ACER
European Union Agency for the Cooperation of Energy Regulators

Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS)

July 6, 2022 –V2.3

This document contains **the Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS)** as revised by ACER, on the basis of the proposal developed by ENTSO-E and the EU DSO entity and submitted to ACER on 14 January 2022, according to Article 5(1)(c) of Regulation (EU) 2019/942[1] and Articles 59(2)(e) and 59(11) of Regulation (EU) 2019/943[2].

On 24 June 2022, ACER's Electricity Working Group broadly endorsed the draft revised NCCS, according to Article 24(2) of Regulation (EU) 2019/942.

On 13 July 2022, the Board of Regulators provided a favourable opinion on the draft revised NCCS, according to Article 22(5)(a) of Regulation (EU) 2019/942.

[1] Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulators OJ L 158 14.6.2019, p. 22

[2] Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity OJ L 158 14.6.2019, p. 54

Revised network code on sector-specific rules for cyber security aspects of cross-border electricity flows

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity, and in particular Article 59(2)(e) thereof,

Whereas:

(1) Cybersecurity risk management is crucial for maintaining security of electricity supply and for ensuring a high level of cybersecurity in the electricity sector.

(2) Digitalisation and cybersecurity are crucial to provide essential services and therefore of strategic relevance for critical energy infrastructure. This Regulation therefore contributes to the key objectives set in the "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade" (JOIN(2020) 18 final).

(3) Directive (EU) 2016/1148 of the European Parliament and of the Council lays down general rules on security of network and information systems. Regulation (EU) 2019/941 complements Directive (EU) 2016/1148 by ensuring that cybersecurity incidents are properly identified as a risk and that the measures taken to address them are properly reflected in the risk-preparedness plans. Regulation (EU) 2019/943 complements Directive (EU) 2016/1148 and Regulation (EU) 2019/941 by setting out specific rules for the electricity sector at Union level.

(4) Article 59(2)(e) of Regulation (EU) 2019/943 empowers the Commission to adopt delegated acts on sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management. This Regulation is adopted as a delegated act to supplement and amend certain non-essential elements of Regulation (EU) 2019/943. It also complements the provisions of Directive (EU) 2016/1148 regarding the electricity sector.

(5) Recital (1) and (15) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity ('ENISA') and on information and communications technology cybersecurity certification recognises the vital role of the energy sector for the economy and foresees ENISA to liaise with the European Union Agency for the Cooperation of Energy Regulators ('ACER').

(6) Regulation (EU) 2019/943 assigns specific responsibilities with regard to cybersecurity to Transmission System Operators ('TSOs') and Distribution System Operators ('DSOs'). Their European associations the European network of TSOs for electricity ('ENTSO for Electricity') and the European entity for DSOs ('EU DSO entity') shall promote cybersecurity in cooperation with relevant authorities and regulated entities.

(7) The provisions of this Regulation should be without prejudice to Union law providing for specific rules on the certification of ICT products, ICT services and ICT processes, in particular without prejudice to the provisions laid down in Article 46 of Regulation (EU) 2019/881 with

regard to the framework for the establishment of European cybersecurity certification schemes.

(8) Technology is evolving constantly and digitalisation of the electricity sector is progressing rapidly. This Regulation shall not be detrimental to innovation and not constitute a barrier to access the electricity market and the subsequent use of innovative solutions that contribute to the efficiency and sustainability of the electricity system.

(9) The information collected for monitoring the implementation of this Regulation shall be limited to a reasonable amount. Stakeholders shall be granted achievable and effective deadlines for submitting such information. Double notification should be avoided.

(10) Cybersecurity protection does not stop at the Union's borders. A secure system requires the involvement of neighbouring third country parties. The Union, its Member States and national institutions should strive to support neighbouring third countries in applying similar cybersecurity rules as set out in this Regulation.

(11) This Regulation has been developed in close cooperation with ACER, ENISA, the ENTSO for Electricity, the EU DSO entity and stakeholders, in order to adopt effective, balanced and proportionate rules in a transparent and participative manner. In accordance with Article 60 of Regulation (EU) 2019/943, the Commission, ACER, the ENTSO for Electricity and the EU DSO entity will follow the procedure and consultation obligations set out in Article 59 of Regulation (EU) 2019/943 before proposing any amendment to this Regulation.

(12) This Regulation is without prejudice of the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security.

HAS ADOPTED THIS REGULATION:

TITLE I
GENERAL PROVISIONS

Article 1. Subject Matter

This Regulation establishes a network code which lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

Article 2. Scope

1. The provisions set out in this Regulation shall apply to the following entities insofar as their activities have a cybersecurity impact directly on cross-border electricity flows:

   (a) electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944;

(b) nominated electricity market operators or 'NEMOs' as defined in Article 2(8) of Regulation (EU) 2019/943;

(c) 'organised market place' or 'organised market' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014 that arrange transactions on products relevant to cross-border electricity flows;

(d) critical service providers as defined in Article 4(12) of this Regulation;

(e) the ENTSO for Electricity established pursuant to Article 28 of Regulation (EU) 2019/943;

(f) the EU DSO entity established pursuant to Article 52 of Regulation (EU) 2019/943;

(g) the European Union Agency for the Cooperation of Energy Regulators or 'ACER' established by Regulation (EU) 2019/942;

(h) national competent authorities designated for this Regulation pursuant Article 5 or 'NCCS-NCA' as defined in Article 6 of this Regulation;

(i) regulatory authorities or 'NRAs' as defined in Article 59 of Directive (EU) 2019/944;

(j) national competent authorities for risk preparedness or 'RP-NCA' established pursuant to Article 3 of Regulation (EU) 2019/941;

(k) managed security service provider or 'MSSP' as defined in Article 4(37) of this Regulation;

(l) national competent authorities on the security of network and information systems or 'CS-NCA' as defined in Article 8 of Directive (EU) 2016/1148;

(m) computer security incident response teams or 'CSIRTs' established pursuant to Article 9 of Directive (EU) 2016/1148;

(n) the European Union Agency for Cybersecurity or 'ENISA' established pursuant to Regulation (EU) 2019/881; and

(o) any entity or third party to whom responsibilities have been delegated or assigned.

2. This Regulation shall not apply to micro or small enterprises, or any other entity not listed in Article 2(1) unless the micro or small enterprise, or any other entity, is classified as a critical-impact or high-impact entity in accordance with the electricity cybersecurity impact index developed under Article 17 of this Regulation or in accordance with the criteria set out in Article 33(3) and (5) of this Regulation.

3. This Regulation shall apply to critical service providers not established in the Union but who deliver services to entities in the Union. Where such a critical service provider delivers services to process data, large-scale services and regular services to entities established in the Union, this critical service provider shall explicitly designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The critical service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established. This representative may be addressed by any competent authority in the Union instead of the critical service provider with regard to obligations of that critical service provider under this Regulation. In the absence of a designated representative within the Union under this

paragraph, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Regulation. The designation of a representative by an entity referred to in this paragraph shall be without prejudice to legal actions, which could be initiated against the entity itself.

4. This Regulation shall apply to high and critical impact entities not established in the Union who are identified in accordance with Article 33(2). This high or critical impact entity shall explicitly designate a representative in the Union. The representative shall be established in one of the Member States. The high or critical entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this paragraph, any Member State may take legal actions against the entity for non-compliance with the obligations under this Regulation. The designation of a representative by an entity referred to in this paragraph shall be without prejudice to legal actions, which could be initiated against the entity itself.

5. This Regulation is without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where such exchange is necessary for the application of this Regulation. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of the entities in scope of this Regulation.

6. This Regulation is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.

Article 3. Objectives

1. This Regulation aims at:

   (a) establishing a solid governance for cybersecurity aspects of cross-border electricity flows to ensure the reliability of the electricity system and to ensure close collaboration with existing governance structure(s) for cybersecurity;

   (b) determining common criteria for performing risk assessments based on defined risk scenarios for the operational reliability of the electricity system with regard to cross-border electricity flows;

   (c) promoting a common electricity cybersecurity framework and by that fostering a common minimum electricity cybersecurity level across the Union;

   (d) providing for clear verification rules in order to assess the application of the minimum and advanced cybersecurity controls;

   (e) establishing information flows by setting up a system for the collection and sharing of information in relation to cross-border electricity flows;

(f) establishing effective processes to identify, classify and respond to cross-border cybersecurity incidents;

(g) setting up effective processes for crisis management to handle cybersecurity incidents of cross-border relevance;

(h) defining common principles for electricity cybersecurity exercises to increase resilience and improve the risk preparedness of the electricity sector;

(i) protecting the information exchanged under this Regulation;

(j) determining a process for monitoring the implementation of this Regulation, to assess the effectiveness of investments in cybersecurity protection and to report on the progress of cybersecurity protection across the Union;

(k) ensuring that the cybersecurity procurement requirements with relevance for cross-border electricity flows are not detrimental to innovation, new systems, processes and procedures.

2. When applying this Regulation, Member States, relevant authorities and system operators shall:

(a) apply the principles of proportionality and non-discrimination;

(b) ensure transparency;

(c) respect the responsibility assigned to the relevant system operator in order to ensure system security;

(d) consult with relevant stakeholders and take account of potential impacts on their systems;

(e) take into consideration agreed European standards and technical specifications;

(f) avoid double reporting and strive to reduce additional administrative burden on all involved entities.

Article 4. Definitions

For the purpose of this Regulation, the definitions in Article 2 of Regulation (EU) 2019/943, the definitions in Article 2 of Directive (EU) 2019/944, the definitions in Article 4 of Directive (EU) 2016/1148, the definitions in Article 2 of Regulation (EU) 2019/941 and the definitions in Article 2 of Regulation (EU) 2019/881 apply.

The following definitions also apply:

(1) ‘asset’ means anything that has value to an entity, including business processes, information, hardware, software, networks and sites;

(2) ‘background verification check’ means a verification of the identity and background of staff or contractors of an entity in accordance with relevant laws, regulations, and ethics, which is proportional to business requirements, the classification of the information to be accessed and the perceived risks. The verification check may be performed by the entity itself, an external company performing a screening, or through a government clearing;

(3) ‘competent authority for cybersecurity’ or ‘CS-NCA’ means all national competent authorities responsible for the implementation, monitoring and supervision of cybersecurity in the

electricity sector at Member State level designated in accordance with Article 8 of Directive (EU) 2016/1148;

(4) ‘competent authority for risk preparedness’ or ‘RP-NCA’ means the competent national authority designated pursuant to Article 3 of Regulation (EU) 2019/941.

(4a) ‘national competent authority designated for the purposes of this Regulation’ or ‘NCCS-NCA’ means a national governmental authority or a regulatory authority designated by a Member State, in accordance with Article 5 of this Regulation;

(5) ‘computer security incident response team’ or ‘CSIRT’ means a team responsible for risk and incident handling in accordance with Article 9 of Directive (EU) 2016/1148;

(6) ‘conformity assessment body’ means a body that performs conformity assessment activities including calibration, testing, certification and inspection, as defined in Article 2(13) of Regulation (EC) No 765/2008;

(7) ‘critical-impact asset’ means an asset needed for a critical-impact process;

(8) ‘critical-impact entity’ means an entity that has a critical-impact process;

(9) ‘critical-impact perimeter’ means a perimeter defined by any entity listed at Article 2(1), 2(3) and 2(4) that contains all critical-impact assets and on which access to these assets can be controlled; the critical-impact perimeter defines the scope where the advanced cybersecurity controls apply;

(10) ‘critical-impact process’ means a business process for which the electricity cybersecurity impact indices are above the critical-impact threshold;

(11) ‘critical-impact threshold’ means the values of the electricity cybersecurity impact indices at Article 17(4), above which a cyber attack on a process will cause disruption of cross-border electricity flows;

(12) ’critical service provider' means a natural or legal person who provides an ICT product, ICT service, or ICT process that is needed for a critical-impact process, and that if compromised may cause a cybersecurity incident with impact above the critical-impact threshold;

(13) ‘regional electricity crisis’ means a present or imminent situation in which more than one Member State has declared an electricity crisis at the same time (simultaneous crisis in two or more Member States) as defined in the "Methodology to Identify Regional Electricity Crisis Scenarios in accordance with Article 5 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on risk preparedness in the electricity sector and repealing Directive 2005/89/EC”;

(14) ‘CSIRT-NCA’ means the CSIRT or the CS-NCA when designated by the Member State as the competent authority to whom entities shall notify incidents or cyber attacks pursuant to Article 14(3) of Directive (EU) 2016/1148;

(15) ‘cyber attack’ means any attempt with malicious intent to gain access to network and information systems. A cyber attack may cause an incident where damages, disruptions or dysfunctionalities occur;

