cybersecurity should demonstrate qualities such as:

- **cost/benefit**: the benefits of implementing a Network Code must outweigh the costs.
- **pragmatic**: grid participants must be able to understand why these proposed Network Code measures are required (some of which will be mandatory) for the benefit of all grid participants.
- **trust & awareness**: grid participants must understand that cross border shared cybersecurity risk is the responsibility of everyone connected to the electricity grid.
- **risk-based**: a culture of risk management is adopted to implement appropriate controls to meet new threats.

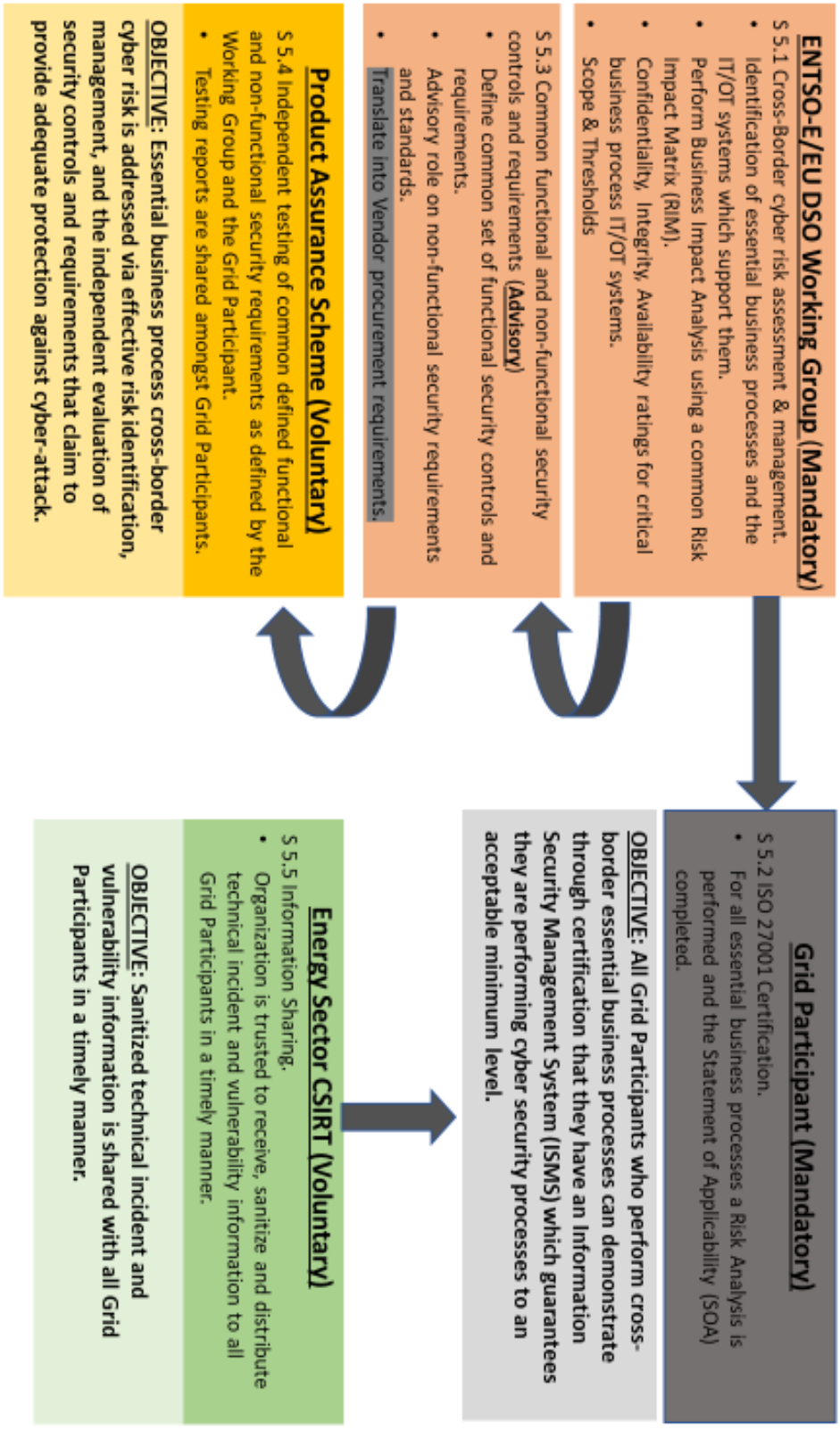

Figure 1 - High-level objectives for the Network Code for cybersecurity

4 Deliverables of the informal drafting team

A first interim report was delivered to DG ENER by the informal drafting team in June 2020. This report provided some initial ideas and suggestions for a Network Code on cybersecurity based primarily upon the work and recommendations of the Smart Grid Task Force – Expert Group 2 (SGTF-EG2) report.[3] This first interim report was distributed to ENTSO-E (representing the TSO community) and four associations representing the DSO communities (GEODE, EURELECTRIC, CEDEC, E.DSO) for their initial consultation. The purpose was to gauge if there was enough consensus opinion amongst these associations to support and develop these recommendations further. Whilst there was a lot of strong opinion both supporting and, in some cases, not supporting these first interim report recommendations, the overall consensus was that generally these recommendations were acceptable and that the majority opinion was favourable to move forward and further develop these ideas.

A second interim report was delivered to DG ENER by the informal drafting team in November 2020. This second interim report incorporated feedback received from the TSO and DSO associations reflecting many of the comments and suggestions made during the first initial consultation process with the five associations. From the TSO side, the main contentious issues identified with the first interim report were mainly related to ISO/IEC 27001 certification and the Product Assurance Scheme. Questions were raised concerning:

- should equivalent certifications be recognised since some TSOs have already invested in alternative certification schemes,
- will costs increase substantially if compliance to standards are demanded,
- and ISO/IEC 27001 only demonstrates that a control has been implemented, not its maturity.

From the DSO side the issues raised were quite similar. The feedback regarding ISO/IEC 27001 certification was mixed. DSOs also expressed some concerns as national regulators require them to implement more specific national schemes, not based on ISO/IEC 27001, in order to comply with the NIS directive, thus requiring ISO/IEC 27001 certification would require some DSOs to comply to two very different standards, which would imply significant effort and investment. The drafting team therefore sought to achieve a more consensual output in relation to the ISO/IEC 27001 certification topic, by considering other common standards if a set of specific criteria is validated.

This final report was delivered to DG ENER in February 2021 and represents the end of the initial informal drafting team process. Previously, alignment with the NIS 2.0 was not possible since the second interim report was delivered to DG ENER before the public release of NIS 2.0 on 15 December 2020. The final report has been modified to achieve alignment with NIS 2.0. Work on a Network Code for cybersecurity will now transition and be taken over by a formal process and drafting team led by ENTSO-E and EU DSO Entity under their respective legal mandates and articles of association. The network code process is defined in the Electricity Regulation (EU) 2019/943 in Chapter VII. The Electricity Regulation[4] calls for a Network Code on cybersecurity to increase the resilience of the

[3] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf
[4] REGULATION (EU) 2019/943

energy sector and protect energy systems. In this Regulation, Article 59 (2) empowers the Commission to adopt delegated acts supplementing this Regulation in accordance with Article 68 concerning the establishment of network codes in respective areas. For cybersecurity, Article 59 (2) (e) calls for sector-specific rules for cybersecurity aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management.

This final report incorporates feedback received from the much wider stakeholder consultation of the second interim report, particularly from the Smart Grid Task Force – Expert Group 2 (SGTF-EG2), NIS Cooperation Group Work Stream 8 (NIS-WS8), T&D Europe, European Smart Energy Solution Providers (ESMIG), Smart Energy Europe and Electricity Coordination Group (ECG) groups. Over 500[5] comments and suggestions were received and considered by the informal drafting team. Whilst the team did not agree with all comments made, the final report does incorporate many of them. The main areas of disagreement or concern were: Governance, particularly of the proposed cyber risk assessment working group and the decisions it will make; the Product Assurance Scheme - how it will fit under the EU Cybersecurity Act and why Common Criteria is thought not to be a suitable solution; the formation of a new energy sector CSIRT instead of using existing organisations like EE-ISAC to share information; and the scoping of ISO 27001 certification (or equivalent) and cost/benefit particularly for smaller energy organisations. There was, however, positive feedback and general agreement on the need to perform cross border cyber risk assessments properly and to define and advise upon common functional and non-functional security controls and requirements for the IT/OT systems and components that support essential business processes. The perception of the many comments received was that there was an expectation of more details and substance in the description of the recommendations proposed in this final draft. The informal drafting team, however, purposely decided to base the final report on high-level principles. It did not have expertise in some key areas such as existing National and EU legislation covering the European energy sector, and how these network code recommendations may conflict with them. This will be taken up and addressed by the formal drafting team.

