IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/45ISM/2025/4524925/
Vol. 2025 (13), Article ID 4524925

# Information and Cyber Security in Energy Sectors Related to Business Processes and Risks*

LAMPE Georg Sven, MASSNER Stephan, WITTSTOCK-LAMPE Anke,
PITZ Fabian, NAUMANN and Michael Matthias

The Bucharest University of Economic Studies, Bucharest, Romania.

Correspondence should be addressed to: LAMPE Georg Sven, lampe@compliance-docs-group.com

* Presented at the 45th IBIMA International Conference, 25-26 June 2025, Cordoba, Spain

## Abstract

Compliance with information and cyber security is of excessive importance for the European energy sector due to the cumulative expansion of information technology and communication infrastructure to regulate energy networks of production and distribution energy. The continuous improvement and development of organizational and technical adaptation processes to fulfil security requirements are indispensable to expand the distribution grids with new "intelligent" technologies as well application in line with demand. It is necessary to protect the corporate assets of telecommunications and IT systems against risks. Possible elementary hazards within the energy grids must be dealt with proactively. To this end, grid efficiency and grid use from renewable energies must be integrated as completely as possible into the energy sector while a consistently high supply quality.

Partially and fully automated grid infrastructure for energy required at first appropriate IT security standards. Furthermore, an active establishing of management system is involved for information and cyber security to protect against cyber-attacks on their ICT based infrastructure. For compliance with various protection objectives, the core requirements were set by the legal framework for all energy sector operators and the model must be adjust and expanded. Moreover, the aim-oriented definitions for the different interests in the field of energy grid and sales regulated field through external market participants must be considered. The regulations for information and cyber security are not formulated specifically enough in their requirements and are sometimes contradictory in comparison with other official requirements. This lack of harmonization leads to inconsistencies in complex cyber security regulation and hazard potential risks.

**Keywords:** Information Security Management System (ISMS), Security Processes, Business Processes, Business Continuity Management, Risk Processes

**Cite this Article as:** LAMPE Georg Sven, MASSNER Stephan, WITTSTOCK-LAMPE Anke, PITZ Fabian, NAUMANN and Michael Matthias Vol. 2025 (13) "Information and Cyber Security in Energy Sectors Related to Business Processes and Risks " Communications of International Proceedings, Vol. 2025 (13), Article ID 4524925, https://doi.org/10.5171/2025.4524925