(16) 'cybersecurity-by-design' means that during the design and development of ICT products, ICT services, and ICT processes, appropriate technical measures for ensuring cybersecurity are considered;

(17) 'cybersecurity cross-border crisis' means a regional electricity crisis that is partially or totally caused or that can be correlated to the materialisation of a risk of cybersecurity nature;

(18) 'cybersecurity operation centre' or 'CSOC' means a team consisting of one or more persons who perform security related tasks (CSOC services) such as handling of incidents and security configuration errors, security monitoring, log analysis, and incident detection;

(19) 'cybersecurity posture' means the overall cybersecurity status of an entity including procedures, processes, skills, tools and resources to defend itself proactively and reactively against cyber attacks;

(20) 'cybersecurity procurement requirements' means the requirements that entities define for new or updated ICT products, ICT processes or ICT services during procurement;

(21) 'early warning' means a provision of concrete information indicating the existence of a possible cyber-threat;

(22) 'early warning system' means a solution for gathering, processing and notifying of early warnings;

(23) 'electricity cybersecurity impact index' or 'ECII' means the indices for business processes of the electricity sector to estimate the possible consequences of cyber attacks to cross-border electricity flows as defined in Article 17(4);

(24a) 'Electricity Coordination Group' is a forum for the exchange of information and coordination of electricity policy measures having a cross-border impact, as defined in the Commission Decision 2012/C 353/02 of 15 November 2012;

(24) 'entity' means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

(25) 'European cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes, as defined in Article 2(9) of Regulation (EU) 2019/881;

(26) 'high-impact asset' means any asset needed for a high-impact process;

(27) 'high-impact entity' means an entity that has a high-impact process;

(28) 'high-impact perimeter' means a perimeter defined by an entity that contains all high-impact assets and on which access to these assets can be controlled; the high-impact perimeter defines the scope where the minimum cybersecurity controls apply;

(29) 'high-impact process' means any business process for which the electricity cybersecurity impact indices are above the high-impact threshold;

(30) 'high-impact threshold' means the values of the electricity cybersecurity impact indices

defined by the ENTSO for Electricity in cooperation with the EU DSO entity above which a cyber attack on a process could cause disruption of cross-border electricity flows;

(31) 'ICT service' means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems as defined in Article 2(13) of Regulation (EU) 2019/881;

(32) 'incident' means any event, including a cybersecurity incident, compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via network and information systems;

(33) 'information and communication technology' or 'ICT' means any information being processed digitally by information technology systems and transferred across communication networks;

(34) 'legacy system' means a network and information system that cannot always be modified or updated to meet minimum cybersecurity requirements;

(35) 'likelihood' means the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically such as a probability or a frequency over a given time period;

(36) 'managed security service provider' or 'MSSP', means any entity which provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. It also includes the use of high-availability security operation centres (either from their own facilities or from other data centre providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture;

(37) 'NIS Cooperation Group' means a group with a mission to achieve a high common level of security for network and information systems in the Union as described in Article 11 of Directive (EU) 2016/1148. It supports and facilitates the strategic cooperation and the exchange of information among Member States. The NIS Cooperation Group is composed of representatives of the Member States, the Commission and ENISA;

(38) 'originator' means an entity that initiates an information exchange, information sharing or information storage event;

(39) 'real-time system' means a system in which its temporal properties are essential for reliability and correctness;

(40) 'risk impact matrix' means a matrix used during risk assessment to determine the resulting risk impact level for each risk assessed;

(41) 'simultaneous electricity crisis' means an electricity crisis affecting more than one Member State at the same time;

(42) 'national single point of contact' means the single point of contact designated by each Member State pursuant to article 8(3) of Directive (EU) 2016/1148;

(43) 'system operation regions' means the system operation regions as defined in accordance with

Article 36 of Regulation (EU) 2019/943;

(44) 'Union-wide critical-impact process' means any electricity sector process, possibly involving multiple entities, for which the possible impact of a cyber incident or cyber attack may be deemed critical during the execution of the Union-wide risk assessment;

(45) 'Union-wide high-impact process' means any electricity sector process, possibly involving multiple entities, for which the possible impact of a cyber incident or cyber attack may be deemed high during the execution of the Union-wide risk assessment;

(46) 'vulnerability' means a weakness, susceptibility or flaw of an ICT asset or a system that can be exploited by a cyber threat;

(47) 'zero day vulnerability' means a vulnerability in an ICT asset, that was not spotted during the testing phase and has been discovered by at least one person but has not yet been publicly disclosed and patched;

(48) 'zero trust architectures' means an architecture for network and information systems in which devices (a) are not trusted even when they are within a secure perimeter, (b) verify all requests they receive and (c) apply the least privilege principle.

Article 5. National competent authority for the purposes of this Regulation (NCCS-NCA)

1. As soon as possible and in any event by 6 months after entry into force of this Regulation, each Member State shall designate a national governmental or regulatory authority (NCCS-NCA) as its competent authority for the purposes of this Regulation. The NCCS-NCA shall be responsible for carrying out the tasks assigned to it in this Regulation. Where appropriate, until the NCCS-NCA has been designated, the national entities responsible for the security of electricity supply shall carry out the tasks of the NCCS-NCA in accordance with this Regulation.

2. Member States shall, without delay, notify the Commission, ACER and the Electricity Coordination Group and make public the name and the contact details of their NCCS-NCA designated pursuant to paragraph 1 and any subsequent changes to thereto.

3. Member States may allow the NCCS-NCA to delegate tasks assigned to them in this Regulation to other national entities with the exception of the tasks listed in Article 14, Article 6(1), and Article 32(1). The NCCS-NCA pursuant to paragraph 1 shall monitor the application of this Regulation by the entities to whom it has delegated tasks. The NCCS-NCA shall communicate the name, contact details, assigned tasks and any subsequent changes thereto of the entities to whom a task has been delegated to the Commission, to ACER, to ENISA and to the NIS Cooperation Group, in order to foster efficiency and smooth cooperation at Member States and Union level.

4. As soon as possible and in any event by 12 months after entry into force of this Regulation, the NCCS-NCAs shall develop and approve processes intended to be used for performing their tasks and to exercise their decision-making powers under this Regulation, informing the cybersecurity risk Working Group pursuant Article 15. The NCCS-NCAs shall review the effectiveness of the adopted processes used to perform their tasks and to exercise their decision-making powers under this Regulation, at least after each cybersecurity risk assessment cycle, informing the cybersecurity

risk Monitoring Body. The NCCS-NCAs may develop the new processes intended to be used for performing their tasks and to exercise their decision-making powers under this Regulation within six months informing the cybersecurity risk Working Group. The NCCS-NCAs shall approve it within 12 months after the recommendation of the cybersecurity risk Monitoring Body.

Article 6. Cooperation between NCCS-NCAs, CS-NCAs, NRAs, RP-NCAs and CSIRTs of a Member State

1. The NCCS-NCAs shall coordinate the cooperation of at least the CS-NCAs, the NRAs, RP-NCAs and CSIRTs with each other within their own Member State with regards to the fulfillment of the obligations laid down in this Regulation. CS-NCAs, the NRAs, RP-NCAs and CSIRTs shall exchange all necessary information and data to carry out their tasks without prejudice to the confidentiality requirements pursuant to Article 11.

2. Where they are separate bodies, the CS-NCA and the CSIRT of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in Title VIII and X of this Regulation.

Article 7. Mutual assistance among NCCS-NCAs

Where a high or critical impact entity is providing services in more than one Member State, or has its seat or other establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the NCCS-NCAs of the Member States concerned shall cooperate with and assist each other as necessary. This cooperation shall entail, at least, that:

(a) the NCCS-NCAs applying supervisory or enforcement measures in a Member State under this Regulation shall inform and consult the NCCS-NCAs in the other Member States concerned on the supervisory and enforcement measures taken and their follow-up;

(b) a NCCS-NCA may request another NCCS-NCA to take supervisory or enforcement measures;

(c) a NCCS-NCA shall, upon receipt of a justified request from another NCCS-NCAs, provide the other NCCS-NCAs with assistance so that the supervision or enforcement actions can be implemented in an effective, efficient and consistent manner. Such mutual assistance may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits.

Article 8. Adoption of terms and conditions or methodologies or plans

1. The following terms and conditions or methodologies and any amendments thereof shall be subject to approval by all NCCS-NCAs:

(a) the cybersecurity risk assessment methodologies pursuant to Article 17(1);

(b) the cross-border electricity cybersecurity risk assessment report pursuant to Article 22;

(c) the minimum and advanced cybersecurity controls and the electricity controls to standards mapping Matrix (ECSMM) pursuant to Article 23 including supply chain security controls in accordance with Article 29 and the mapping pursuant to Article 31;

(d) a cybersecurity procurement recommendation pursuant to Article 37; and

(e) the cybersecurity incidents classification scale methodology pursuant to Article 40(6).

2. The regional cybersecurity risk treatment plans pursuant to Article 22 and any amendments thereof shall be subject to approval by all NCCS-NCAs of the concerned system operation region.

3. The ENTSO for Electricity shall develop, in cooperation with the EU DSO entity, the terms and conditions, methodologies and plans required by this Regulation, shall regularly inform the NCCS-NCAs and ACER about the progress of developing them, and shall submit proposals of those terms and conditions, methodologies and plans for approval to the NCCS-NCAs according with paragraphs 1 and 2 within the respective deadlines set out in this Regulation. The NCCS-NCAs may jointly prolong these deadlines in exceptional circumstances, notably in cases where a deadline cannot be met due to circumstances external to the sphere of ENTSO for Electricity or of the EU DSO entity.

4. Where TSOs deciding on proposals for terms and conditions or methodologies listed in paragraph 1 are not able to reach an agreement, they shall decide by qualified majority voting. The qualified majority shall be reached within each of the respective voting classes of TSOs. A qualified majority for proposals listed in paragraph 1 shall require the following majority:

(a) TSOs representing at least 55 % of the Member States; and

(b) TSOs representing Member States comprising at least 65 % of the population of the Union.

A blocking minority for decisions on proposals for terms and conditions or methodologies listed in paragraph 1 shall include TSOs representing at least four Member States, failing of which the qualified majority shall be deemed attained.

For TSOs' decisions on proposals for terms and conditions or methodologies listed in paragraph 1, one vote shall be attributed per Member State. If there is more than one TSO in the territory of a Member State, the Member State shall allocate the voting powers among the TSOs.

5. The proposals for terms and conditions, methodologies or plans shall include a proposed timescale for their implementation and a description of their expected impact on the objectives of this Regulation. They shall be subject to prior consultation in accordance with the procedure set out in Article 9.

6. The ENTSO for Electricity shall submit the proposal for terms and conditions, methodologies or plans for information to ACER while it submits the proposal for approval to the NCCS-NCAs.

7. Upon a joint request of the NRAs, ACER shall issue an opinion on the proposal for terms and conditions, methodologies or plans within six months of the receipt of the request and notify NRAs and NCCS-NCAs of the opinion. NRAs and NCCS-CSAs shall coordinate with each other before the NRA requests an opinion to ACER. ACER may include recommendations in such opinion. ACER shall consult ENISA before issuing an opinion on the proposals listed in Article 8(1).

8. The NCCS-NCAs shall consult and closely cooperate and coordinate with each other in order to reach an agreement on the proposed terms and conditions, methodologies or plans. Before approving the terms and conditions or methodologies, they shall revise and complete the proposals where necessary, after consulting the ENTSO for Electricity and the EU DSO entity, in order to ensure that they are in line with this Regulation and contribute to market integration, non-discrimination, effective competition and the proper functioning of the market. When applicable, they shall take into account the opinion issued by ACER according to paragraph 7.

9. In the event that NCCS-NCAs jointly request an amendment to approve the proposed terms and conditions or methodologies, the ENTSO for Electricity shall develop, in cooperation with the EU DSO entity, a proposal for amended terms and conditions or methodologies and submit it for approval within two months following the request of the NCCS-NCAs.

10. The NCCS-NCAs shall take coordinated decisions concerning the submitted terms and conditions or methodologies within six months following the receipt of the terms and conditions or methodologies by the last NCCS-NCA concerned. Where ACER issued an opinion according to paragraph 7, the NCCS-NCAs shall take their decisions within six months from the receipt of ACER's opinion. If the ENTSO for Electricity submitted a proposal for amended terms and conditions or methodologies according to paragraph 9, the period within which the NCCS-NCAs shall decide is prolonged by two months.