The final report delivers five key recommendations for a cybersecurity network code, several options for each recommendation and in the opinion of the informal drafting team the preferred option with an explanation.

[5] A spreadsheet documenting all comments and suggestion received and the team response is available upon request at nccs.feedback@entsoe.eu.

5 Final report

Based upon the feedback received from the five associations on the first interim report, and from wider stakeholder consultation on the second interim report, the informal drafting team now proposes the following five strong recommendations for a Network Code on cybersecurity as the basis for further development and refinement under the formal drafting process in 2021.

5.1 Cross border cyber risk assessment and management

Grid Participants already perform local cyber risk assessments, but there is now a need to assess the "bigger picture" cyber risk viewpoint. TSOs and DSOs either belong to islands or to larger synchronised areas forming an interconnected grid. Grid participants who belong to synchronised areas may directly impact their neighbours and the whole synchronized area through a cyber-attack on key IT/OT systems. These cyber risks need to be properly analysed and addressed, to minimise any potential cascading effects to neighbours or all other grid participants in the same synchronised area or beyond (for example, managing cross border electricity flows, High Voltage Direct Current (HVDC) connections etc.).

In order to identify, assess, evaluate, analyze and manage the cross-border cybersecurity risks the first recommendation is that a formal ENTSO-E/EU DSO Entity working group should be formed with a mandate to perform cross-border cybersecurity risk assessments and risk management particularly focusing on events, those which could seriously impact cross border transmission and/or distribution with a focus on operational security and safety risk.

The mission statement of this working group should specifically be:

To identify cross border cyber security risk and determine an overall cyber risk posture, proposing qualitative and quantitative criteria to measure risk treatment.

1. It is tasked with the identification of "essential business processes and events"; those common business processes supported by IT/OT systems and infrastructure which if successfully cyber attacked causing event materialization would cause serious problems for the overall safety, security, reliability, and proper functioning of the European electricity grid. The list of cross border essential business processes identified must remain confidential amongst grid participants. It is the opinion of the informal drafting team that no other body can or should define "essential business processes and events" since the knowledge and expertise to correctly identify them lies primarily within the TSO and DSO communities.
2. It is tasked with maintaining and consistently applying a commonly agreed cross border cyber Risk Impact Matrix (RIM) with thresholds for the identification of unacceptable cross border cyber risk event materialisation. The content of this risk impact matrix (RIM) must not contradict any other current Network Code. Grid participants should continue to use local and nationally agreed RIMs for local risk assessment purposes. The thresholds set must be constantly reviewed and if necessary adjusted based upon current threat and risk assessments. A cyber incident taxonomy

like the ENTSO-E Incident Classification Scale would be helpful to quantify cyber incidents and events. A change management process will be required to make these necessary adjustments.

3. It should be represented by experts from TSOs, DSOs and other grid participants, and the assumptions and decisions made by the working group should be periodically and challenged by Member States, ENISA and ACER under a clear governance structure (to be defined by the formal process) so that they remain valid. The working group must ensure good representation of the electrical grid community with the right experience and expert knowledge to identify essential processes and events, and to advise on appropriate common functional and non-functional security controls and requirements (Section 5.3) for the essential business processes identified, in order to protect against current the threat actors..
4. It is tasked with quickly adjusting to new cyber threats and threat actors, using information shared by Member States, security and Intelligence organisations, and other knowledgeable providers of threat information (Section 5.5 – Information sharing). It should also analyse and evaluate all incidents and near misses and feed this back into the cross-border cyber risk assessment process.

Examples of risk impact when an incident will affect an "essential business process" if the "thresholds" are passed:

- Loss of generation (supply) causing an imbalance of greater than X GW.
- Loss of consumption (demand) causing an imbalance of greater than X GW.
- The unauthorised access, unauthorized modification, or unplanned availability of critical data to key systems, e.g. Energy Management Systems (EMS), Distribution Management Systems (DMS), Day ahead forecast schedules (Market), Common Grid Model (CGM).
- Unauthorized access to and simultaneous control over many the same IOT devices which might potentially impact the security of supply to X households.
- Exploits of a serious vulnerability in common equipment purchased and used by multiple grid participants.

Note: X thresholds are defined and stated in the Risk Impact Matrix (RIM) and are primarily derived based upon the guidance already provided by the Emergency and Restoration Network Code - ENTSO-E Incident Classification Scale.[6] e.g. for the European synchronized area the maximum imbalance that the grid is designed to withstand is 3 GW. Any imbalance exceeding this threshold could cause serious grid instability and blackout scenarios. Accepted thresholds must be periodically reviewed and re-evaluated based upon the cross-border cyber risk assessment.

It is important to note that this working group has no mandate and is not intended to replace local internal company risk management activities. Local cyber risk identification and management shall remain the responsibility of each individual grid participant.

[6] https://eepublicdownloads.entsoe.eu/clean-documents/SOC%20documents/Incident_Classification_Scale/180411_Incident_Classification_Scale.pdf

5.2 ISO/IEC 27001 Certification or proof of equivalence

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. Grid participants that pose a potential risk to others in their synchronized area and beyond must comply with a common standard for managing the cross border cyber risk for electricity flows. The ISO/IEC 27001 provides such a common standard for an Information Security Management System for aligned risk management. Where a standard is to be referenced it should be European or an International standard. . Furthermore, the SGTF-EG2 report draws the same conclusion, including conformance to ISO/IEC 27001, and this has now also been generally accepted by the associations of the TSOs and DSOs, although it must be recognised that some organisations do not agree (as recognized in Section 4). However, it is recognised that other common standards are a valid alternative approach if they provide a validated mapping with ISO/IEC 27001 ISMS requirements and security controls which can be independently verified and audited in a harmonized way.

To make sure that any implementation is harmonised across the EU, the standard must be independently verified in a harmonised way. Certification of ISO/IEC 27001 will ensure this independent verification. From a cyber risk perspective, every grid participant in the European energy system could pose a risk. Besides grid stability, mutual trust is also a key factor so all participants should be obliged to meet the same minimum level of cybersecurity. A common certifiable standard will give us such a common security baseline that everyone can rely upon.

The key factor for the ISO/IEC 27001 certification process is the definition of the Statement of Applicability (SoA) and a scoping statement. The definition of the scope directly affects the amount of effort and resources required to achieve certification in relation to covered assets, risk management, business processes and maturity of the certification itself. It is therefore mandatory to have a common definition of scope for all grid participants to assure a comparable minimum baseline of certification quality across all TSOs, DSOs and other grid participants.

According to ISO/IEC 27003, which provides guidance for ISO/IEC 27001, the scope of an ISMS can include:

- one or more specific processes
- one or more specific functions
- one or more specific services
- one or more specific sections or locations
- an entire legal entity
- an entire administrative entity and one or more of its suppliers

The recommendation is that the scope of certification should cover at least all essential business processes that a grid participant performs. Grid participants may of course choose a larger scope. It is the responsibility of the grid participant to identify and clearly delineate their essential business processes.

As specified in the Statement of Applicability for ISO/IEC 27001, the above scope must have: "no exclusions OR list and justification of the controls excluded". This statement on exclusions is to demonstrate that the ISMS has all 114 controls from ISO/IEC 27001 and the 14 from ISO/IEC 27019 applied or has otherwise excluded certain controls (and documented them) as not relevant. ISO/IEC 27001 certification does not include maturity levels, but the certification itself needs a high maturity. The management system itself undergoes a continuous improvement process and therefore constantly gains maturity. For the purposes of the ISMS, the definition of critical infrastructure is based on the EU wording from Council Directive 2008/114/EC.[7]

In line with the recommendations of the Smart Grid Task Force Expert Group 2 report, the scope above is compatible with the minimum required Baseline Protection for Energy System Operators, as it establishes an Information Security Management System (ISO/IEC 27001) with consideration of ISO/IEC 27002, ISO/IEC 27019 and the minimum security requirements protecting the EU Energy System (utilising the EU Cybersecurity Act).

Whilst it is true that ISO/IEC 27001 does not explicitly address maturity or quality of controls very well (it only ensures that the ISMS has been correctly implemented and is periodically reviewed), a common level of maturity can nevertheless be assured by issuing a common setting specific requirements in the accreditation scheme for auditors and certification bodies. "Accreditation" means that the certification practices have been checked to ensure that the certificates issued are legitimate, trustworthy, and meaningful thus ensuring a common baseline all over Europe. The proposed certification scheme for in-scope grid participants would include not only processes but also a minimum scope, identified by the ENTSO-E/EU DSO entity working group (as defined by Section 5.1).

