



Strengthening the cybersecurity of our wind assets, delivering a resilient energy system

Wind energy supplies 20% of Europe's electricity today. Reaching climate neutrality will require increasing this to 50% through a more decentralized, electrified energy system. As wind and grid infrastructure expand, cybersecurity risks grow—particularly the danger of hidden hardware or software vulnerabilities and digital dependencies that suppliers from foreign countries of concern could exploit.

To manage these risks, the European industry has identified critical digital systems in wind and grid infrastructure that require strategic scrutiny. Without project-level risk assessments also looking into supplier cybersecurity threats, these systems should not be procured from suppliers linked to high-risk foreign countries.

To support a consistent understanding of supplier-related cybersecurity threats, WindEurope—supported by Accenture—has developed the Supplier Cybersecurity Threat Assessment Framework. This framework provides EU and national authorities with a transparent way to assess supplier risks for critical systems, informing decisions on project eligibility for auctions, state or EU support, and grid connection.

This methodology consists of a structured questionnaire designed to assess cybersecurity threats and resilience across suppliers and systems. It guides the assessor through targeted questions grouped by roles, attributes, and topics, enabling a transparent, evidence-based evaluation of risk and maturity levels.

We call for this threat assessment framework to be embedded in all relevant legislation:

- By national Governments when implementing the Net-zero Industry Act articles 25 and 26 on cybersecurity prequalification criteria for wind farms
- By relevant market surveillance authorities when implementing the EU Cyber Resilience Act Articles 53 and 54 and 57 on supplier oversight, product risk handling, and regulatory intervention
- By relevant national regulatory authorities and System Operators when implementing the Network Code Cybersecurity articles 20, 24 and 26
- The European Commission, in particular DG Connect and DG Grow, and in due course the European Parliament and National Governments, in any relevant new or revised legislation for instance the EU Cybersecurity Act
- By relevant national competent authorities and Systems Operators when implementing NIS2 Directive Articles 7, 21 and 22 on supply chain security and risk management
- By relevant national Ministries when implementing Foreign Direct Investment screening article 13 on Determination of likely negative impact on security and public order