11. The ENTSO for Electricity and the EU DSO entity shall publish the terms and conditions or methodologies on their websites after their approval by the NCCS-NCAs, except where such information is considered as confidential in accordance with Article 11.

12. If the ENTSO for Electricity in cooperation with the EU DSO entity fails to submit a proposal for terms and conditions or methodologies to the NCCS-NCAs in accordance with paragraphs 6 or 9, they shall provide the NCCS-NCAs and ACER with the relevant drafts of the proposals for the terms and conditions or methodologies and explain what has prevented the submission of a proposal. The NCCS-NCAs shall jointly take the appropriate steps for the adoption of the required terms and conditions or methodologies, for instance by requesting amendments to the drafts pursuant to this paragraph, by revising and completing those drafts, or, where no drafts have been provided, by defining and approving the required terms and conditions or methodologies.

13. Where the NCCS-NCAs have not been able to reach agreement within the periods referred to in paragraph 10, they shall inform the Commission, and may request the Commission to take the appropriate steps to make possible the adoption of the required terms and conditions or methodologies.

14. The NCCS-NCAs may jointly request proposals for amendments of the approved terms and conditions or methodologies from ENTSO for Electricity and the EU DSO entity and determine a deadline for the submission of those proposals. The ENTSO for Electricity, in cooperation with the EU DSO entity, may propose amendments to the NCCS-NCAs also on its own initiative. The proposals for amendment to the terms and conditions, or methodologies shall be developed and approved in accordance with the procedure set out in this Article.

15. At least after each cybersecurity risk assessment cycle, the ENTSO for Electricity in cooperation

with the EU DSO entity, shall review the effectiveness of the methodologies adopted according to points (a), (c) and (e) of paragraph 1 and shall report the findings of the review to the competent NCCS-NCAs and ACER without undue delay.

Article 9. Public consultation

1. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall consult stakeholders, including ACER, ENISA and the NCCS-NCA of each Member State, on the draft proposals for terms and conditions or methodologies listed in Article 8(1)(a), (b), (c), (d) and (e). The consultation shall last for a period of not less than one (1) month.

2. The proposals for methodologies submitted by the ENTSO for Electricity in cooperation with the EU DSO entity at Union level shall be published and, simultaneously, submitted to public consultation at Union level. Proposals submitted by the ENTSO for Electricity in cooperation with the EU DSO entity at regional level shall be submitted to public consultation at least at regional level.

3. The ENTSO for Electricity in collaboration with the EU DSO entity shall duly take into account the views of stakeholders resulting from the consultations prior to its submission for regulatory approval. In all cases, a sound justification for including or not including the views resulting from the consultation shall be provided together with the submission of the proposal and published in a timely manner before, or simultaneously with the publication of the proposal for methodologies.

Article 10. Recovery of costs

1. The costs borne by TSOs and DSOs subject to network tariff regulation and stemming from the obligations laid down in this Regulation (i.e. including the costs borne by ENTSO-E and the EU DSO entity) shall be assessed by the relevant NRAs of each Member State. Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms.

2. If requested by the relevant NRAs, TSOs and DSOs referred to in paragraph 1 shall, within a reasonable period prescribed by the NRA, provide the information necessary to facilitate the assessment of the costs incurred.

Article 11. Confidentiality obligation

1. Any information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraphs 2, 3, 4 and 5. All information exchanged among entities listed in the Article 2, for the purposes of implementing this Regulation, shall be protected, considering the level of classification of the information applied to the information by the originator.

2. The obligation of professional secrecy shall apply to any entities subject to the provisions of this Regulation.

3. Any information exchanged with or transmitted among entities listed in the Article 2(1), 2(3) and 2(4), for the purposes of implementing Article 22 of this Regulation, shall be anonymised and aggregated if suitable and possible.

4. Information received by any entities or authorities in the course of their duties may not be divulged to any other entity or authority, without prejudice to cases covered by national law, other provisions of this Regulation or other relevant Union legislation.

5. Without prejudice to cases covered by national or Union legislation, an authority, entity or natural person who receives information pursuant to this Regulation may not use it for any other purpose than carrying out its duties under this Regulation.

6. ACER, after consulting ENISA, all NCCS-NCAs, ENTSO for Electricity and the EU-DSO Entity, within 12 months after the entry into force of this Regulation shall release a guideline addressing mechanisms that all entities at Article 2(1), 2(3) and 2(4) shall use to exchange information, and in particular envisaged communication flows, methods to anonymise and to aggregate information for the purpose of implementation of this article.

7. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Regulation. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of critical-impact or high-impact entities.

Article 12. Monitoring

1. ACER shall monitor the implementation of this Regulation in accordance with Article 32(1) of Regulation (EU) 2019/943. In carrying out the monitoring activities, ACER may cooperate with ENISA and request support from the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group on the implementation of this Regulation.

2. The monitoring shall take place at least every three (3) years and shall:

   (a) assess the contribution of the measures implemented to the objectives set out in the Article 3;

   (b) verify the status of implementation of the applicable cybersecurity risk management measures, with regard to the high-impact and critical-impact entities;

   (c) identify whether additional rules on common requirements, planning, monitoring, reporting and crisis management to the ones laid out in this Regulation may be necessary to prevent risks for the electricity sector; and

   (d) identify areas of improvement for the revisions of this Regulation, or to determine uncovered areas and new priorities that may emerge due to technological advances.

3. Within 12 months after entry into force of this Regulation, ACER, in cooperation with ENISA and after consultation of the ENTSO for Electricity and EU DSO entity, shall define the relevant information that shall be communicated to ACER for the monitoring purposes under this Regulation as well as the process and frequency for the collection, based on the performance indicators defined in accordance with paragraph 5.

4. NCCS-NCAs shall have permanent access to relevant information held by ACER, which ACER has collected in accordance with this Article.

5. ACER in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity, shall issue non-binding performance indicators for the assessment of operational reliability that are related to cybersecurity aspects of cross-border electricity flows.

6. The entities listed in Article 2(1), 2(3) and 2(4) of this Regulation shall submit to ACER the information required for ACER to perform the tasks referred to in paragraph 1.

Article 13. Benchmarking

1. Within 12 months after entry into force of this Regulation, ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide. The non-binding cybersecurity benchmarking guide shall have the aim to explain to NRAs the principles of benchmarking of the implemented cybersecurity controls against the objectives laid down in Article 3, taking into consideration the costs of implementing the controls and the effectiveness of the function played by processes, products, services, systems and solutions used to implement such controls. ACER shall take into account existing benchmarking reports when establishing the non-binding cybersecurity benchmarking guide. ACER shall submit the non-binding cybersecurity benchmarking guide to the NRAs for information.

2. Within 12 months after the establishment of the benchmarking guide pursuant to paragraph 1, the NRAs shall carry out a benchmarking analysis to assess whether current investments in cybersecurity:

   (a) mitigate risks having an impact on cross-border electricity flows;

   (b) provide the desired results and what are the efficiency gains for the development of the electricity systems, and

   (c) are efficient and integrated into the overall procurement of assets and services.

3. For the benchmarking analysis, the NRAs may take into account the non-binding cybersecurity benchmarking guide established by ACER, and shall assess in particular:

   (a) the average expenditure in cybersecurity for mitigating risks having an impact on electricity cross-border flows, especially with respect to the high-impact entities and to the critical-impact entities; and

   (b) in cooperation with ENTSO-E and the EU DSO entity, the average prices of cybersecurity services, systems and products that mainly contribute to the enhancement and maintenance of the cybersecurity posture in the different system operation regions;

   (c) existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of the obligations of this Regulation, as well as to identify possible measures needed to foster efficiency in spending, particularly where cybersecurity technological investments may be needed.

4. Any information related to benchmarking analysis shall be classified and processed pursuant to

data classification requirements of this Regulation, the minimum cybersecurity controls and the cross-border electricity cybersecurity risk assessment report. The benchmarking analysis pursuant to paragraphs 2 and 3 shall not be made public.

5. Without prejudice to the confidentiality requirements pursuant to Article 11 and to the need to protect the security of entities subject to the provisions of this Regulation, the benchmarking analysis pursuant to paragraphs 2 and 3 shall be shared with all NRAs, all NCCS-NCAs, ACER, ENISA and the Commission.

Article 14. Agreements with TSOs not bound by this Regulation

1. Within 18 months after entry into force of this Regulation, all TSOs of a system operation region that is neighbouring to a third country may endeavour to conclude with the third country TSO(s) not bound by this Regulation agreements setting the basis for their cooperation concerning secure cybersecurity protection and setting out arrangements for the compliance of the neighbouring third country TSO(s) with the obligations set out in this Regulation.

2. TSOs shall inform the competent NCCS-NCA of the agreements concluded under this Article.

TITLE II
GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

Article 15. Cybersecurity risk working group

1. Within 3 months after entry into force of this Regulation, the ENTSO for Electricity and the EU DSO entity shall:

   (a) establish a cybersecurity risk working group, and

   (b) define the terms of reference for the Working Group;

   The ENTSO for Electricity and the EU DSO entity shall co-chair the Working Group.

   The Working Group shall consist of representatives of the ENTSO for Electricity, in collaboration with the EU DSO entity, NEMOs and relevant number of the stakeholders listed in Article 2(1) (a), (c), (d), (k) and (o) that represent critical-impact and high-impact entities.

2. The Working Group shall support the ENTSO for Electricity and the EU DSO entity in cybersecurity risk assessments pursuant to Article 19 and 20, in particular with regard to the following tasks:

   (a) development of the cybersecurity risk assessment methodologies pursuant to Article 17(1);

   (b) development of the cross-border electricity cybersecurity risk assessment report pursuant to Article 22;

   (c) development of the common electricity cybersecurity framework pursuant to TITLE IV;

   (d) development of the cybersecurity procurement recommendation pursuant to Article 37;

   (e) development of the cybersecurity incidents classification scale methodology pursuant to

Article 40(6);

(f) development of the transitional electricity cybersecurity impact index pursuant to Article 50(1);

(g) development of the consolidated transitional list of high-impact and critical-impact entities pursuant to Article 50(3);

(h) development of the transitional list of Union-wide high-impact and critical-impact processes pursuant to Article 50(4);

(i) development of the transitional list of European and international standards and controls pursuant to Article 50(5).

(j) performance of the Union-wide cybersecurity risk assessment pursuant to Article 19;

(k) performance of the regional cybersecurity risk assessments pursuant to Article 20;

(l) definition of the regional cybersecurity risk treatment plans pursuant to Article 21; and

(m) development of guidance on European cybersecurity certification schemes for ICT products, ICT services, and ICT processes in accordance with Article 38.

(n) development of guidelines for the implementation of this Regulation in consultation with the cybersecurity risk Monitoring Body pursuant to Article 17.

3. The ENTSO for Electricity, in collaboration with the EU DSO entity, shall regularly inform ACER, ENISA, the NIS Cooperation Group and the Electricity Coordination Group on the implementation cybersecurity risk assessments.

4. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall organise stakeholder involvement via the cybersecurity risk Working Group. This shall include regular meetings with stakeholders to identify problems and propose improvements related to the implementation of this Regulation. This shall not replace the stakeholder consultations in accordance with Article 9.

Article 16. Cybersecurity risk monitoring body

1. Within 3 months after entry into force of this Regulation, ACER shall establish a cybersecurity risk monitoring body (hereafter the 'Monitoring Body'). The Monitoring Body shall consist of representatives of ACER, ENISA and one representative of each NCCS-NCA. The Commission may participate as an observer in the Monitoring Body.

2. The Monitoring Body shall support ACER in the following tasks:

(a) monitoring the implementation and governance of the NCCS-NCAs pursuant to Article 5(4);

(b) monitoring the implementation of application of the cybersecurity standards pursuant to Article 12(2)(b); and

(c) monitoring the adoption process and the implementation of the terms and conditions or methodologies pursuant to Article 8(1)

3. ACER may organise stakeholder involvement via the cybersecurity risk monitoring body. This may include regular meetings with stakeholders to identify problems and propose improvements notably

related to monitoring the implementation of this Regulation.

Article 17. Cybersecurity risk assessment methodologies

1. Within 9 months after entry into force of this Regulation the ENTSO for Electricity, in cooperation with EU DSO entity, shall develop proposals for the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level.

2. The methodologies shall assess cybersecurity risks using the same risk impact matrix. The matrix shall meet the following requirements:

   (a) Consequences of cyber-attacks are measured based on the following criteria:
      (i) Loss of load;
      (ii) Reduction of power generation;
      (iii) Loss of capacity in the primary frequency reserve;
      (iv) Loss of capacity for a black start;
      (v) The expected duration of outage affecting customers in combination with the scale of the outage in customer numbers;
      (vi) any other quantitative or qualitative criteria that could reasonably act as an indicator of the effect of an attack on cross border electricity flows.