If we accept the need for a common, certifiable, and mandatory standard for ISMS, the ISO/IEC 27001 is currently the best option. The recommendations on ISMS scoping principles are therefore:

1. Any grid participant who performs one or more "essential business processes" identified by the cyber risk assessment and management process (Section 5.1) and who meets the thresholds identified, must be certified to ISO/IEC 27001 or to a comparable mappable and certifiable standard. The certificate must cover all cross border "essential business processes" performed by the grid participant (the minimum scope). There is nothing to stop a grid participant from going above and beyond this minimum scoping level.

2. If the grid participant does not perform one or more "essential business processes" or does not meet the thresholds identified, then certification is not required. For example, in Northern Europe there are many small grid operators, many of which will probably not meet the thresholds set for essential business processes and will therefore not be in scope for certification to ISO/IEC 27001. However, even small DSOs should be encouraged to have and maintain an Information Security Management System and take their cyber responsibilities seriously even if they don't come into

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG

scope. It should be recognised that a coordinated cyber-attack against a number of smaller DSOs could result in thresholds being reached.

3. All core ISMS processes need to be in scope and fully implemented. The application of controls, as stated in Annex A of the ISO/IEC 27001 standard are applicable if they are implemented and necessary for the secure operation of the critical processes. The recommendation for implementation of ISO/IEC 27001 certification should be based in conjunction with the controls and implementation guidance of ISO/IEC 27019, the energy sector-specific standard in the ISO/IEC 27K series which contains both additional implementation guidance to ISO/IEC 27002 as well as additional energy sector specific controls (especially for legacy systems) which are not contained in ISO/IEC 27001 Annex A.

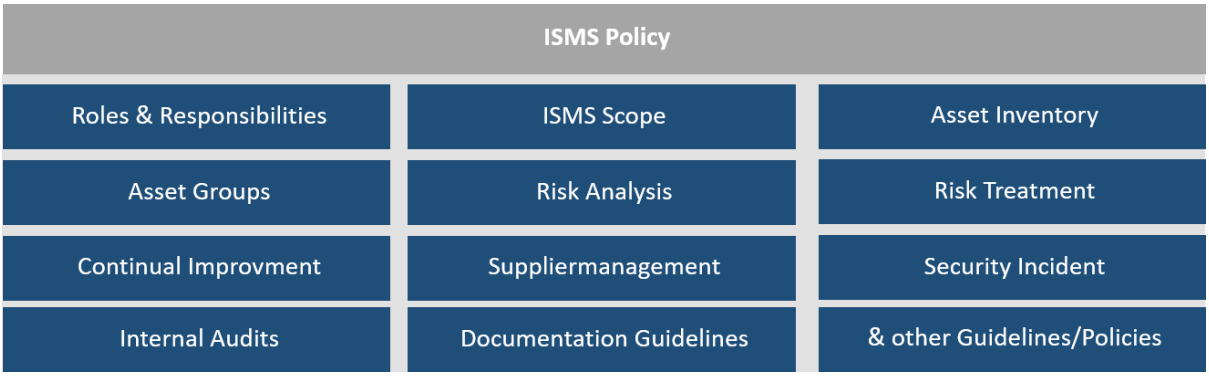

Figure 2 - ISMS Policy

ISMS costs will vary between each grid participant. Under the commonality approach, security is not a competitive disadvantage, as similar and proportional expenditure would be required from all grid operators. Cost estimates should include the FTEs for the ISMS team, compliance team, risk treatments and process improvements outside of the core security department activities, and so the overall cost to the organisation are likely to be significantly higher when new or improved controls are determined to be required through risk assessment or existing processes are seen as not adequate for the scope covered.

5.3 Common functional and non-functional security controls and requirements.

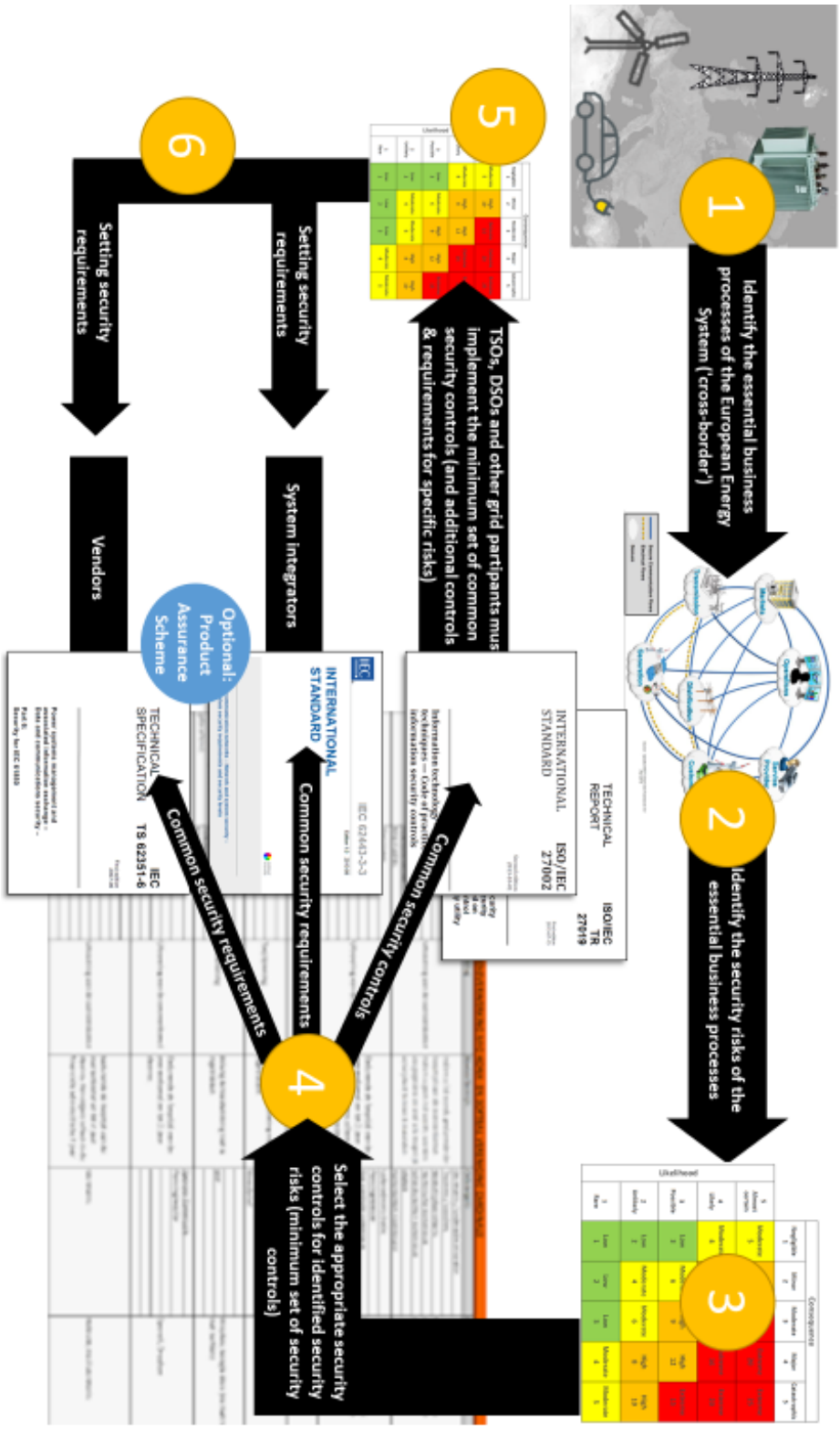

Figure 3 - Process to define a common set of security controls

The cross-border cyber risk assessment process (Section 5.1) identifies cross-border essential business processes operated by grid participants, and the underlying IT/OT systems, which support them. The recommendation of the informal drafting team is that the ENTSO-E/EU DSO entity working group identified in Section 5.1 should also identify and propose a common set of security functional and non-functional controls and requirements for all grid participants who operate these essential business processes. In addition to the mission statement described in Section 5.1, this working group would also be specifically responsible for:

1. Performing a Business Impact Analysis (BIA) on every essential business process identified by the cross-border cyber risk assessment, using the agreed Risk Impact Matrix (RIM). For each essential business process identified with its Business Impact Analysis ratings, the working group will select a set of minimum set of common security controls to mitigate the assessed cybersecurity risk to that essential business process. The purpose or objective is to derive a common set of security requirements for system integrators and vendors to deliver systems and products that conform to and implement the minimum set of security controls for the same essential business process identified. Whilst overall advisory, this working group should reserve the right through governance procedures to state that some common security controls and requirements for some cross-border essential business processes are mandatory.
2. 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.

