DSO ENTITY
DSOs FOR EUROPE

European Network of
Transmission System Operators
for Electricity
entsoe

Supporting document for the methodologies for the provisional list of standards

Table of Contents

1 Introduction 3

1.1 Legal status of this document 3

2 Standards which provide guidance on risk management 4

3 Cybersecurity controls from standards and national frameworks 5

4 Cybersecurity control from national legislation 6

5 ANNEX I: MINIMUM AND ADVANCED CYBERSECURITY CONTROLS 7

1 Introduction

This document has been developed jointly by the European Network of Transmission System Operators for Electricity (ENTSO-E) and the EU DSO entity to accompany provisional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity (hereafter referred to as the "provisional list of standards”). This document should be read in conjunction with the provisional list of standards.

The document provides all interested parties with information about the rationale for the for the provisional list of standards, outlining why certain standards have been selected.

1.1 Legal status of this document

This document accompanies the provisional list of standards and is provided for information purposes only. Consequently, this document is not legally binding.

2 Standards which provide guidance on risk management

For risk management, the following standards were selected for the transitional list:

- ISO 31000 Risk management - Guidelines
- ISO/IEC 27005 Information security, cybersecurity, and privacy protection — Guidance on managing information security risks
- NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

The ISO 31000 and ISO/IEC 27005 standards are recommended, as they are designed to work together with the ISO/IEC 27001 standard for information security management systems. The ISO/IEC 27001 standard is the widely used for information security management in the electricity sector.

The ISO 31000 and ISO/IEC 27005 standards are also recommended for European standardization in the ENISA report *Risk management standards – Analysis of standardisation requirements in support of cybersecurity policy* (March 2022, recommendations 3 and 9).

The NIST SP 800-37 standard is included, as some parties are using the NIST Cybersecurity Framework for compliance with the NIS directive. For such parties, a risk management method from NIST may be better suited.

NIST 800-161 is included to cover supply chain risk management. The network code requires entities to consider threats through the supply chain. NIST 800-161 provides guidance on how this can be done.

The ISA/IEC 62443-3-2 standard was not included in the list, as the standard is aimed at performing detailed technical risk assessments. It does not seem well-suited to perform high-level risk assessments as part of a cybersecurity management system, as the NCCS requires.

A list of national standards was prepared based on the knowledge of the TSOs and DSOs participating in NCCS expert groups. The list is not exhaustive, as not all member states were represented in these working groups.

3 Cybersecurity controls from standards and national frameworks

For the cybersecurity controls equivalent to the controls that are expected to be part of the minimum and advanced cybersecurity controls, the following standards were selected for the provisional list:

- ISO/IEC 27002 Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27019 Information technology — Security techniques — Information security controls for the energy utility industry
- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
- NIST Framework for Improving Critical Infrastructure Cybersecurity

The ISO/IEC 27002 and ISO/IEC 27019 were selected as they are designed to work together with the ISO/IEC 27001 standard for information security management systems. Also, many parties in the electricity sector are already following these standards.

The NIST documents are included, as some parties are using the NIST for compliance with the NIS directive.

The ISA/IEC 62443-2-1 standard was not included, as it is not widely used, and the controls can be mapped to the ISO/IEC 27002 standard.

Additional standards for the technical implementation of controls are included for guidance.

4 Cybersecurity control from national legislation

National cybersecurity legislation relevant to entities in scope of the NCCS was sent to ENTSO-E and the DSO entity by the national competent authorities and NRAs. The legislation was gathered in this section of the provisional list of standards.

ENTSO-E and the DSO Entity did not have the capacity or mandate to verify the submitted legislation. It was included as it was provided by the nation authorities.

The national legislation is not mapped to the controls in Annex A. Such a mapping is foreseen in the mapping matrix that will be part of the common electricity cybersecurity framework. See Article 34 of the NCCS.

5 ANNEX I: MINIMUM AND ADVANCED CYBERSECURITY CONTROLS

Annex I gives cybersecurity controls equivalent to the controls that are expected to be part of the minimum and advanced cybersecurity controls. The controls were selected from ISO/IEC 27001 Annex A, as this standard is widely used in the electricity sector.

The provisional list does not include a mapping of the ISO/IEC 27001 Annex A controls to other European and international standards or to national legislative or regulatory. Such a mapping will be developed later in the mapping matrix for electricity cybersecurity controls against standards described in Article 34 of the NCCS.

The provisional list selects controls from ISO/IEC 27001 Annex A without any modifications. When the binding minimum and advanced cybersecurity controls are developed according to Article 29 of the NCCS, the selected controls may be extended based on the results of the Union-wide or regional risk assessment.

Controls were selected taking into account the required effort to implement them. In particular for the minimum controls, the provisional list excludes controls that would be difficult to implement for smaller entities.

Controls were only selected if they can be used to mitigate the risks that are in scope of the NCCS, that is, risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. Controls related to privacy have been excluded, although most entities will need to implement them to comply with other regulations such as the GDPR.