   (b) The likelihood of a cyber-attack shall be measured as the frequency of incidents per year.

3. The cybersecurity risk assessment methodologies shall include:

   (a) a list of cyber threats to be considered, including at least the following supply chain threats:
      (i) a severe and unexpected corruption of the supply chain;
      (ii) the unavailability of ICT products, ICT services, or ICT processes from the supply chain;
      (iii) cyber attacks initiated through actors in the supply chain;
      (iv) leaking of sensitive information through the supply chain, including supply chain tracking; and
      (v) the introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain.

   (b) criteria to evaluate the consequences and cybersecurity risks as high or critical using defined thresholds for consequences and likelihood; and

   (c) an approach to analyse the cybersecurity risks coming from legacy systems, the cascading effects of incidents and the real-time nature of systems operating the grid.

4. The methodology for the risk assessment at Union level shall describe how the electricity cybersecurity impact indices (ECII), and the high-impact and critical-impact thresholds will be defined. The ECII shall provide a way for entities to estimate the consequence criteria in paragraph (2)(a) on their business process during the business impact assessments they perform pursuant

Article 35(4).

5. The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the Electricity Coordination Group on the proposals for the cybersecurity risk assessment methodologies that are developed pursuant to paragraph 1.

Article 18. Cybersecurity risk assessment cycle

The cybersecurity risk assessments at Union level, at regional level and at Member State level shall be performed every 3 years. The first risk assessment cycle shall start 24 months after entry into force of this Regulation.

TITLE III
RISK MANAGEMENT AT UNION AND AT REGIONAL LEVEL

Article 19. Union-wide cybersecurity risk assessment

1. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall perform a cybersecurity risk assessment at Union level using the methodologies at Article 17 to identify, analyse, and evaluate the possible consequences of cyber attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows.

2. The Union-wide risk assessment shall include the following elements:

   (a) the Union-wide high-impact and critical-impact processes; and

   (b) a risk impact matrix that entities and the NCCS-NCAs shall use to assess the cybersecurity risk identified in the Member State cybersecurity risk analysis and in the cybersecurity risk assessment at entity level.

3. For Union-wide high-impact and critical-impact processes, the cybersecurity risk assessment shall include:

   (a) an assessment of the possible consequences of a compromise to confidentiality, integrity, or/and availability of information used in the process using the metrics defined in the Union-wide cybersecurity risk assessment methodology; and

   (b) electricity cybersecurity impact indices and high-impact and critical-impact thresholds that the NCCS-NCAs can use to identify high-impact and critical-impact entities involved in the Union-wide high-impact and critical-impact processes.

4. Within 9 months after the start of each cybersecurity risk assessment cycle, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall submit a draft of the report at Article 22 on the results of the Union-wide cybersecurity risk assessment to ACER for opinion. ACER shall issue an opinion on the draft report within 3 months after its receipt. The ENTSO for Electricity and the EU DSO entity shall take utmost account of ACER's opinion when finalising the report.

5. Within 3 months after receipt of ACER's opinion, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall notify the final report at Article 22 to ACER, ENISA and the NCCS-

NCAs.

Article 20. Regional cybersecurity risk assessments

1. Within 30 months after the start of each risk assessment cycle, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall perform a cybersecurity risk assessment for each system operation region aggregating the Member State cybersecurity risk assessments in Article 32. The regional cybersecurity risk assessments shall identify, analyse, and evaluate the risks of cyber attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The regional cybersecurity risk assessments shall not consider the legal, financial or reputational damage of cyber attacks.

2. The regional cybersecurity risk assessments shall integrate the information from the cybersecurity risk assessments at Union level and at Member State level to provide a complete summary of the cybersecurity risks in the cross-border electricity cybersecurity risk assessment report at Article 22.

3. The regional cybersecurity risk assessment shall consider the regional electricity crisis scenarios related to cybersecurity identified pursuant to Article 6 of the Regulation (EU) 2019 /941.

Article 21. Regional cybersecurity risk treatment and acceptance

1. Within 30 months after the start of each risk assessment cycle, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop for each system operation region a cybersecurity risk treatment plan.

2. The regional cybersecurity risk treatment plans shall include:

   (a) the minimum and advanced cybersecurity controls that high-risk and critical risk entities shall apply in the system operation region; and

   (b) the residual cybersecurity risks in the system operation regions after applying the controls referred to in paragraph (a).

3. The ENTSO for Electricity shall submit the regional risk treatment plan to the relevant transmission system operators, the NCCS-NCAs as well as to the Electricity Coordination Group. The Electricity Coordination Group may recommend amendments.

4. The ENTSO for Electricity shall update the regional risk treatment plans at least after every cybersecurity risk assessment cycle, unless circumstances warrant more frequent updates.

Article 22. Cross-border electricity cybersecurity risk assessment report

1. Within 30 months after the start of each risk assessment cycle, the ENTSO for Electricity, in collaboration with the EU DSO entity, shall provide to the Electricity Coordination Group a report to assess cybersecurity risks with regard to cross-border electricity flows (the ‘Cross-Border Electricity Cybersecurity Risk Assessment Report’).

2. The report shall include at least the following information:

   (a) the list of Union-wide high-impact and critical-impact business processes identified in the

Union-wide cybersecurity risk assessment in accordance with Article 19, including for each process the estimate of the possible risk of a cyber attack on the process that was assumed during the regional cybersecurity risk assessments pursuant Article 20;

(b) current cyber threats, with a specific focus on emerging threats and risks for the electricity system;

(c) incidents for the previous period at Union level, providing a critical overview of how such incidents may have had an impact on electricity cross border flows;

(d) overall status of implementation of the cybersecurity measures;

(e) status of implementation of the information flows pursuant Article 40 and Article 41;

(f) list of information and/or specific criteria for classification of information pursuant to Article 49;

(g) identified and highlighted risks that may derive from insufficient supply chain management;

(h) results and accumulated experiences from mandatory regional and cross-regional cybersecurity exercises;

(i) an analysis of the development of the overall cross-border cybersecurity risks in the electricity sector since the last regional cybersecurity risk assessments;

(j) any other information that may be useful to identify a partial failure of this Regulation or the need for a revision of this Regulation or any of its tools; and

(k) the list of derogations pursuant to Article 25(4).

All entities listed in Article 2(1) at points (a), (b), (c), (d), (e), (f), (j), (k), (m) and (o), 2(3) and 2(4) shall contribute to the development of the report, respecting the confidentiality of information in accordance with Article 11.

The entities listed in Article 2(1) at points (h), (i), (l) and (n) may contribute to the development of the report. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall consult these entities from an early stage.

3. The report shall be subject to the rules on protection of exchange of information pursuant to Article 11.

4. Without prejudice to Article 11(4) and 12(5), ENTSO for Electricity and the EU DSO entity may release a sanitised public version of the report. The sanitised public version shall not contain the information that for the nature of their confidentiality may cause damages to entities in scope of this Regulation. Before the release of the sanitised public version, the NIS Cooperation Group shall provide its approval of the sanitised public version of the report. The ENTSO for Electricity in coordination with the EU DSO entity are responsible for the compilation and the release of the sanitised public version of the report.

5. Without prejudice to Article 11, ENISA may request from ENTSO for Electricity and the EU DSO entity information relevant for Article 15 (1) (a) Directive (EU) XX/YY [proposed Directive on measures for a high common level of cybersecurity across the Union; ('NIS 2 Directive')].

TITLE IV
COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

Article 23. Common electricity cybersecurity framework

1. Where reference is made to the common electricity cybersecurity framework in this Regulation, this shall be understood as referring to the following controls and the cybersecurity management system:

   (a) the minimum cybersecurity controls, developed in accordance with Article 24, that shall be applied by all high-impact and critical-impact entities inside the high-impact perimeter and by entities handling information pursuant to Article 49;

   (b) the advanced cybersecurity controls, developed in accordance with Article 24, that shall be applied by all critical-impact entities inside the critical-impact perimeter;

   (c) an electricity controls to standards mapping matrix ('ECSMM'), developed in accordance with Article 31, that maps the controls from (a) and (b) to selected European and international standards and national legislative or regulatory frameworks; and

   (d) the cybersecurity management system pursuant to Article 28.

2. Within 30 months of development of the common electricity cybersecurity framework in accordance with paragraph 1, the controls and cybersecurity management system at paragraph 1 shall be supplemented by the minimum and advanced cybersecurity supply chain security controls pursuant to Article 30.

3. Within 30 months after the start of each cybersecurity risk assessment cycle, the ENTSO for Electricity, in collaboration with the EU DSO entity, shall assess the need to review the controls and the cybersecurity management system at paragraph 1, and, when available, at paragraph 2, and in case this is considered necessary, shall develop a proposal for a revised version of the controls and the cybersecurity management system.

Article 24. Minimum and advanced cybersecurity controls

1. Within 30 months from the start of each cybersecurity risk assessment cycle, the ENTSO for Electricity, in collaboration with the EU DSO entity shall jointly develop a proposal for minimum and advanced cybersecurity controls.

2. The minimum and advanced cybersecurity controls shall be verifiable by an accredited conformity assessment body in accordance with the procedure set out in Article 26.

3. The minimum and advanced cybersecurity controls shall be based on the risks that are identified in the regional cybersecurity risk assessments pursuant to Article 20.

4. The minimum cybersecurity controls shall include controls to protect the information pursuant to Article 49.

5. Within 12 months after the adoption or update of the minimum and advanced cybersecurity controls, all entities listed in Article 2(1), 2(3) and 2(4) shall, during the establishment of the risk treatment plan pursuant to Article 35(5), apply the minimum cybersecurity controls within the high-

impact perimeter and advanced cybersecurity controls within the critical impact perimeter.

Article 25. Derogations from the minimum and advanced cybersecurity controls

1. The NCCS-NCA may provide derogations for any entity listed in Article 2(1) seated in their Member State from the minimum and advanced cybersecurity controls in the following cases:

   (a) in exceptional circumstances, when the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefit;

   (b) when the entity can provide a risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable according to the risk acceptance criteria pursuant to Article 35(3)(b).

3. Derogations from the minimum or advanced cybersecurity controls shall be granted for a maximum of three years, renewable. Before granting the derogation the NCCS-NCA shall decide whether a derogation is to be granted within 3 months after receipt of the request for a derogation.

4. The list of the derogations, including the information on which ground of paragraph 2 the derogation has been granted, shall be included as an annex to the Cross Border Electricity Cybersecurity Risk Assessment Report. The ENTSO for Electricity and the EU DSO entity shall jointly update the list, when necessary.

Article 26. Verification of the common electricity cybersecurity framework

1. No later than 24 months after publication of the common electricity cybersecurity framework each critical-impact entity, shall demonstrate its compliance with the management system and the minimum or advanced cybersecurity controls that are part of the common electricity cybersecurity framework.

2. The entity shall verify compliance by at least one of the following options:

   (a) being certified or audited by an independent conformity assessment body; or

   (b) being verified by a national verification scheme.

3. The verification of compliance shall cover all assets within the critical-impact perimeter of the entity.

4. The verification of compliance shall be regularly repeated at the latest every 36 months counting from the end of the first verification at paragraph 1.

5. The entity shall report on the outcome of the compliance verification to the competent NCCS-NCA.

Article 27. Cybersecurity supervision and enforcement

1. Member States shall ensure that NCCS-NCAs, when exercising their supervisory tasks in relation to high-impact and critical-impact entities, in particular regarding the obligations laid down in Articles 26, 28, 30, 32, 33, 35, 36, 41, 42, 43, 44 and 46, have the power to subject those entities to:

(a) on-site inspections and off-site supervision, including random checks;

(b) regular audits;

(c) targeted security audits based on risk assessments or risk-related available information;

(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;

(e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies;

(f) requests to access data, documents or any information necessary for the performance of their supervisory tasks; and

(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

2. Where exercising their powers under points (e) to (g) of paragraph 1, the NCCS-NCA shall inform the entity of the purpose of the request and specify the information requested.

3. Where exercising their powers under points (a) to (d) of paragraph 1, the NCCS-NCA shall inform the entity of the methods that are proposed to be uses for performing supervisory actions and shall state clearly the mutual liability obligations that will derive from the execution of such actions.