Grid participants that operate essential business processes must perform a cyber risk assessment and select controls to mitigate the risks according to their (certified) Information Security Management System (ISMS). They must consider the commonly identified security controls when mitigating the risk and provide justification if they chose not to select a common control.

Grid participants define their own security requirements to system integrators and vendors when procuring new systems or products. They must however consider the common security requirements identified per essential business process as a baseline. The product assurance scheme (Section 5.4) will help them to easily find products that already meet the common security requirements.

The information technology (IT) and operational technology (OT) systems and components installed in the electricity sector, are in many cases legacy systems and technologies, which don't have adequate state-of-the-art security features. These legacy systems are used in combination with energy utility components (e.g. transformers) which have a lifetime up to decades, unlike more regular office IT components which typically have a life of just a few years. For that reason, it is important to assess and manage the weaknesses and risks resulting from the use of legacy systems and technologies. If unacceptable risks are identified and standard security controls cannot be implemented, alternative compensating security controls must be considered under the adopted risk assessment methodology.

The reference baseline set of controls should be ISO/IEC27019. Common security controls should be implemented unless there is a good reason for excluding a control. In that case, the justification must

be recorded, and it may be necessary for alternative measures to mitigate the security risks. Grid operators may choose to replace a common security control with an equivalent control from another standard, providing evidence is provided (mapping to ISO/IEC 27019 baseline control).

The drafting team is of the opinion that the definition of common security controls and requirements cannot easily be performed by any other body since the knowledge and experience of the common essential business processes primarily lies within the TSO and DSO communities. However, it should be recognised that crucial to success would be the early involvement and cooperation of equipment vendors. The governance of this working group must be clearly defined under the formal Network Code process. The working group established under Section 5.1 would therefore specifically be tasked with:

1. The definition of functional security requirements for every cross-border essential business process for the European energy system in terms of Confidentiality, Integrity and Availability, Common security requirements will be related to a common data classification scheme (defined as part of the risk impact matrix). The higher the data classification, the more rigorous and detailed the set of appropriate security controls. Security requirements should be determined without respect to any cost/benefit analysis but based purely on cyber risk.

2. The definition of non-functional security requirements for every cross-border essential business process identified in terms of, for example, quality, level of security provided, and compliance to standards. All grid participants may apply their own National standards for security controls, many of which may be tactical and strategic in nature. However, from a pan-European perspective these should be based upon European or international standards.

3. Maintaining a watching brief over all standards, controls frameworks, maturity frameworks etc. with a view to the adoption of the most suitable and applicable International standards and controls. In other words, benefit from the work of others, with special attention for legacy components and systems.

4. Identify gaps in standards and feed this back to the relevant standards organisations for suggested improvement.

Functional security requirements for essential business processes should be defined by the working group. Non-functional security requirements are additional and should be defined by the grid participant. The translation of security controls into actual security requirements for procurement purposes is the responsibility of the grid participant, however the baseline for security controls must be ISO/IEC 27019. All 128 controls as defined by ISO/IEC 27019 must be considered as applicable, and where not applicable these must be documented. Controls from other standards can be considered so long as they are mapped to the relevant ISO/IEC 27019 control. ISO certification is about processes of the Information Security Management System, and directly about the essential business processes of the 'grid participant'. The minimum set of controls is about mitigating the cross-border cyber risks and following the right processes of plan-do-check-act-cycle, like ISO/IEC 27001. The Smart Grid Architecture Model (SGAM) Framework, where data classification with Confidentiality, Integrity and

Availability is combined with the perspective of (grid) functions, systems, and communication assets, could be used particularly for OT systems.

5.4 Product Assurance Scheme

With the definition of a set of security requirements for cross-border essential business processes identified under Section 5.3, it is then necessary that an agile and cost-effective product assurance scheme is developed so that supplier claims of meeting these security requirements can be independently verified.

Product assurance means independent verification that the product meets the security requirements and that the required security measures are implemented effectively. Product assurance may be achieved through product certification, but other methods may also be considered if they better meet TSO's and DSO's requirements.

The recommendation of the informal drafting team is to develop a new product assurance scheme that meets the requirements in **Error! Reference source not found.**. Using products certified under t he scheme should be voluntary. The scheme should be compatible with the European Cybersecurity Framework as defined in the EU Cybersecurity Act. When a scheme is available under this framework that meets the requirements of TSOs and DSOs, this scheme should be used. When no such scheme is available, a new scheme may be developed that meets the requirements in Articles 51, 52, and 54 of the Cybersecurity Act, so that ENISA could select it as a candidate certification scheme.

The scope of the assurance scheme should be ICT products as defined in the EU Cybersecurity Act, that is, elements or groups of elements of a network or information system. The focus of the scheme is expected to initially be OT components. But it may also cover software applications or larger systems.

5.4.1 Requirements for an assurance scheme

The assurance scheme should allow grid participants to cost-effectively implement the common security controls by giving them ready access to components and systems that can be used to implement them. To meet this goal, the product assurance scheme should meet the following requirements.

Area of the scheme	**Requirements to scheme**
Requirements to evaluate against	• **Requirements defined top-down by risk owners:** The requirements against which the scheme evaluates are derived by primarily TSOs and DSOs as risk owners from the common functional security controls defined for the whole system. • **Requirements cover secure development:** The scheme ensures that suppliers apply security throughout their development lifecycle.

Evaluation methods	• **Thorough, independent evaluation:** The scheme ensures that components are thoroughly evaluated by a lab independent from the supplier.
Governance	• **Enabling innovation:** The scheme does not hold back innovation, e.g. through high cost or long delays. • **Mandatory vulnerability handling:** The scheme requires that suppliers fix any vulnerabilities found.

Table 1 - Requirements to the product assurance scheme

The Joint Research Center has published Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS) (EU Joint Research Center, 2020). These include requirements to a certification scheme for industrial components to be set up under the EU Cybersecurity Act.

The ICCS requirements provide a way to fulfil some of the requirements in **Error! Reference source n ot found.**. The ICCS requirements on evaluation activities and certification processes (such as peer reviews) ensure thorough and independent evaluation. Secure development is covered by the ICCS development process audit activity. The ICCS does not yet have a process to handle vulnerabilities or to deal with updates, which is a prerequisite for dealing with innovation.

The ICCS partly contradicts the requirement in **Error! Reference source not found.** that requirements a re defined by risk owners. Instead, security objectives are defined by the ICCS governance group, consisting of representatives of the national cybersecurity certification authorities, in what are called generic Component Context Analyses (gCCA). Detailed requirements are worked out in a Component Cybersecurity Profile (CPP) provided by the applicant for a certificate. As risk owners, TSOs and DSOs can of course define their own gCCAs and CPPs. But these would not have a formal place in the scheme.

The ICCS intends to use existing standards, in particular Common Criteria, IEC 62443, and the evaluation methodology that is being developed by CEN-CENELEC JTC 13 WG3. So, it does not create new schemes that need to be considered in the analysis in Sections 5.4.2 to 5.4.5.

The informal drafting team recommends that it is investigated during the formal phase if the ICCS can be adapted to meet the needs of TSOs and DSOs. The ICCS is still under development. TSOs and DSOs would be an important user group of the scheme. Yet no TSO or DSO representatives were part of the ERNCIP IACS Thematic Group that developed the ICCS requirements.

The need for these requirements is explained below.

Requirements defined by top-down by risk owners: The requirements against which products and systems are evaluated are defined by TSOs and DSOs. The requirements could be defined by an ENTSO-E/EU DSO entity working group, working closely with the working groups that perform the cross-border risk assessment and/or defines the common functional security controls. In this way, the requirements can be aligned with the risks that this group identifies and the controls it selects to

mitigate these risks (considering the interconnected cyber risk appetite that has been defined by ENTSO-E/EU DSO entity working group).

Suppliers of products should be consulted when defining the requirements. They bring their expertise to select good technologies, and they can check that the requirements are feasible for current or upcoming products. The ENTSO-E/EU DSO entity working group should also consult relevant government agencies at EU and national level, such as ENISA, ACER, national cybersecurity certification authorities, national regulatory agencies, and national competent authorities. The consultation process will be formalized when the ENTSO-E/EU DSO entity working group is set up.

The requirements should be derived top-down starting with the security measures for the whole system and working down to the individual components. A reference architecture can be used to define the different components within the system and analyse what requirements should be put on each component. Component certification schemes, such as Common Criteria, usually work bottom-up. They first define the threats a component should resist to and the measures needed for that purpose. Then they define the requirements to the system to operate the component securely. Such an approach does not work well for operational technology environments used in the electricity grid where individual components are often not secure, and security is expected to come from the architecture of the systems.

Requirements cover secure development: Besides ensuring that the tested product meets the defined technical security requirements, the scheme should also ensure that suppliers of products and systems apply security throughout their development lifecycle. One of the major problems in the electricity sector is that there are still suppliers with a low security maturity. A scheme that rewards suppliers for increasing their maturity would greatly improve the security of the sector. The requirements should cover the full development cycle. Suppliers should be required to make a good security design by performing threat assessments and clearly defining security requirements. They should be required to implement secure programming practices and protect the source code. And they should be required to perform thorough security testing on each release.

Thorough, independent evaluation: The scheme should ensure that the system or component is thoroughly evaluated by a test laboratory that is independent of the supplier. When DSOs and TSOs order the evaluation, they can ensure the independence and thoroughness by selecting a good test lab and setting the scope of the test. But if products are certified, the supplier usually selects and pays for the test lab. There is a risk that they shop around for the testing laboratory with the lowest price and the highest chance of passing the evaluation. Different approaches have been developed to mitigate this risk. The Common Criteria scheme puts detailed requirements on the evaluation activities that a lab performs and requires the results of these activities to be extensively documented. This approach has a high cost. The French CSPN certification meets it by using government-selected labs and specifying a minimum amount of days of hands-on testing. The right approach for the network code assurance scheme will need to be developed. Some accreditation scheme for test labs will probably be needed. For functional security requirements, test cases can be defined to ensure repeatable testing. For non-functional requirements, a time-boxed penetration tests or code reviews could be used if the testers have a clear incentive to find vulnerabilities. The resources spent on the

evaluation should be spent on activities that provide strong assurance, such as technical design reviews, code reviews, and hands-on tests. Testers should spend their time looking for vulnerabilities. Bureaucratic overhead should be minimized.

Enabling innovation: The assurance scheme should not hold back innovation. The smart grid requires new functions to be rolled out to components and systems at an increased pace. To deal with renewable energy and electric vehicles, grid operators will need increasingly advanced automation. TSOs and DSOs are therefore trying to speed up the development and roll-out of new systems, e.g. by using agile processes, cloud platforms, and open-source. The product assurance scheme should not unnecessarily limit such developments. Certification could prove a limiting factor in different ways. It could add significant cost to new systems, so that the business case of some innovations becomes negative. It could cause delays in rolling out new components if they take months or years to certify. It could force smaller, innovative suppliers out of the market, because they cannot implement the complex functions and processes required. The scheme should be designed to anticipate these problems.

Mandatory vulnerability handling: The scheme should ensure that any vulnerability found is fixed in time. Many DSOs and TSOs still find that it takes considerable effort, time, and cost to get some vulnerabilities fixed. The scheme should require suppliers to provide a security update that fixes a vulnerability within a given time, depending on its severity. If the vendor does not comply, it loses its certificate. This requirement meets the objective in Article 54 that the scheme includes rules concerning how previously undetected cybersecurity vulnerabilities are to be reported and dealt with. Applying the security updates to their systems remains the responsibility of the TSO or DSO and is covered by the Common Security Control and Requirements pillar.

This mechanism should apply both to vulnerabilities in the code developed by the supplier itself and to dependencies, such as libraries and third-party applications. Many security functions on smart grid products are implemented through such dependencies. For instance, open-source libraries are often used to secure communication through TLS or IPsec. The assurance scheme should ensure that suppliers update the dependencies when a vulnerability is found. Some certification schemes encourage suppliers to stay with the vulnerable version, as they would otherwise need to recertify.

5.4.2 Current schemes

Current assurance schemes do not meet the above requirements. Table 2 below shows that none of the existing international schemes meet all the requirements. Some national schemes, such as the French CSPN and the UK CPA scheme come closer, but they would have to be extended to a European scheme. The evaluation method that is being developed by CEN-CENELEC JTC13 WG3 is not yet considered here but should be considered by the ENTSO-E/EU DSO entity working group as it becomes more worked out.

Requirement to scheme	Common Criteria	IECEE for IEC 62443	IEC 62351 conformance
Requirements defined top-down by risk owners			
Requirements cover secure development			
Thorough, independent evaluation			
Enabling innovation			
Mandatory vulnerability handling			

Table 2 - Overview of how existing certification schemes meet the requirements to the product assurance scheme. Green means that the scheme meets the requirement. Yellow means that the scheme can meet the requirement with some minor extensions. Orange means the scheme does not cover the requirement, and major extensions are needed. Red means the scheme contains elements that make it difficult to meet the requirement.

5.4.3 Common Criteria

Common Criteria is a security certification standard developed by North-American and European governments in the mid-1990's. A version of the scheme is available as an international standard ISO/IEC 15408:2009. Common Criteria is meant to be applicable to any product. The standard provides catalogues of functional requirements, and assurance requirements that specify how a product should be evaluated. From these catalogues, requirements can be selected for a specific product type, based on a threat assessment. This results in what is called a protection profile for the product type. ENISA has prepared a candidate certification scheme based on Common Criteria under the cybersecurity certification framework from the EU Cybersecurity Act. Common Criteria has been applied in the electricity sector in two protection profiles for smart metering. The German national security authority, BSI, has developed a mandatory protection profile for smart metering gateways in the home. ESMIG has developed a protection profile for smart meters.

Requirements defined top-down by risk owners: TSOs and DSOs can define the requirements against which to certify by developing protection profiles. The ENTSO-E/EU DSO entity working group could for instance develop protection profiles for different grid components, such as RTUs, IEDs, and SCADA systems. There is not a standard method to develop such profiles in a top-down manner. Common Criteria is more oriented to a bottom-up approach. The implicit assumption often seems to be that users first select a component certified against a certain protection profile. They then determine which measures they should take at system level to securely use the component, based on the objectives from the operational environment in the protection profile. But there is nothing to stop TSOs and DSOs to work the other way around and develop a method to derive protection profiles from the controls at process and system levels. More challenging will be to get all manufacturers in the industry to understand the requirements in the protection profiles. The requirement catalogues are written in an abstract language that will require specialists at the manufacturers to interpret. Training and consulting are available. But many small manufacturers may not be able to comply with the profiles, at least not at short notice.

Requirements cover secure development: Common Criteria contains requirements on secure development in its security assurance components, mainly in the development, life-cycle support, and tests classes. At security levels EAL1 to EAL3, developers with a sound development process can be expected to implement the requirement. Bus as the requirements are written quite formally, suppliers without experience with Common Criteria will need to spend time to understand them. At higher assurance levels, even suppliers with mature processes will need to do considerable work may be required to meet the secure development requirements.

Thorough, independent evaluation: Common Criteria provides a workable way to ensure independence of test labs through accreditation but getting thorough testing at reasonable costs will require TSOs and DSOs to carefully select the evaluation activities.

Common Criteria should allow suppliers to get their components certified at any accredited lab. For this purpose, there are international agreements such as the Common Criteria Recognition Arrangement (CCRA), and the European SOG-IS (which is planned to be replaced with the ENISA EUCC scheme). Accreditation should provide enough assurance on the independence of the labs.

Few accredited labs however have experience in the electricity sector. They will initially not fully understand the cyber risks that a component may face. So, they may be less effective in the vulnerability assessment activities, including penetration testing. TSOs and DSOs will need to carefully tune the assurance requirements to get the right level of thoroughness in testing. Common Criteria allows users to choose how strict the evaluation should be by selecting an evaluation assurance level (EAL), a standard package of assurance components. But these EALs likely will not meet the needs of DSOs and TSOs. The lower assurance levels up to EAL 3 are designed to be achievable without major reengineering of existing products. But most of the evaluation consists of paper reviews. Penetration testing is limited to attackers with basic potential. So, these levels seem insufficient for critical processes. (EAL 3 also does therefore not meet the requirements of the ‘high’ assurance level in the EU Cybersecurity Act, as it requires penetration testing simulating skilled attackers.) The assurance levels higher than EAL 3 usually requires products to be reengineered and development process to be adjusted. This would result in high development costs. TSOs and DSOs will hence likely need to extend EALs with their own assurance components to get the evaluation activities they need.

Enabling innovation: Common Criteria does not seem well-suited to enable innovation due to high certification costs, and difficulties in dealing with changes in products. The initial cost of certification is expected to be high for many suppliers. Only a small part of the cost will be the fees of the evaluation lab and certification body. More costs can be expected in preparing the product and documentation for certification. Most suppliers do not have experience with Common Criteria and will need to train their personnel or hire new employees or external consultants. At higher assurance levels, the product may require a substantial redesign. Then there is the cost and effort in keeping the product certified when there are updates with new features. Common Criteria has been struggling with changes in products. Only the product version that has been evaluated by a lab is certified. Any change in the product renders it ‘unevaluated’. Initially, this meant that the new version would have to go through the entire certification process. Extensions to the standard now allow that only a subset of the evaluation activities is performed in case of minor changes. It is not clear if this update process would

work well with the typical release cycles of products in the electricity sector, e.g. if most product updates would be considered minor and if the costs for the subset evaluation of minor changes is reasonable. The process seems to be used sparingly in other sectors than electricity, with maintenance reports for updates being available for only a small part of the certified products.