4. Where an entity is subject to supervisory tasks under points (a) to (d) of paragraph 1, and after the NCCS-NCA has fulfilled its obligation at paragraph 3, the concerned entity shall promptly inform the NCCS-NCA of any risk that such actions with the methods communicated at paragraph 3, will pose to cross-border electricity flows if implemented as proposed. The concerned entity, where possible, shall suggest non-binding corrections to the methods and the actions that would limit the risk for any disturbance to cross border electricity flows when the NCCS-NCA will exercise its supervisory role under this Regulation. The NCCS-NCA shall inform the concerned entity of the methods that are decided to be used for the concerned tasks, prior the start of the execution.

5. Member States shall ensure that NCCS-NCAs, where exercising their enforcement powers in relation to entities, have the power to:

(a) issue warnings on the entities' non-compliance with the obligations laid down in this Regulation;

(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Regulation;

(c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Regulation and desist from repeating that conduct;

(d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in this Regulation in a specified manner and within a specified period;

(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible

protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for in this Regulation.

Article 28. Cybersecurity management system

1. Within 24 months after being notified by the NCCS-NCA in accordance with Article 33, each high-impact and critical-impact entities shall establish a cybersecurity management system that is based on a European or international standard and requires entities to:

   (a) determine the scope of the management system considering interfaces and dependencies with other entities;

   (b) ensure that all senior management of the concerned entity is informed of regulatory and legal obligations and actively contributes to the implementation of the management system through timely decisions and prompt reactions;

   (c) ensure that the resources needed for the cybersecurity management system are available;

   (d) establish a cybersecurity policy that shall be documented and communicated within the entity and to parties affected by the security risks;

   (e) assign and communicate responsibilities for roles relevant to cybersecurity;

   (f) perform cybersecurity risk management as defined in Article 35;

   (g) determine and provide the resources required for implementation, maintenance and continual improvement of the management system; these shall consider the determination of the necessary competence and awareness of cybersecurity resources;

   (h) determine the need for internal and external communications relevant to cybersecurity;

   (i) create, update and control documented information related to the management system;

   (j) evaluate the cybersecurity performance and effectiveness of the cybersecurity management system;

   (k) conduct internal audits at planned intervals to ensure that the management system is effectively implemented and maintained;

   (l) obligations for top management to review the implementation of management system at planned intervals; and

   (m) control and correct non-conformity to the management system.

2. The scope of the cybersecurity management system shall include all assets within the high-impact and critical-impact perimeter of an entity.

3. The NCCS-NCAs shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and

specifications relevant to the security of network and information systems.

Article 29. Minimum and advanced cybersecurity supply chain security controls

1. Within the 30 months of development of the controls and the cybersecurity management system contained in the common electricity cybersecurity framework , the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a proposal for the minimum and advanced cybersecurity controls including minimum and advanced cybersecurity supply chain security controls that mitigate the supply chain risks identified in the regional cybersecurity risk assessments. The minimum and advanced cybersecurity supply chain security controls shall cover the entire lifecycle of all ICT products, ICT services and ICT processes inside the high-impact or critical-impact perimeters of an entity.

2. The minimum cybersecurity supply chain controls shall include controls for high-impact and critical-impact entities to:

   (a) include cybersecurity requirements in the procurement requirements for ICT products, ICT services, and ICT processes covering at least:

      (i) technical cybersecurity procurement requirements for the ICT product, ICT service or ICT process used, or to be used;

      (ii) background verification checks of the staff of the supplier involved in the supply chain and dealing with sensitive information or with access to the high-impact or critical-impact assets of the entity;

      (iii) processes for secure and controlled design, development and production of ICT products, ICT services and ICT processes, promoting cybersecurity-by-design and zero trust architectures;

      (iv) controls over the access of the supplier to the assets of the entity;

      (v) obligations of the supplier to protect and restrict access to the entity's sensitive information;

      (vi) propagation of cybersecurity procurement requirements to subcontractors of the supplier to ensure that the cybersecurity procurement requirements apply;

      (vii) traceability of the application of the cybersecurity procurement requirements from the development through production until delivery of ICT products, ICT services or ICT processes;

      (viii) support for security updates throughout the entire lifetime of ICT products, ICT services or ICT processes; and

      (ix) the right to audit design, development and production processes of the supplier.

   (b) only select and contract suppliers that can meet the cybersecurity procurement requirements as stated in paragraph (1) and that possess a level of cybersecurity appropriate to the cybersecurity risks of the ICT product, ICT service, or ICT processes that the supplier delivers;

(c) diversify sources of supply for ICT products, ICT services and ICT processes and limit vendor lock-in;

(d) include the cybersecurity procurement requirements as stated (1) in contracts with suppliers, collaboration partners and other parties in the supply chain, covering ordinary deliveries of ICT products, ICT services and ICT processes as well as unsolicited events and circumstances like termination and transition of contracts in cases of negligence of the contractual partner; and

(e) monitor, review or audit the cybersecurity procurement requirements for supplier processes throughout the entire lifecycle of each ICT service and ICT process on a regular basis.

3. For the cybersecurity procurement requirements in paragraph 2(a), entities may use the principles and recommendation in the cybersecurity procurement recommendation in accordance with Article 37, or may define their own requirements based on the results of the cybersecurity risk assessment at entity level.

4. The advanced cybersecurity supply chain security controls shall include controls for critical-impact entities to verify during procurement that ICT products, ICT services and ICT processes, that will be used as critical-impact assets, satisfy the cybersecurity procurement requirements. The ICT product, ICT service or ICT process shall be verified either through a European cybersecurity certification scheme pursuant to Article 38 or through verification activities selected and organized by the entity. The depth and coverage of the verification activities shall be sufficient to provide assurance that the ICT product, ICT service or ICT process can be used to mitigate the risks identified in the risk assessment at entity level. The critical-impact entity shall document the steps taken to reduce the risks identified.

5. The minimum and advanced cybersecurity supply chain security controls in this Article shall apply to ICT product, ICT services, and ICT processes for which the procurement requirements are defined 6 months or more after the finalisation of the minimum and advanced cybersecurity controls.

Article 30. Security measures for critical service providers

1. Critical service providers shall implement processes for secure design, development and production by:

(a) providing cybersecurity training to their staff;

(b) ensuring cybersecurity-by-design by considering cyber threats and security requirements; and

(c) verifying the cybersecurity of an ICT product, ICT service or ICT process through testing, reviews or audits.

2. Critical service providers shall implement vulnerability management, including:

(a) monitoring vulnerabilities in both internally and externally developed software and hardware, including open-source libraries;

(b) reporting vulnerabilities to their NCCS-NCA without undue delay;

(c) classifying and prioritizing the mitigation of vulnerabilities on objective criteria that reflect their risk to critical-impact processes; and

(d) providing mitigations for vulnerabilities classified as high-impact under paragraph (c) as soon as possible.

3. Critical service providers shall protect access they have to customer assets and to information that would lead to cybersecurity risks at customers if compromised by:

(a) performing background verification checks on the staff with access to the assets or to information;

(b) limiting access to the assets and information to those staff members that need the access to carry out their tasks;

(c) taking appropriate measures to protect, control and log remote access to customer assets; and

(d) notifying customers about cybersecurity incidents that may affect them.

4. Critical service providers shall apply the measures in paragraphs (1), (2), and (3) to all processes related to the ICT products, ICT services or ICT processes they provide that are needed for critical-impact processes. The critical service provider shall ensure that the implementation of the measures is appropriate to the cybersecurity risks.

Article 31. Electricity controls to standards mapping matrix

1. Within 30 months from the start of each cybersecurity risk assessment cycle, the ENTSO for Electricity, in collaboration with the EU DSO entity shall jointly develop a proposal for the ECSMM mapping the controls set out in TITLE IV(1)(a) and (b) to selected European and international standards as well as relevant technical specifications. The ENTSO for Electricity and the EU DSO entity shall track the conformity of the different controls with the controls set out in Article 23(1)(a) and (b).

2. The NCCS-NCAs may provide to the ENTSO for Electricity and the EU DSO entity a mapping of the controls set out in TITLE IV (1) (a) and (b) to the national legislative or regulatory frameworks, including relevant Member States' national standards pursuant to Article 22 of Directive (EU) XX/YY [proposed Directive on measures for a high common level of cybersecurity across the Union; ('NIS 2 Directive')]. If the NCCS-NCA of a Member State provide such a mapping, then the ENTSO for Electricity and the EU DSO shall integrate this national mapping into the ECSMM.

TITLE V
RISK ASSESSMENT AT MEMBER STATE LEVEL

Article 32. Member State cybersecurity risk assessment

1. Every cybersecurity risk assessment cycle, each NCCS-NCA shall perform a cybersecurity risk assessment on all high-impact and critical-impact entities in its Member State using the

methodology developed in accordance with Article 17. The Member State cybersecurity risk assessment shall identify and analyse the risks of cyber attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The Member State cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber attacks.

2. The cybersecurity risk assessment report should take into account the Member State's risk preparedness plan established pursuant to Article 10 of Regulation (EU) 2019/941.

3. Within 21 months after the start of the cybersecurity risk assessment cycle each NCCS-NCA supported by the CSIRT shall provide a Member State cybersecurity risk assessment report to the ENTSO for Electricity and the EU DSO entity, containing the following information for each high-impact and critical-impact business process:

   (a) the implementation status of the minimum and advanced cybersecurity controls;

   (b) recommended additional controls to reduce cybersecurity risks;

   (c) a list of all security incidents reported in the previous 3 years pursuant to Article 41(3);

   (d) a summary of the cyber threat information reported in the previous 3 years pursuant to Article 41(5);

   (e) for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity and availability; and

   (f) when necessary, a list of additional entities identified as high-impact or critical-impact pursuant to 33(1), (2), (3), and (5).

4. The information in the report shall not be linked to specific entities or assets. The estimate of the risk in point (e) shall be given as an estimate of the consequences and likelihood according to the risk-impact matrix.

5. The report shall also include a risk assessment of the temporary derogations issued by the NCCS-NCAs in the Member States pursuant to Article 25.

6. The ENTSO for Electricity and the EU DSO entity may request additional information from the NCCS-NCAs in relation to the tasks specified in paragraph 3(a), (b) and (c).

7. The NCCS-NCAs shall ensure that the information they provide is accurate, correct, and not older than 21 months.

Article 33. Identification of high-impact and critical-impact entities

1. The NCCS-NCAs shall identify the high-impact and critical-impact entities in its Member State. The NCCS-NCAs may request information from an entity in its Member State to determine the ECII values for the entity. If the determined ECII of an entity is above the high-impact or critical-impact threshold, the identified entity shall be listed in the cybersecurity risk assessment report.

2. The NCCS-NCA shall identify high-impact and critical-impact entities not established in the Union, unless these entities have already been identified under this paragraph and have designated

a representative in the Union in accordance with Articles 2(3) and 2(4). The NCCS-NCA may request information from an entity to determine the ECII values for the entity. If the determined ECII of an entity is above the high-impact or critical-impact threshold, the identified entity shall be listed in the cybersecurity risk assessment report.

3. The NCCS-NCAs may identify additional entities in its Member State as high-impact or critical-impact entities if the following two criteria are met:

   (a) the entity is part of a group of entities for which there is a significant risk that they will be affected simultaneously by a cyber attack; and

   (b) the ECII aggregated over the group of entities is above the high-impact or critical-impact threshold.

4. If the NCCS-NCA identifies additional entities in accordance with paragraph 3 of this article, all processes at these entities for which the ECII aggregated over the group are above the high-impact threshold shall be considered high-impact processes. All processes for which the aggregated ECII are above the critical-impact thresholds shall be considered critical impact processes.

5. Where NCCS-NCAs would identify entities described at paragraph 3(a) of this article, they shall inform NCCS-NCAs, the ENTSO for Electricity and the EU DSO entity. ENTSO for Electricity and the EU DSO Entity, based on the information received from all NCCS-NCAs, shall provide to NCCS-NCAs an analysis of the aggregation of entities in more than one Member State that can create a distributed disturbance to the cross border electricity flows, and therefore, can result in a cybersecurity incident. In case an aggregation of entities in multiple Member States is identified as an aggregation which ECII is above high-impact or critical impact threshold, all concerned NCCS-NCAs shall identify the entities in such aggregation as high-impact or critical-impact entities for their respective Member State, based on the aggregated ECII for the aggregation of the entities, and the identified entities shall be listed in the cybersecurity risk assessment report.

6. In each risk assessment cycle, the NCCS-NCA shall, within 9 months after being notified by ENTSO for Electricity and EU DSO entity of the cybersecurity risk assessment report, notify the entities on the list that they have been identified as a high-impact or critical-impact entity in its Member State.

7. When a service provider is reported to a NCCS-NCA as being a critical service provider pursuant Article 36 (1)(c), the NCCS-NCA shall notify it to the NCCS-NCAs of the Member States in whose territories the seat or representative in accordance with article 2(3) of the critical service provider is situated. The latter NCCS-NCAs shall notify the service provider that it has been identified as being a critical service provider.