Mandatory vulnerability handling: Vulnerability handling and patching is not addressed well in the Common Criteria standards themselves but could be addressed using the EUCC certification scheme. A fix of a vulnerability is treated as a change to the product. So, when a supplier fixes a vulnerability, they lose their certificate. The assurance requirements include requirements that a supplier has a flaw remediation process. But these requirements are not included in any of the standard evaluation assurance levels (EALs) the standard defines. The flaw remediation process is only checked when the product is evaluated. If it turns out later that the process is not followed, this has no effect on the certificate. The EUCC scheme tries to fix these issues, following recommendations from earlier studies. It defines patch management processes at three levels, depending on how many changes are needed to the product. A critical update process is defined for exploitable vulnerabilities in critical infrastructures. Suppliers are required to provide security updates for vulnerabilities. A certificate can be suspended and eventually withdrawn if the supplier fails to inform the certification body of a vulnerability or does not provide a vulnerability analysis in time. These additions to Common Criteria would provide much better vulnerability handling. But they have not been applied yet, and it remains to be seen how they perform in practice.

5.4.4 IECEE for IEC 62443

IEC 62443 is a set of standards for industrial cyber-security. As an IEC standard, it can be certified through the IEC System of Conformity Assessment Schemes for electrotechnical Equipment and Components (IECEE). Manufacturers have been developing a scheme for products, solutions, and processes. Overall, the certification scheme is less mature than Common Criteria. It builds on processes developed for electrical specifications. The security-specific part is only seven pages. Details are missing on the evaluation methods and vulnerability handling.

Requirements defined top-down by risk owners: To define the requirements against which can be certified, TSOs and DSOs would have to extend the standard with profiles for specific products. According to the standard, the manufacturer that applies for a certificate chooses which requirements from the IEC 62443 standard are assessed. The value of a certificate is then not clear unless its scope is carefully reviewed. To avoid this problem, TSOs and DSOs would have to define which requirements should at least be included. Different requirements will likely be needed for different product categories. Some requirements will need to be further specified, as they are not specified precisely enough in IEC 62443. The TSO and DSO working group defining the profiles may build on work on IEC 62443 profiles from IEC TC 65 WG10.

Requirements cover secure development: The focus of the certification is the capabilities of a system integrator (using IEC 62443-2-4) or manufacturer (using IEC 62443-4-1) to deliver secure solutions or products. The certification can also be used to evaluate if these capabilities have been applied to a specific product (using IEC 62344-4-2) or system (using IEC 62443-3-3). The focus on capabilities has

the benefit that it will help to improve the security maturity of manufacturers. There are now major differences between manufacturers, but mature manufacturers are now delivering products with good security.

Thorough, independent evaluation: The IECEE scheme tries to ensure the quality of the evaluation through accrediting lab and establishing an expert task force. But these measures seem too weak to ensure thorough, independent evaluation. There are hundreds of IECEE approved testing labs. Most will have electrotechnical expertise but will now also be allowed to issue cybersecurity certificates. So, it is difficult to ensure that suppliers only approach labs with enough cybersecurity expertise. The expert task force established for IEC 62443 testing should mitigate this risk. But it is not clear how this task force works or what it can do if labs do not meet its standard. The scheme includes on requirements on the evaluation activities to be performed. How the requirements are tested or audited is left to the evaluating testing laboratory. So, there can be large differences in how thorough the requirements are tested. Some labs may only do a paper review of documentation provided by the supplier, while others perform extensive penetration testing. For the scheme to work, TSOs and DSOs will need to take extend the scheme to ensure that only qualified labs can issue certificates, and that they perform a minimum set of testing activities.

Enabling innovation: The cost of IEC 62443 certification is expected to be lower than for Common Criteria. The certification process is less formal, leading to lower cost at the evaluation lab and certification body. The IEC 62443 requirements are also easier to understand and implement for most industrial vendors. But the scheme does not have a clear process defined for when and how updates to the product need to be recertified.

Mandatory vulnerability handling: It is not clearly defined how vulnerability handling is handled by the standard. Suppliers are required to have processes to handle vulnerabilities according to the IEC 62443-2-4 or IEC 62443-4-1 standards. These processes are evaluated for the certification (if put in scope). But suppliers can define their own process. They can for instance determine the thresholds for when they report vulnerabilities to their customers, and when they fix a vulnerability. So, certification on its own provide little assurance that vulnerabilities are handled well. TSOs and DSOs will probably need to set additional requirements to the vulnerability handling processes.

5.4.5 IEC 62351 conformity assessment

IEC 62351 is a series of technical standards for the data and communication security of electrical systems. It defines security measures for the communication protocols most used by grid operators (IEC 60870-5-104, IEC 61850, and IEC 60870-6 (ICCP)). IEC 62351 is working at a much more detailed specification level than Common Criteria and IEC 62443. It describes exactly which technical measures need to be implemented. So, it is not technology independent, and less widely applicable than the other standards. The benefit is that the standard would allow interoperability between products from different manufacturers. This is especially important for communication security, access control, and key management, where components from multiple manufacturers need to work together.

No certification scheme is yet available for IEC 62351. But as an IEC standard, conformity to IEC 62351 could be certified under the IECEE system. Also, some parties that do protocol testing for IEC 60870-5-104 and IEC 61850 are offering conformance testing.

Requirements defined top-down by risk owners: The requirements in IEC 62351 are defined in IEC standardization groups in which also many TSOs and DSOs participate. But it is not easy to align the requirements with a risk assessment. While Common Criteria and IEC 62443 provide lists of measures that can be selected, IEC 62351 is a more descriptive specification. It is not easy to select only parts of it. It would be possible to require only certain parts of the standard.

Requirements cover secure development: Secure development processes are not covered by IEC 62351.

Thorough, independent evaluation: The situation is similar as for IEC 62443 certification. There is no mechanism in place to ensure that only qualified labs perform the evaluation. An expert task force, as set up for IEC 62443, is also not in place. No evaluation activities are described to test for conformance.

Enabling certification: The situation is like that for IEC 62443. The cost of certification is expected to be lower than for Common Criteria. The overhead for evaluation is lower, and suppliers in the electricity sector are already familiar with the requirements. Many have implemented at least parts of them. But it is not clear how recertification would work for product updates. That IEC 62351 provides detailed specification, probably has a mixed effect on innovation. On the one hand, the specifications allow better interoperability between products from different suppliers. This will make it easier to deploy for instance key management and centralized access control. But if new security measures are needed, the IEC 62351 series itself will often need to be updated. It leaves little room for supplier-specific solutions that would be allowed under Common Criteria or IEC 62443.

Mandatory vulnerability handling: The IEC 62351 standard has no requirements on handling vulnerabilities. Need for a new scheme

5.4.6 Conclusions

As none of the existing international assurance schemes meet the requirements, therefore a new scheme should be developed. It is a recommendation that the network code ask ENTSO-E and the EU DSO entity to develop a new product assurance scheme meeting the requirements in a certain time. Given the complexity of such schemes it would be recommended to allow at least three years for the development. The costs and benefits of the scheme should be further analysed during the formal phase of the network code process. However, collective commissioning and funding of testing will ultimately save time and money.

Where possible the scheme should be aligned with the work being done by ENISA under the EU Cybersecurity Act, in particular to the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS) that is under development. The scheme could, for instance, be a lightweight sector-specific version of the EUCC scheme that is being developed under this act or a variant of the IECEE certification scheme for IEC 62443.When developing the scheme, ENTSO-E and the EU-DSO entity should seek active involvement of all stakeholders, including ENISA, national

cybersecurity certification authorities, national regulatory agencies, national competent authorities, suppliers, certification bodies, and test labs, possibly through association or groups representing them.

It is recommended that using the scheme is voluntary. TSOs, DSOs and other grid participants should make their own decisions on the purchase and use of commercially available systems, components or services that have been certified under the Product Assurance Scheme. If the scheme is successful, it will make certified components available to TSOs and DSOs at a reasonable price. Using these components, they can then more easily meet the common functional security control. So, there will be a clear business case to use certified components, and no regulatory compulsion is needed.

5.5 Information Sharing

To protect critical infrastructure in an increasingly interconnected world, decisions and actions should be based on recent data. Even small delays can make a difference when it comes to either preventing an incident or responding to an event. Therefore, the appropriate conditions for grid participants and relevant partners – be it in the public or the private sector - to be able to share technical information in a timely way are vital for the stability of the European electricity grid. Besides compulsory regulation, an appropriate environment must also be provided to allow establishing an EU-wide business culture of situational awareness and preparation that are essential for all critical infrastructure, and for operators of “essential business processes” of the electricity grid. Such information enables participants to understand the current cybersecurity threat situation: e.g. what happened in recent incidents, what mitigation measures were implemented, or what are the current, potential, or future threat vectors.

Technical Information in this specific context refers to any information usable for better protection against and analysis or understanding of external or internal cybersecurity threats. It includes at least:

- Vulnerability bulletins, related to software and IT/OT components
- Indicators of Compromise (IoCs): e.g. virus signatures, compromised URL and IP addresses, hashes of malware files, etc.
- Incident information: targeted services, observed Kill Chains, etc.
- Descriptive observations and correlation that characterize the threat: Tactics, Techniques and Procedures (TTP)
- Technical scripts and tools to investigate or identify specific attacks

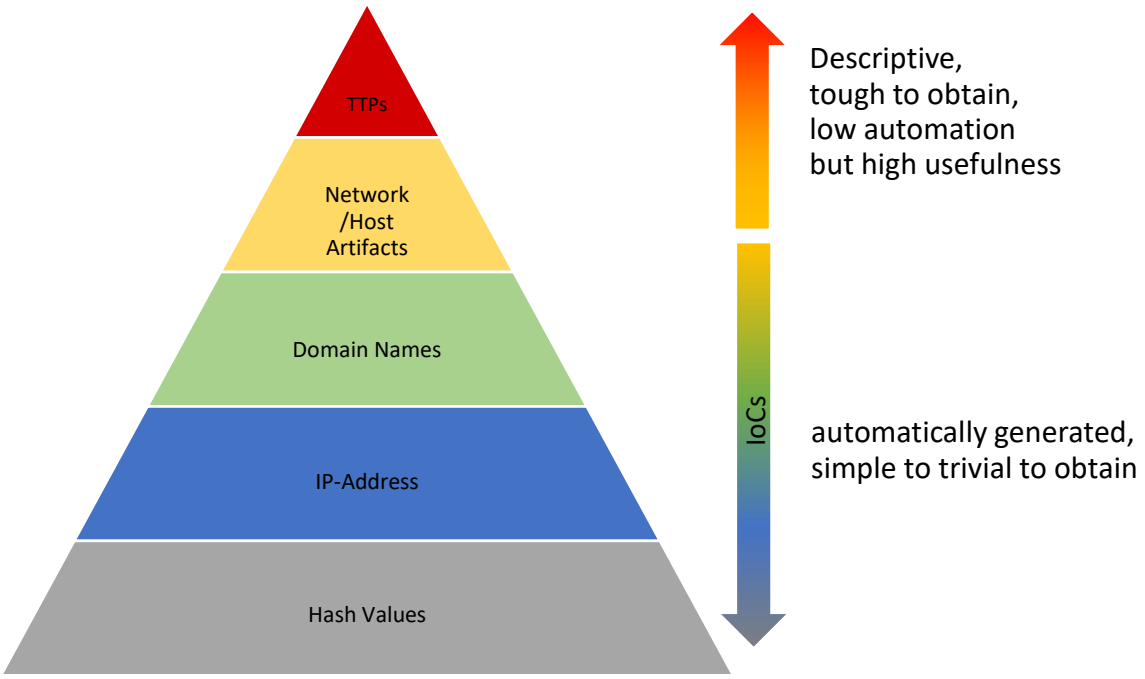

Figure 4 - Pyramid of Pain reflecting the threat intelligence level (Source: David J. Bianco)

Grid participants will only share sensitive and confidential technical information concerning cyber incidents and vulnerabilities if there is a high degree of trust that this information will be properly handled, sanitized, and protected against unintended disclosure. Therefore, a highly trusted environment is required to exchange such information in timely manner. The benefit of sharing such information is that all grid participants have access to up-to-date technical details of the latest cyber-attacks on peer grid organizations, and in other sectors with comparable systems providing them with the opportunity to protect themselves immediately against similar attacks. Without such timely information, grid participants would unnecessarily continue to be exposed longer to already known and exploited attack vectors. A sensitive point regarding sharing such delicate information that could jeopardise or even destroy this well-meant intention is an increased reporting obligation beyond those given in the NIS Directive. An undesired side effect might be that anything that is not covered by such an additional compulsory regulation might not be reported. Therefore, besides any mandatory reporting, a suitable environment must be provided to the grid participants so that they will have confidence in and trust each other. Only in such a voluntary setting of high trust, further information, beyond compulsory reporting, will be shared. The formal team will need to take into consideration all other European cyber reporting initiatives so that there is alignment.

Several schemas for technical information exchange already exist in the European Union:

- In some countries, grid participants are in direct contact with the national CSIRT. Communication about cyberattacks above a certain threshold is mostly mandatory for Operators of Essential Services (OES). In some cases, national authorities may want the victims to keep information private for a certain period, to better control public communication on the event and handle the incident under optimal conditions.

- In some other countries, grid participants share technical information within a sectorial CSIRT dedicated to energy (privately owned or public), which is closely linked with the national CSIRT and international CSIRT-networks.

Additionally, in some cases, grid participants are members of specific sectorial and local ISACs (Information Sharing and Analysis Centres) or associations to promote exchange (e.g. EE-ISAC[8] consisting of utilities, academia and research institutions, government and NGO, and service providers ; Industrial Control System SIG by FIRST.org).

To enable closed and trusted interactions between grid participants, the different cases above will have to be integrated in an all-embracing communication scheme, where a dedicated "European trusted Energy CSIRT" is implemented for gathering, evaluation and distributing the energy-sector specific information (see Figure 5). This CSIRT will be the trusted hub connected to grid participants by the means of a national CSIRT or by a sector specific CSIRT to gather the mandatory reporting flow (according to the NIS Directive). But it will also be directly connected to grid participants to ensure a timely distribution of information and enable a voluntary information sharing stream among grid participants. It should operate at EU-Level to process all the necessary information and data, and make sure that information is being properly sanitized, stored as anonymized (or pseudonymized) data, and shared within the trusted community of grid participants. Grid participants that provide the data are also the data owner and should decide what detail of information is shared with the trusted community, and if it can be released outside of this trusted community after a period of time. This principle creates trust and facilitates voluntary information sharing within the community of grid participants.

The schematic below (Figure 5) depicts the communication flow of the mandatory and voluntary reporting.

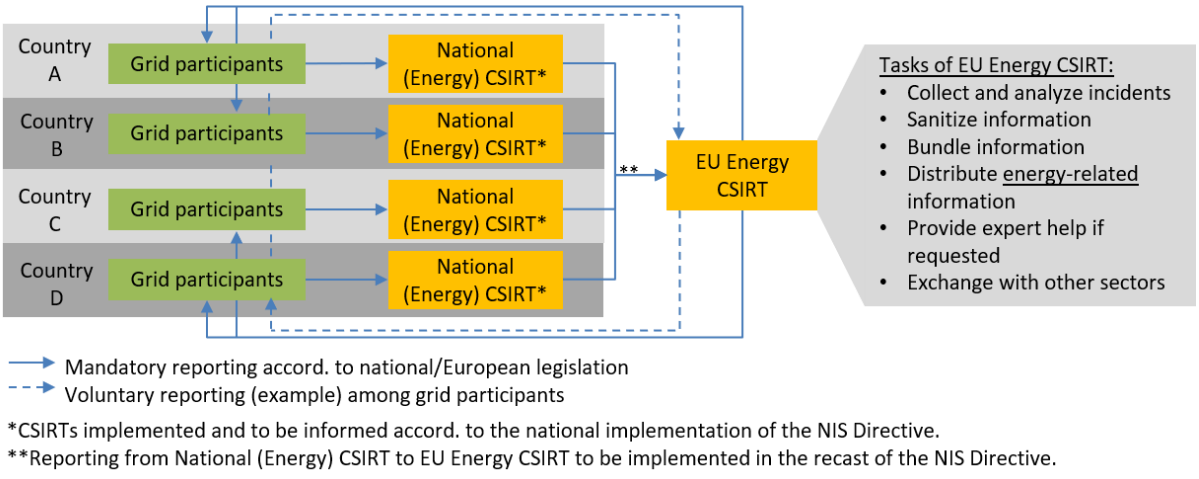

Figure 5 - Schematic of a trusted EU-CSIRT-Structure for the Energy Sector

Furthermore, this European trusted Energy CSIRT handling technical information must be able to appropriately apply threat modelling by taking the sector-specific requirements and conditions into

[8] https://www.ee-isac.eu/

account to assess the interrelationships and interdependencies and thus derive the threats or risks properly. This information is vital for other grid participants to take immediate action if necessary, so that the EU Energy CSIRT shall inform grid participants and national CSIRTs of the threat landscape without undue delay and in parallel. Possibly, the EU Energy CSIRT shall make use of a trusted platform where grid participants can filter the information based on agreed categories (e.g. voltage level, geographic region, assets attacked, etc.) so that the awareness of the recipients does not suffer due to an unnecessarily high volume of information.