Article 34. National verification schemes

1. The NCCS-NCA may establish a national scheme to verify that critical-impact entities have implemented the national legislative or regulatory framework that is included in the ECSMM. The national verification scheme may be based on inspection by the NCCS-NCA, or on peer reviews by critical-impact entities in the same Member State supervised by the NCCS-NCA.

2. If the NCCS-NCA decides to establish a national verification scheme, the NCCS-NCA shall ensure

that the verification is performed according to the following requirements:

(a) any party performing the peer review or inspection shall be independent from the critical-impact entity being verified, and shall have no conflicts of interest;

(b) The staff performing the peer review or inspection shall have demonstrable knowledge of:

(i) cybersecurity in the electricity sector;

(ii) cybersecurity management systems;

(iii) the principles of auditing;

(iv) cybersecurity risk assessment;

(v) the common electricity cybersecurity framework;

(vi) the national legislative or regulatory framework and European and international standards in scope of the verification; and

(vii) the critical-impact business processes in scope of the verification.

(c) The party performing the peer review or inspection shall be allowed sufficient time to perform these activities. The time allowed for the activities shall be comparable to the time required for the certification of the cybersecurity management system with comparable scope by a conformity assessment body. The calculation of overall peer review or inspection time shall include sufficient time for reporting;

(d) The party performing the peer review or inspection shall take measures to protect the confidential information they collect during the verification; and

(e) Peer reviews or inspections shall be performed at least once every year and cover the full verification scope at least every three years.

3. If the NCCS-NCA decide to establish a national verification scheme, the NCCS-NCA shall report to ACER on an annual basis how frequently they have performed inspections under the scheme.

TITLE VI
RISK MANAGEMENT AT ENTITY LEVEL

Article 35. Cybersecurity risk management at entity-level

1. Each high-impact and critical-impact entity as identified by the NCCS-NCA shall perform a cybersecurity risk management for all its assets in its high-impact and critical-impact perimeters. Each high-impact and critical-impact entity shall perform a risk management cycle covering the phases in paragraph (2) at least every 3 (three) years.

2. Each high-impact and critical-impact entity shall use a cybersecurity risk management approach that applies the following phases:

(a) context establishment;

(b) cybersecurity risk assessment;

(c) risk treatment; and

(d) risk acceptance.

3. During the context establishment phase, each high-impact and critical-impact entity shall:

(a) define the scope of the cybersecurity risk assessment including at least the high-impact and critical-impact processes identified by the ENTSO for Electricity and the EU DSO entity, and other processes that may cause incidents with a high-impact or critical- impact on cross-border electricity flows if compromised by a cyber attack; and

(b) define criteria for risk evaluation and for risk acceptance in accordance with the risk impact matrix defined by the ENTSO for Electricity and the EU DSO entity.

4. During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

(a) identify risks by taking into account:

(i) all assets supporting the Union-wide high-impact and critical-impact processes with an assessment of the possible impact on cross-border electricity flows if the asset is compromised;

(ii) possible cyber threats taking into account the cyber threats identified in the latest Cross-Border Electricity Cybersecurity Risk Assessment Report and supply chain threats;

(iii) vulnerabilities including vulnerabilities in legacy systems;

(iv) possible cybersecurity incident scenarios, including cyber attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows; and

(v) existing implemented controls.

(b) analyse the likelihood and consequences of the cybersecurity risks identified in (a) and determine the cybersecurity risk level using the risk impact matrix;

(c) classify assets according to the possible consequences of a compromise and determine the high-impact and critical-impact perimeter using the following steps:

(i) for all processes in scope of the risk assessment perform a business impact assessment using the electricity cybersecurity impact indexes (ECII);

(ii) classify a process as high-impact or critical-impact if its ECII is above the high-impact or critical-impact threshold respectively;

(iii) determine all high-impact and critical-impact assets as the assets needed for the high-impact and critical-impact processes respectively;

(iv) define high-impact and critical-impact perimeters containing all high-impact and critical-impact assets respectively, and so that access to the assets can be controlled on the perimeters; and

(d) evaluate risks by prioritizing the cybersecurity risks against risk evaluation criteria and risk

acceptance criteria as defined in paragraph (3)(b).

5. During the risk treatment phase, each high-impact and critical-impact entity shall establish a risk treatment plan by selecting risk treatment options appropriate to manage the risks and identify the residual risks after treatment.

6. During the risk acceptance phase, each high-impact and critical-impact entity shall decide whether to accept the residual risk based on the risk acceptance criteria established in paragraph (3)(b).

7. Each high-impact and critical-impact entity shall register the assets identified in paragraph (1) and (2) in an asset inventory that includes all interfaces with the environment in which the entity operates. The asset inventory shall not be part of the risk assessment report.

8. The NCCS-NCA may inspect the asset inventory during on-site inspections pursuant Article 27.

Article 36. Reporting on the risk assessment at entity level

1. Each high-impact and critical-impact entity shall, within 12 months after the start of each cybersecurity risk assessment cycle, provide to the NCCS-NCA the following information:

   (a) a list of controls selected for risk treatment pursuant to Article 35(5) with the current implementation status of each control;

   (b) for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity, and availability; and

   (c) a list of critical service providers for the their critical-impact processes.

   The controls in (a) shall not be linked to specific assets in the report. The estimate of the risk in (b) shall be given as an estimate of the consequences and likelihood according to the risk impact matrix at Article 17(2).

2. The NCCS-NCA may request additional information from the high-impact and critical-impact entity.

3. The entity shall ensure that the information it provides is accurate, correct and from the current cybersecurity risk assessment cycle.

TITLE VII
CYBERSCURITY PROCUREMENT RECOMMENDATIONS

Article 37. Cybersecurity procurement recommendations

1. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall set up a rolling work programme to develop sets of cybersecurity procurement recommendations that high-impact and critical-impact entities may use as a basis for the procurement of ICT products, ICT services and ICT processes in the high-impact and critical-impact perimeters. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall provide ACER at the end of each risk assessment cycle with a programme description containing:

(a) a reference architecture to describe and classify the types of ICT products, ICT services and ICT processes used by high-impact and critical-impact entities in the high-impact and critical-impact perimeter; and

(b) a list of the types of ICT products, ICT services, and ICT processes for which sets of cybersecurity recommendations shall be developed in the next risk assessment cycle, based on the priorities of high-impact and critical-impact entities.

2. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall select the types of ICT products, ICT services, and ICT processes for which sets of cybersecurity procurement recommendations are developed based on the priorities of high-impact and critical-impact entities.

3. The sets of cybersecurity recommendations shall be based on the outcomes of the cybersecurity risk assessment at regional level. Each system operation region shall have a set of requirements that should be similar and/or comparable to the set of requirements in other system operation regions. The sets shall cover at least the requirements in Article 29(2)(a). Where possible, the requirements shall be selected from European and international standards.

4. The ENTSO for Electricity and the EU DSO entity shall ensure that the sets of cybersecurity procurement recommendations comply with the principles of procurement pursuant to Directive (EC) 2014/24. The ENTSO for Electricity and the EU DSO entity shall ensure that the sets of cybersecurity procurement recommendations are compatible with the available European cybersecurity certification schemes relevant to the ICT product, ICT service, or ICT process. In particular, they shall ensure that the applicable security objectives in Article 51 of Regulation (EU) 2019/881 are met by the ICT products, ICT services and ICT processes to be procured.

5. The ENTSO for Electricity, in collaboration with the EU DSO entity, shall publicly consult the proposal for the sets of cybersecurity procurement recommendations pursuant to Article 9 of this Regulation.

Article 38. Guidance on European cybersecurity certification schemes for ICT products, ICT services and ICT processes

1. Without prejudice to the framework for the establishment of European cybersecurity certification schemes pursuant to Article 46 of Regulation (EU) 2019/881, the ENTSO for Electricity and the EU DSO entity may provide sector-specific guidance on the use of European cybersecurity certification schemes, whenever a suitable scheme is available for a type of ICT product, ICT service or ICT process used by critical-impact entities. This sector-specific guidance may include profiles with additional testing requirements and rules for determining the exploitability of vulnerabilities.

2. If a suitable European certification scheme is not available, the ENTSO for Electricity, in cooperation with the EU DSO entity, may develop sector-specific guidance on the application of an existing European cybersecurity certification scheme for a certain type of ICT product, ICT service or ICT process.

3. The ENTSO for Electricity and the EU DSO entity shall closely cooperate with ENISA when developing the guidance in accordance with paragraph (1). The ENTSO for Electricity in

cooperation with the EU DSO entity shall consult the main stakeholders on the guidance in accordance with Article 9. The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by all involved stakeholders before finalising the guidance.

TITLE VIII
INFORMATION FLOWS, CYBERSECURITY INCIDENT AND CRISIS MANAGEMENT

Article 39. Scope of TITLE VIII

Without prejudice to Directive (EU) 2016/1148, Title VIII sets out requirements for cross-border information flows, cybersecurity incidents and crisis management. For the information flows, cybersecurity incident and crisis management at national level, the national implementation of the Directive (EU) 2016/1148 applies.

Article 40. Role of public authorities concerning information sharing

1. In the event of a cybersecurity incident notification received from a high-impact or critical impact entity pursuant to Article 41(3), the NCCS-NCA shall:

   (a) assess the level of confidentiality classification of the information received from the entity, inform the entity about the outcome of its assessment without undue delay but within twenty-four (24) hours of receipt of the information;

   (b) be responsible for proactively verifying and finding any other similar cybersecurity incident in the Union reported to other NCCS-NCAs, to correlate information provided in the context of the cybersecurity incident from other cybersecurity incidents in order to eventually enrich existing information, strengthen and coordinate cybersecurity responses;

   (c) be responsible for the sanitisation and the anonymization of the relevant information;

   (d) share information with the national single points of contact through the competent national CSIRT without undue delay but no later than twenty-four (24) hours after the reception of a reportable cybersecurity incident and provide updated information on a regular basis to the NCCS-NCAs; and

   (e) disseminate reportable cybersecurity incident information received from the national single points of contact to critical-impact and high-impact entities in its Member State without undue delay but no later than twenty-four (24) hours after the determination of relevant technical information allowing the entities to organize effectively their cybersecurity defence;

   (f) NCCS-NCA may request the reporting high-impact or critical impact entity to further disseminate the reportable sanitized cybersecurity incident via operational secured electricity platforms to other entities that may be affected, with the aim to generate situational awareness by the electricity sector and to prevent the materialization of a risk that may escalate in a cross border cybersecurity electricity incident would be categorised under level 4 or 5. In

order to do so, the NCCS-NCA competent for the high-impact or critical impact entity and the entity, may establish a formal binding agreement.

2. The NCCS-NCA receiving the information from the high-impact and/or the critical-impact entity and the NCCS-NCAs receiving the information through the national single point of contact shall not disseminate information towards other critical-impact and/or high-impact entities and shall withhold it as long as the information constitutes a high risk and could harm, hinder or disrupt the investigation of an ongoing cyber attack, or for any other national security consideration.

3. In the event of zero day vulnerability is disclosed by a high-impact or critical impact entity pursuant to Article 41(4), the NCCS-NCA shall:

   (a) Share available information with the vendor and request the vendor, where possible, to identify a list of NCCS-NCAs that may be impacted by the zero day vulnerability and shall be informed;

   (b) share available information with all other NCCS-NCAs identified at the previous point, based on need-to-know principle;

   (c) share also, where they exist, mitigation strategies and measures to the reported zero day vulnerability;

   (d) share the information in line with the provisions of the policy to promote and facilitate coordinated vulnerability disclosure established pursuant to article 5(2)(c) of [NIS2D] of the Member State where the zero day vulnerability has been reported, with the aim to prevent that a cybersecurity incident would materialize because of non-disclosed zero day vulnerability with the relevant stakeholders; and

   (e) support, with ENISA's guidance, the concerned entity to receive from the vendor an effective, coordinated and rapid management of the zero day vulnerability or of effective and efficient mitigation measures.

4. In the event of cyber threats received from a high-impact or critical-impact entity pursuant to Article 41(5), the NCCS-NCA shall disseminate to the national single points of contact and to the entities in its Member State without undue delay information on cyber threats or any other information of importance for preventing, detecting, responding to or mitigating the risk.

5. NCCS-NCAs may delegate fully or partly responsibilities under paragraph 1, 2, 3 and 4 concerning one or more specific entities that operate in more than one Member State, to another NCCS-NCA in one of those Member States, following an agreement among the concerned NCCS-NCAs.

6. The ENTSO for Electricity, in cooperation with the EU DSO entity and with the support of ENISA and CSIRTs network, shall develop a cybersecurity incidents classification scale methodology within twelve (12) months after the entry into force of this Regulation.

   The methodology shall:

   (a) provide the classification for the gravity of a cybersecurity incident according to 5 levels, the two highest level being 'high' and 'critical';

(b) the classification shall be based on the assessment of the following parameters:

(i) the classification of the asset exposed determined according to Article 35(4)(c); and

(ii) the severity, the depth and the surface of the cyber attack.

7. Within two (2) years after entry into force of this Regulation, the ENTSO for Electricity, in collaboration with the EU DSO entity, shall perform a feasibility study to assess the possibility and the financial needs to develop a common tool for all entities with automatic connections to the relevant authorities tools.

The feasibility study that shall take into account the following:

(a) such a tool would support critical-impact and high-impact entities with relevant security related information for operations of cross-border electricity flows, such as near real-time reporting of cybersecurity incidents, early warnings related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system;

(b) such a tool would be maintained through a suitable and highly trustable environment. National and international information sharing networks shall be protected using state of the art best practice techniques and standards; and

(c) such a tool would allow for data collection from critical-impact and high-impact entities and facilitate sanitisation and anonymization of the data and its prompt dissemination to critical impact and high impact entities.

8. The ENTSO for Electricity, in cooperation with the EU DSO entity, may:

(a) analyse and facilitate initiatives proposed by entities to test such tools;

(b) consult ENISA, the national single points of contact and the representatives of main stakeholders when assessing the feasibility; and

(c) present the results of the feasibility study to ACER.

Article 41. Role of high-impact and critical-impact entities regarding information sharing

1. Each high-impact and critical-impact entity shall:

(a) establish at least the following CSOC capabilities for all systems within the cybersecurity perimeter of the entity pursuant to Article 35(4)(c):

(i) ensuring that relevant systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on cybersecurity incidents;

(ii) conducting security monitoring, including but not limited to detecting intrusions and assessing vulnerabilities of network and information systems within the cybersecurity perimeter of the entity pursuant to Article 35(4)(c);

(iii) analysing and, if necessary, taking all actions required under its responsibility and capacity to protect the entity; and

(iv) participating in the information collection and sharing described in this Article.

(b) without prejudice to paragraph 1(a), have the right to procure all or parts of the CSOC capabilities pursuant to paragraph 1(a) through MSSP; and

(c) designate a single point of contact for the purpose of information sharing with any external entity.

2. ENISA shall provide the entities with non-binding guidance on establishing CSOC capabilities or engaging with MSSPs.

3. Each critical-impact entity and each high-impact entity shall share any information related to a reportable cybersecurity incident with its NCCS-NCA without undue delay but no later than four (4) hours after its determination.

A cybersecurity incident shall be considered reportable when the cybersecurity incident is:

(a) sufficiently scoped by the affected entity to determine the cybersecurity incident classification ranging from "high" to "critical" following the cybersecurity incident classification scale methodology pursuant to Article 40(6); and

(b) the cybersecurity incident classification is confirmed by the authorised representative of the entity.

4. Each critical-impact entity and each high-impact entity shall share any information related to zero day vulnerabilities not publicly known to its NCCS-NCA, without undue delay but not later than twenty-four (24) hours after its determination by the authorised representative of the entity.

5. Each critical-impact entity and each high-impact entity shall share without undue delay to its NCCS-NCA any information related to a cyber threat that may have a cross-border effect if the following cybersecurity information is collected in the entity's own environment notwithstanding the success of the cyber attack.

Information concerning a cyber threat shall be considered reportable when:

(a) it provides any relevant information for preventing, detecting, responding or mitigating the impact or risk concerning cybersecurity risks; or

(b) the identified artefacts used in the context of an attack lead to information such as compromised URL or IP addresses, hashes or any other attribute useful to contextualize and correlate the attack.

A cyber threat can be further assessed and contextualised with additional information provided by service providers or third parties not subject to this Regulation.

6. Each critical-impact entity and high-impact entity shall, when reporting information pursuant to this Article, specify:

(a) that the information is submitted pursuant to this Regulation;

(b) whether the information concerns:

(i) a reportable cybersecurity incident referred to in paragraph 3;

(ii) zero day vulnerabilities not publicly known referred to in paragraph 4; or

(iii) a cyber-threat referred to in paragraph 5.

(c) in the case of a reportable cybersecurity incident, the level of the cybersecurity incident according to the incident classification scale methodology of the ENTSO for Electricity at Article 40(6) and information leading to this classification including at least the criticality of the cybersecurity incident.

7. The reporting of the information required under Article 14(3) of Directive (EU) 2016/1148 constitutes reporting of information compliant with paragraph 6 when it also includes the information listed in paragraph 6 from (a) to (c).

8. Each critical-impact entity and high-impact entity shall alert its NCCS-NCA by clearly identifying specific information that shall only be shared with the NCCS-NCA in cases where the information sharing could be source of a cyber attack or a cyber incident. Entities shall have the right to provide a sanitised version of the information to the CSIRT.

Article 42. Detection of cybersecurity incidents and handling of cybersecurity incident related information

1. Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cybersecurity incidents with the necessary support from the NCCS-NCA, the CSIRTs network, the ENTSO for Electricity, the EU DSO entity and ENISA.

2. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cybersecurity incidents that will or may affect cross-border electricity flows in order to minimize the impact of a cybersecurity incident and cyber attack and to react rapidly on those flows.

3. In case that a cybersecurity incident has an effect on cross-border electricity flows, the CSOCs or MSSPs of affected critical-impact and high-impact entities shall join their efforts to share information coordinated by the NCCS-NCA of the Member State in which the cybersecurity incident was reported the first time. Critical-impact and high-impact entities shall supervise the joint efforts of the CSOCs or MSSPs, for which they remain those being the final responsible.

4. Critical-impact and high-impact entities are responsible for and shall:

(a) report reportable cybersecurity incidents pursuant to Article 41(3);

(b) ensure that their own CSOC or MSSP have access to the information provided by the national single point of contact through their NCCS-NCA on a need-to-know basis, as well as notifying the NCCS-NCA and the national single point of contact with a list of the CSOCs or MSSPs from which the NCCS-NCA and national single points of contact may expect to receive reportable cybersecurity incidents and to which NCCS-NCA and national single points of contact may have the need to provide information;

(c) establish incident management procedures for cybersecurity incidents, including roles and responsibilities, tasks and reactions based on the observable evolution of the cybersecurity

incident within the critical-impact and high-impact entity and in the nearby cybersecurity perimeters; and

(d) test the overall incident response procedures at least every year by testing at least one scenario affecting directly or indirectly cross-border electricity flows. This annual test may be conducted by critical-impact and high-impact entities during the regular exercises according to Article 46. Any live cybersecurity incident response activities with a consequence classified at least Scale 2 according to the incident classification scale methodology of ENTSO for Electricity at Article 40(6) with a cybersecurity root cause, can serve as an annual test of the cybersecurity incident response plan.

5. Where deemed necessary, the tasks at Paragraph 1 may be delegated by the Member States also to the Regional Coordination Centers after following the process indicated at Article 37(2) of Regulation (EU) 2019/943.

Article 43. Crisis management

1. Unless otherwise defined by the Member State, the responsibility for crisis management in the event of a cybersecurity incident impacting the cross-border electricity flows rests with the NCCS-NCA.

2. The critical-impact or high-impact entity impacted by a regional electricity crisis shall investigate in cooperation with its NCCS-NCA the root cause of the crisis to determine whether the crisis is caused by a cybersecurity incident.

3. When a cybersecurity cross-border electricity crisis is declared by the NCCS-NCA, the NCCS-NCA from the affected Member States shall jointly create an ad hoc cybersecurity crisis coordination group. The ad hoc cybersecurity crisis coordination group shall:

(a) coordinate the efficient retrieval and further dissemination of all relevant cybersecurity information to the entities involved in the crisis management process;

(b) organize the communication between all the stakeholders impacted by the crisis including the entities pursuant to paragraph 4 and the NCCS-NCAs, in order to reduce overlaps and increase the efficiency in the analyses and technical responses to remedy the cybersecurity cross-border crisis; and

(c) provide the expertise required to the entities impacted by the cybersecurity cross-border crisis.

4. Unless otherwise defined by the Member State pursuant to paragraph 1, NCCS-NCA shall define the participants in the crisis management process on a Member State level, such as entities.

5. Critical-impact and high-impact entities shall develop and have available capabilities, internal guidelines, preparedness plans, and staff to take part in the detection and mitigation of cybersecurity cross-border crisis, with the support of its RP-NCA, NCCS-NCA, the CSIRT Network and ENISA shall provide the necessary support to these entities in order to actively manage the crisis.

6. Where deemed necessary, the tasks at Paragraph 5 may be delegated by the Member States also to the Regional Coordination Centres after following the process indicated in Art. 37(2) of Regulation (EU) 2019/943.

Article 44. Crisis management plans and business continuity

1. ACER shall develop a Union-level cybersecurity crisis management plan for the electricity sector. ACER shall closely cooperate with ENISA, with the ENTSO for Electricity, the EU DSO entity, NCCS-NCAs, RP-NCAs and the NRAs when developing the plan.

2. Each RP-NCA shall develop a national cybersecurity crisis management plan for the electricity sector taking into account the Union-level cybersecurity crisis management plan and taking into account the national risk preparedness plan established according to Article 10 of Regulation (EU) 2019/941. The RP-NCA shall coordinate with the critical impact and high impact entities, the NCCS-NCA in its Member State.

2(a) Where deemed necessary, the tasks at Paragraph 1 and 2 may be delegated by the Member States also to the Regional Coordination Centres after following the process indicated in Art. 37(2) of Regulation (EU) 2019/943.

3. Critical impact and high impact electricity entities shall assure that:

   (a) cross-border cybersecurity incident handling procedures are incorporated in their crisis management plans; and

   (b) their cybersecurity-related crisis management processes are part of the general crisis management activities and compatible with incident handling processes.

4. Critical impact and high impact entities shall develop a crisis management plan for a cybersecurity-related crisis which is incorporated into their general crisis management plans and which shall include at least the following:

   (a) rules of declaration of the crisis as described in Article 14(2) and (3) of the Regulation (EU) 2019/941;

   (b) clear roles and responsibilities for crisis management, including the role of other relevant critical impact and high impact electricity entities; and

   (c) up-to-date contact information as well as rules for communication and information sharing during a crisis situation including the connection to the CSIRT.

   The crisis management plans shall be tested during the cybersecurity exercises as described in Articles 46 and 47.

5. The critical-impact and high-impact entities shall incorporate their crisis management plans into their business continuity plans for the critical processes. The crisis management plans at entity level shall include:

   (a) processes depending on availability, integrity and reliability of IT services;

   (b) all business continuity locations including the locations for hardware and software; and

   (c) all internal roles and responsibilities connected to business continuity processes.

The critical-impact and high-impact entities shall update their crisis management plans at least every three years and whenever necessary.

6. The critical-impact and high-impact entities shall test their business continuity plans at least once every 3 years or after major changes in a critical business process. The outcome of the business continuity plan tests shall be documented. The critical impact and high impact entities may include the test of their business continuity plan in the cybersecurity exercises.

   The critical-impact and high-impact entities shall update their business continuity plan whenever necessary and at least once every 3 years taking into account the outcome of the test.

   In case a test identifies deficiencies in the business continuity plan, the critical impact and high impact entity shall correct those deficiencies within 180 calendar days after the testing and shall conduct a new test to provide evidence that the corrective measures are effective.

   In case a critical-impact or high-impact entity cannot correct the deficiencies within 180 calendar days, it shall report the reasons to its NCCS-NCA in accordance with Article 36.

Article 45. Cybersecurity early warning capabilities for the electricity sector

1. ENISA shall facilitate the Electricity Cybersecurity Early Warning Capabilities (ECEWC). ENISA shall ensure the ECEWC is operable within 3 years after the entry into force of this Regulation. ENISA shall cooperate closely with the NCCS-NCA and relevant research institutions.

2. ENISA shall:

   (a) collect voluntary shared information from:

      (i) CSIRTs network, NCCS-NCAs;

      (ii) the entities listed in Article 2 (1), 2(3) and 2(4); and

      (iii) any other entity that wants to share relevant information on a voluntary basis.