To join the trusted community of grid participants, members and connected entities will have to commit and respect specific Terms of Reference, which may specify:

- In which cases information sharing to the European trusted Energy CSIRT is mandatory (e.g. only based on NIS Directive requirements)
- How exceptions are processed, to conform with national specific rules
- What information is expected to be shared to the European trusted Energy CSIRT
- How to handle and use the sanitized information shared by the European trusted Energy CSIRT
- When the information can be expected to be shared outside the community – except those covered by specific provisions of national obligations
- Technical conditions to secure communications and data processing: sharing and encryption methods, standard operating procedures

To inform and instruct concerning restrictions for the further spreading of shared information, it is recommended to use the Traffic Light Protocol (TLP).

A responsibility to share technical information must go hand in hand with a responsibility to monitor and detect intrusions. Grid participants must be obligated to identify risks and to detect threats.

Several options are possible to set up the European trusted Energy CSIRT in the European landscape, where different structures for cyber technical information sharing are already in place:

- Build on the experimental TSO SOC, extend to all grid participants, and install the SOC as a permanent institution, financed by ENTSO-E and EU DSO Entity.
    - Opportunity: an existing trusted hub base, dedicated to grid operators
    - Attention point: governance adaptation is required to include all grid participants
- Build on the existing base of energy sectorial CSIRTs and federate the network
    - Opportunity: cooperation model in line with the revised NIS principles, plus easiness to evolve and align with future evolutions (emergence of cross-sector CSIRTs, etc.)
    - Attention point: communication scheme to be adapted for MS without sectorial CSIRT; sharing of voluntary information might be more difficult because such network is not dedicatedly founded and hosted by grid participants.
- Use the existing EE-ISAC and create a subgroup dedicated to Grid Participants
    - Opportunity: rely on an existing information sharing organisation, dedicated to energy
    - Attention point: EE-ISAC members variety (suppliers, manufacturers, consultancies) cannot enable the same level of trust than the Grid operator’s community could. Hence a subgroup would have to be instantiated with specific rules and governance.

The recommended option for the sharing of technical information is a European trusted Energy CSIRT, a jointly managed, owned, and combined ENTSO-E/EU DSO entity team. Other less preferred options include separate CSIRT teams for ENTSO-E and EU DSO entity, or an outsourced Energy sector specific CSIRT team.

Such CSIRT team(s) should be established to perform and maintain the following activities:

1. Actively build up and maintain a highly trustable environment to exchange sensitive information between grid participants
2. Collect and analyse technical incident and vulnerability information from all European grid participants (act as the trusted information broker).
3. Sanitize this information by using a commonly agreed procedure so that the source of the information (participant) and impact of the incident or vulnerability is not disclosed. It will be specified how and where the sanitization is realized: by the source or by the trusted hub.
4. Use a standardised common taxonomy for cyber incidents (e.g. Mitre ATT&CK framework) to classify the information that supports rapid and stringent reporting. This allows the recipients of the shared information, to be clear what kind of threat it is.
5. Timely distribution of this technical information to all grid participants via secure means with no undue delay.
6. Report this technical information to other CSIRTs after a delay agreed with the information provider. The important point is that all grid and market participants should be given the opportunity to check their own IT/OT systems for the same cyber-attack or vulnerability first before this eventually becomes public domain knowledge.
7. Provide expert help and advice for incident response (if requested), with special attention for ICS/SCADA cybersecurity.
8. Leverage and manage bilateral information exchange with CSIRTs of other sectors to mitigate possible cascading effects and to benefit of their experience
9. Organise sector-specific exchange experiences and coordinate or participate in table-top exercises.
10. Collect and share information on its own account (skilled capabilities) to grid participants

6 Conclusions

The combination of the five recommendations defined in this final report will together in the view of the informal drafting team significantly improve the cross-border cybersecurity risk posture of European grid participants. It is important to stress that the ongoing renewable energy transition will deliver an unprecedented deployment of large grid connected IoT devices which when aggregated will form an unpredictable pool of energy. A growing risk is where the control and connectivity of these decentralised pools of energy are relying solely on public internet connections.

This final report of the informal drafting team has made its recommendations. The next stage of this Network Code process will be for the formal drafting teams to clearly define the legal mission, mandate, working structure and governance of:

1. The working group with responsibilities for cross-border cyber risk identification and management (Section 5.1) and the definition of appropriate controls and requirements to protect essential business processes (Section 5.3).
2. The accreditation scheme for grid participant auditors and certification bodies (Section 5.2). Only an EU accreditation body can give accreditation to certification bodies.
3. The product assurance scheme (as defined in Section 5.4). Any new assurance scheme must be in line with the EU Cybersecurity Act.
4. The information sharing scheme (as defined in Section 5.5). The body chosen to receive, sanitize and distribute grid participant incident and vulnerability information in a timely manner must be completely trusted to work with and for all grid participants.

Some Smart Grid Task Force Expert Group 2 (SGTF-EG2) recommendations were considered not suitable for inclusion in a Network Code on cybersecurity, for example, the security of the supply chain problem, cyber maturity, and crisis management. The informal drafting team does consider existing standards such as IEC 62443-4-1 as suitable and applicable, since certification ensures that a secure development lifecycle (SDLC) process is well defined, implemented and enforced across a product's lifespan, from design to end-of-life. However, it was the opinion of the informal drafting team that the security of the supply chain is such a difficult, complex, and political topic, that it does not fit well for inclusion in this Network Code. For cyber maturity, ENISA are currently mapping control frameworks to the ES-C2M2[9] Cybersecurity Capability Maturity Model, and the formal drafting team should include and reference this work when the mapping has been completed. For crisis management, this topic naturally fits best under existing ENTSO-E Network Codes and Guidelines, Regulation 2019/941 on risk-preparedness in the electricity sector and the new NIS 2.0 Directive, although the recommendation on information sharing (Section 5.5) would provide a means to distribute crisis management information to all grid participants in a secure and timely manner.

[9] https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program

Annex A – Drafting Team

Name	Association	Company	E-Mail
Anders Åhlgren	**GEODE**	Jönköping Energi	anders.ahlgren@jonkopingenergi.se
Peter Allaert	**CEDEC**	Fluvius	peter.allaert@fluvius.be
Grzegorz Bojar	**ENTSO-E**	PSE	grzegorz.bojar@pse.pl
Andrea Foschini	**ENTSO-E**	Terna	andrea.foschini@terna.it
Bart Luijkx	**Eurelectric**	Alliander	bart.luijkx@alliander.com
Nuno Medeiros	**EDSO**	EDP Distribuição	nuno.medeiros@edp.pt
Jeff Montagne	**EDSO**	Enedis	jeff.montagne@enedis.fr
Alina Neagu	**ENTSO-E**	ENTSO-E	alina.neagu@entsoe.eu
Caoimhín Ó BRIAIN	**Eurelectric**	Eurelectric	cobriain@eurelectric.org
Armin Selhofer	**GEODE**	Oesterreichs Energie	a.selhofer@oesterreichsenergie.at
Rolf Strenge	**CEDEC**	EWE Netz	rolf.strenge@ewe-netz.de

Co-Leads

Name	Association	Company	E-Mail
Keith Buzzard	**ENTSO-E**	ENTSO-E	keith.buzzard@entsoe.eu
Christiane Gabbe	**Eurelectric**	EON SE	Christiane.gabbe@eon.com

Annex B – Topic Champions

As part of the informal drafting process a "Champion" for each recommendation has been identified. The Champion acts as the SPOC to make collaboration and consultation as easy and transparent as possible. During the consultation process the Champion will answer and document all open questions.

Topic	Topic Champion	Co-Champion
Cross border Cyber Risk Assessment	Keith Buzzard	Bart Luijkx
ISO/IEC 2700x certification	Christiane Gabbe	Nuno Medeiros
Technical information Sharing (IOC)	Jeff Montagne	Armin Selhofer
Functional Security Requirements	Bart Luijkx	Keith Buzzard
Product and system testing assurance scheme	Peter Allaert	Anders Åhlgren

Annex C - Figures

Annex D – Tables