   (b) assess and classify collected information;

   (c) scan the information ENISA has access to for identifying cyber risk conditions and relevant indicators for aspects of cross-border electricity flows;

   (d) identify conditions and indicators that frequently correlate with larger cyber attacks within the electricity sector;

   (e) define whether further analysis and preventive actions shall be taken through assessment and identification of risk factors;

   (f) inform the NCCS-NCAs on the identified risks and recommended preventive actions specific to the entities concerned;

   (g) inform all entities listed in Article 2(1), 2(3) and 2(4) on the results of the information assessed pursuant to paragraphs 2(b), (c) and (d);

   (h) periodically develop a situational awareness report; and

(i) derive applicable indicators of compromise from the collected information, where possible.

3. The CSIRT network member shall disseminate the information received from ENISA to the entities without undue delay of receipt of the information.

4. ACER shall monitor the effectiveness of ECEWC. ENISA shall assist ACER by providing all necessary information. The analysis shall be part of the monitoring pursuant to Article 12.

TITLE IX
ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

Article 46. Cybersecurity exercises at entity and Member State level

1. In [year of publication +3] and every three years afterwards, each critical impact entity shall organise and perform a cybersecurity exercise at entity level including one or more scenarios with cybersecurity incidents affecting directly or indirectly cross-border electricity flows.

2. The cybersecurity exercises at entity level and at Member State level shall be consistent with the national cybersecurity strategy pursuant to Article 5 of Directive (EU) XX/YY [proposed Directive on measures for a high common level of cybersecurity across the Union; ('NIS 2 Directive').

3. By derogation from paragraph 1, the RP-NCA after taking advice from NCCS-NCA may decide to organize in a cybersecurity exercise at national level instead of performing the cybersecurity exercise at entity level. In this regard, the NCCS-NCA shall inform:

   (a) all critical-impact entities of its Member State, the NRA, CSIRT and the CS-NCA at the latest by 30 June of the year preceding the cybersecurity exercise at entity level; and

   (b) each entity that shall participate in the national exercise 6 months before the exercise takes place.

   The RP-NCA with the technical support of CSIRT, shall organise this national exercise alone, with or under another national cybersecurity exercise. In order to be able to group these exercises, the RP-NCA shall have the authority to deviate from the year referred in paragraph 1, for up to one year.

4. By 31 December [year of publication +1] and every three years afterwards, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall make available an exercise scenario template to perform the exercise, built on the most recent risk assessment results performed, for each of the exercises referred to in paragraph 1 and 2, including among other key success criteria. The ENTSO for Electricity and the EU DSO entity shall involve ACER and ENISA in the development of the template and the methodology.

Article 47. Regional or cross regional cybersecurity exercises

1. In [year of publication +4] and every three years afterwards, in each system operation region, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall organise a cybersecurity

exercise. The critical-impact entities in the system operation region shall participate in the cybersecurity exercise. The ENTSO for Electricity may decide to organise cross regional cybersecurity exercises instead of one exercise per system operation region.

2. ENISA shall support the ENTSO for Electricity and the EU DSO entity in the preparation and organisation of the cybersecurity exercise at regional or at cross-regional level.

3. The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the entities that shall participate in the exercise 6 months before the exercise takes place.

4. The organiser of a regular cybersecurity exercise at Union level according to Article 7(5) of Regulation (EU) 2019/881 or of any mandatory cybersecurity exercise related to electricity sector within the same geographic perimeter, may invite the ENTSO for Electricity and the EU DSO entity to participate. In such cases, obligations under paragraph 1 are derogated, under the condition that all critical-impact entities in the system operation region take part in the same exercise.

5. If the ENTSO for Electricity and the EU DSO entity participate to the exercise in paragraph 4, they can deviate from the usual exercise rhythm pursuant to paragraph 1, for up to one year concerning regional or cross-regional cybersecurity exercises.

6. By 31 December [year of publication +2] and every three years afterwards, the ENTSO for Electricity, with the support of EU DSO entity, shall make available an exercise template to perform the exercise, built on the most recent risk assessment results, and including among others key success criteria. The ENTSO for Electricity shall involve the Commission and may seek advice from ACER, ENISA and the Joint Research Centre on the organisation and execution of the exercise.

Article 48. Internal, national, regional or cross-regional cybersecurity exercises

1. Upon request from a critical-impact entity, critical service providers providing services for the critical-impact entity in the area corresponding with the scope of the exercise, shall participate in the exercises referred in Article 46(1), Article 46(3) and Article 47(1).

2. The cybersecurity exercises organisers, with the advice of ENISA if requested by the organiser, shall analyse and finalize the exercise through a lessons-learnt report addressed to all participants. The lessons-learnt report shall include at least:

   (a) the exercise scenarios, meeting reports, main positions, successes and lessons learnt at any level of the electricity value chain;

   (b) the evaluation of whether the key success criteria were met; and

   (c) a list of recommendations for entities participating in the exercise to correct, adapt or change cybersecurity crisis processes, procedures, associated governance models, and potentially, contractual engagements with critical service providers.

   (d) The cybersecurity exercise organisers shall, when asked, share relevant output from the exercise with the NIS Cooperation Group to help meet the requirements of [Article 12 of NIS2D].

The organiser shall share with each participant information pursuant to paragraphs 2(a) and (b). The organiser shall share the list of recommendations pursuant paragraph 2(c) exclusively with the affected entity addressed.

3. The cybersecurity exercise organiser defined in Article 46 and Article 47 shall follow-up regularly with the entities participating in the exercises on the implementation of the recommendations pursuant to paragraph 2(c).

TITLE X
PROTECTION OF INFORMATION

Article 49. Principles for the protection of information exchanged for the purposes this Regulation

1. The entities in scope at Article 2(1), 2(3) and 2(4) shall ensure that information provided, received, exchanged or transmitted under this Regulation is accessible only on a need-to-know basis (when the information can be shared with someone that need to obtain the information to fulfil a requirement).

2. The entities in scope at Article 2(1), 2(3) and 2(4) shall ensure that information are inventoried and tracked during the entire life-cycle of the information, and may be released at the end of their life-cycle only after being anonymised.

3. The entities in scope at Article 2(1), 2(3) and 2(4) shall ensure that all necessary organisational and technical measures are in place to safeguard and protect and confidentiality, integrity, availability and non-repudiation of information provided, received, exchanged or transmitted in the implementation of this Regulation, independently from the means used. The protection measures shall respect principles at paragraphs 3 and 4. Organisational and technical measures and shall be proportional and shall take into consideration risks related to know past and emerging threats to which those information may be subject in the context of the entity and in the context of this Regulation. The security measures implemented by technical or/and organisational means to mitigate such risks to the information shall, at the extent possible, be based on National, European or international standards and best practices, and shall be documented.

4. The entities in scope at Article 2(1), 2(3) and 2(4) shall ensure that any individual who is granted access to information provided, received, exchanged or transmitted under this Regulation is briefed on the entity level applicable security rules, measures and procedures relevant to the protection of information and that the concerned person acknowledges the responsibility to protect the information as instructed during the briefing.

5. The entities in scope at Article 2(1), 2(3) and 2(4) shall ensure that access to information provided or exchanged under this Regulation is limited to individuals:
   (a) who are authorised to access that information based on their functions and limited to the execution of the tasks assigned; and

(b) for whom the entity was able to assess ethical and integrity principles, as well as for whom the party was able to perform a background verification check with a positive outcome to evaluate reliability of the individual in accordance with the entity' best practices and standard security requirements, or, where necessary, with the national laws and regulations.

6. The entities in scope at Article 2(1), 2(3) and 2(4) shall ensure that when providing information to a third party not in scope, for operational reasons, the concerned entity would have the written prior consent of the originating entity. Where the entity thinks that the information shall be shared beyond the need-to-share principle in order to prevent a cross-border electricity flows crisis or to any cross-border crisis within the EU in another sector, the sharing entity shall consult the competent NCCS-NCA, and if authorised, anonymise such information so that the information would not lose the elements necessary to inform the public of an imminent and serious risk to cross border electricity flows and possible mitigations, as well as safeguarding the identity of the originator and of the entities that have been processing the concerned information within this Regulation.

7. By derogation to paragraph 8, the NCCS-NCAs are authorised to provide information to a third party not in scope, for operational reasons, without a written prior consent of the originating entity but informing the originating entity at the earliest time possible, without undue delay. Before disclosing any information under this Regulation to a third party not in scope, the concerned NCCS-NCA shall ensure that the third party not in scope is aware of the security rules in force and shall ensure that the third party not in scope can protect the received information in accordance respecting all obligations at paragraphs (3), (4), (5), (6), (7).The NCCS-NCA shall anonymise such information so that the information would not lose the elements necessary to inform the public of an imminent and serious risk to cross border electricity flows and possible mitigations, as well as safeguarding the identity of the originator and of the entities that have been processing the concerned information within this Regulation. In this case, the third party not in scope shall protect the received information in accordance with provisions already in force at the entity level, or where this is not possible, with provisions and instructions provided by the NCCS-NCA.

8. Where the entity needs an information to be shared in order to prevent a cross-border electricity flows crisis or to any cross-border crisis within the EU in another sector, the sharing entity shall anonymise such information so that the information would not lose the elements necessary to inform the public of an imminent and serious risk of a cross-border electricity flows crisis or to any cross-border crisis within the EU in another sector, and of the possible mitigation measures or strategies, as well as safeguarding the identity of the originator and of the entities that have been processing the concerned information within the objectives of this Regulation.

9. Provisions in this article shall be in place prior an entity in scope at Article 2(1), 2(3) and 2(4) would be able to provide, receive, exchange or transmit any information.

10. Provisions in this article are not applicable to entities not in scope that are provided with information pursuant paragraph 9 of this article. In this case provisions at paragraph 13 shall be applied, or the NCCS-NCA may opt to provide the entity with written provisions to apply in case information are received pursuant to this Regulation.

11. All entities exchanging information pursuant TITLE VIII of this Regulation, shall ensure as a minimum that all information exchanged are protected in line with the principles for information protection as from the [NIS2D], where no other framework can be applied.

TITLE XI FINAL PROVISIONS

Article 50. Transitional provisions

1. Within 2 months after entry into force of this Regulation, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a transitional electricity cybersecurity impact index (ECII). The ENTSO for Electricity shall notify the transitional electricity cybersecurity impact index to the NCCS-NCAs.

2. Within 4 months of receipt of the transitional electricity cybersecurity impact index the NCCS-NCAs shall identify high-impact and critical-impact entities in their Member State based on the transitional ECII and shall develop a transitional list of high impact and critical impact entities. The transitional list of high impact and critical impact entities shall be based on a precautionary principle, so that entities may only gain more responsibilities in the revised list after the end of the transition period, compared to where they stand in the national transitional list of high-impact and critical-impact entities.

3. Within 6 months after entry into force of this Regulation, the NCCS-NCAs shall notify the entities on the transitional list that they have been identified as a high-impact or critical-impact entity.

4. Within 2 months after entry into force of this Regulation, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a transitional list of Union-wide high-impact and critical-impact processes. The entities listed in Article 2(1), (3) and (4) shall use the transitional list of high-impact and critical-impact processes to determine the transitional high-impact and critical-impact perimeters and to determine which assets are in the scope of the first cybersecurity risk assessment at entity level.

5. Within 2 months after entry into force of this Regulation the NCCS-NCAs shall provide a list of relevant national legislation with relevance for cybersecurity aspects of cross-border electricity flows to the ENTSO for Electricity and the EU DSO entity. Within 3 months after entry into force of this Regulation the ENTSO for Electricity, in cooperation with the EU DSO entity, shall prepare a transitional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows.

6. The transitional list of European and international standards and controls shall include:

   (a) European and international standards and national legislation which provide guidance on methodologies for cybersecurity risk management at entity level; and

   (b) cybersecurity controls equivalent to the controls that are expected to be part of the minimum and advanced cybersecurity controls.

7. The ENTSO for Electricity and the EU DSO entity shall consult ENISA, ACER, the NCCS-NCAs

on the proposal for a transitional list of standards. The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by these parties when finalising the transitional list of standards. The ENTSO for Electricity and the EU DSO entity shall publish the transitional list of standards on their websites.

8. Until the minimum and advanced cybersecurity controls are defined, all entities listed in Article 2(1), 2(3) and 2(4) shall strive to progressively apply the guidance on cybersecurity risk assessment methodologies and the cybersecurity controls pursuant to paragraph 6 within the transitional high-impact and critical-impact perimeters defined pursuant paragraph 4.

Article 51. Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the Union.

2. By 12 months after the entry into force of this Regulation the information flows, cybersecurity incident and crisis management provisions pursuant to Articles 39, 40, 41, 42, 43 and 44 shall be established and operational.

3. This Regulation shall be binding in its entirety and directly applicable in all Member States.