THE DORA REGULATİON – REQUİREMENTS AND CHALLENGES FOR POLİSH BANKS

Zofıa Polkowska

Szkoła Główna Handlowa

zpolko@sgh.waw.pl

Abstract**:** Regulation (EU) 2022/2554 on digital operational resilience sets out a new framework for digital risk management, including in the banking sector. The aim of this article is to assess the challenges associated with the implementation of the Digital Operational Resilience Act (DORA) in the Polish banking sector. An analysis of legal acts and a critical review of the literature on the digital transformation of the sector were carried out. The author discusses the key requirements set by DORA in the area of digital operational resilience, including ICT (Information and Communication Technology) risk management, incident reporting, system testing and supervision of relations with external suppliers. The publication also presents the main challenges faced by Polish banks in the process of adapting to the new regulations, such as the need to invest in IT infrastructure, organisational changes and cooperation with suppliers. The article also contains recommendations for the practical implementation of DORA.

Key words: *banking, DORA, operational resilience, cybersecurity, Polish banking sector*

INTRODUCTİON

The development of digital technologies and the increase in cyber threats have necessitated the regulation of the operational resilience of financial institutions. Regulation (EU) 2022/2554 of the European Parliament and of the Council on the digital operational resilience of the financial sector, known as DORA (Digital Operational Resilience Act), imposes uniform obligations on institutions in this area. The aim of the Regulation is to strengthen the operational resilience of financial institutions, including banks, to threats related to information and communication technologies (ICT). The new regulations impose a number of obligations on banks to ensure operational resilience in the event of cybersecurity and ICT disruptions. Regulation (EU) 2022/2554 identifies five pillars of digital operational resilience:
1. ICT risk management.
2. ICT incident reporting.
3. Digital resilience testing.
4. ICT service provider risk management.
5. Cooperation and exchange of information on cyber threats.

Banks are required to implement a comprehensive ICT risk management framework, including, among other things, continuous monitoring of all sources of ICT risk, implementation of a process for detecting unusual activities, and configuration and maintenance of resilient systems to minimise the impact of risk. Banks are required to report ICT incidents and test tools and systems for threat detection. As part of their cooperation with external ICT service providers, contracts will have to include information necessary for proper monitoring, including a description of the level of service provision and the location of data processing.

Banks were required to implement the requirements of the regulation from 17 January 2025.

METH`ODOLOGY

The article analyses legal acts and critically reviews literature on the digital transformation of the banking sector. The aim of the analysis was to identify challenges related to the implementation of the DORA regulation. The analysis covered banks in the Polish banking sector operating as joint-stock companies in 2024–2025.

FİNDİNGS

- The article identifies five main areas that have been regulated by the new regulation: ICT risk management, ICT incident handling, testing of digital operational resilience, supervision of external ICT service providers, and exchange of information on cyber threats. The article highlights the challenges associated with meeting the requirements of the regulation, such as

the need to modernise technological infrastructure, increased operating costs, the obligation to provide training in the area of cybersecurity, and the need to implement new reporting procedures. It also draws attention to the need for banks to cooperate with, among others, the Financial Supervision Authority in order to properly implement the Regulation, and with technology providers in order to meet the requirements set out in DORA. The article presents recommendations for banks on the implementation of the requirements set out in the Regulation, including building a culture of cyber resilience among employees, incorporating ICT risk management into banks' strategies, and developing sectoral cooperation in the exchange of information on threats. The article contributes to the discussion on the digital transformation of the banking sector in Poland and the role of regulation in shaping a resilient banking system. The article identifies challenges for banks in the Polish sector related to the implementation of DORA, such as:

- the need to adapt ICT infrastructure – modernisation of infrastructure and automation of risk management processes,
- insufficient competence and awareness of employees in the field of cybersecurity,
- regulation of cooperation with suppliers, renegotiation of contracts and implementation of control procedures,
- the need to prepare new reports,
- audits related to the implementation of regulations.

New reporting obligations may also result from obligations imposed by European Supervisory Authorities, including the European Banking Authority and the European Securities and Markets Authority, on the Financial Supervision Authority.
During the two-year period allocated for preparation for the implementation of the obligations imposed by the Regulation, banks analysed the gap in order to assess their maturity in relation to regulatory requirements and to identify areas that require modification and investment. As part of the implementation of the obligations, specific problems may arise in the sector for individual banks, which may materialise in various areas. It should be noted that in the Polish sector, recommendations have been developed by the Polish Bank Association (ZBP) in cooperation with representatives of the sector. In accordance with the Regulation, agreements may be concluded in the sector for the exchange of information on cyber threats.

CONCLUSİONS

The aim of implementing Regulation 2022/2554 is to increase the digital resilience of, among others, the banking sector. Banks in the Polish sector, thanks to the implementation of earlier regulations, such as Recommendation D of the Polish Financial Supervision Authority (KNF), have achieved maturity in terms of digital resilience. However, the implementation of the Regulation requires the adaptation of many processes in banks, including risk management, ICT incident reporting and cooperation with ICT suppliers. The significant role of information exchange and cooperation with regulators in order to properly meet the requirements of the Regulation should also be noted.
The benefits of implementing the new regulation include harmonisation of regulations on cooperation with suppliers and other institutions, increased operational resilience, enhanced cyber security protection for the sector, and increased customer confidence through the security of digital services. The regulation introduces a comprehensive approach to ICT incident management in the European Union's financial sector. The requirements imposed are aimed at building the overall digital resilience of the entire sector. Compliance with these obligations requires banks to invest in technology, processes and staff. Measures in this area support the security of the financial system in the face of growing cyber threats.

REFERENCES

Lichosik, A. (2023). DORA jako prawny instrument ochrony cyfrowego bezpieczeństwa rynku finansowego. *Studia Prawnoustrojowe*, (62). https://doi.org/10.31648/sp.9581
Bujalski R., Operacyjna odporność cyfrowa sektora finansowego (DORA), LEX/el. 2023.
M. Mariański, Problematyka regulacji rynku finansowego w ujęciu transgranicznym. Analiza na przykładzie prawa polskiego i prawa francuskiego, Olsztyn 2020
Xu M., David J.M., Hi S., The Fourth Industrial Revolution: Opportunities and Challenges, International Journal of Financial Research; Vol. 9, No. 2; 2018; https://www.researchgate.net/publication/323638914_The_Fourth_Indu.

Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2023). Digital sovereignty as control: the regulation of digital finance in the European Union. *Journal of European Public Policy*, *31*(8), 2226–2249. https://doi.org/10.1080/13501763.2023.2295520
Koleśnik J., Piaskownica regulacyjna jako akcelerator innowacyjności w polskim systemie bankowym, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 2017, nr 475, s. 90-99
Błędowski P., Kurczewska U., Zaleska M. (red.) *Ekonomiczne i społeczne skutki nowych technologii, Warszawa 2020, Oficyna Wydawnicza SGH*
Ślązak E., *Sztuczna inteligencja w detalicznych usługach bankowych* [w:] *Usługi i produkty finansowe dla klinetów indywidualnych,* Koleśnik J. (red.), Warszawa 2024, Oficyna Wydawnicza SGH
Zaleska, M. (2018, July 25). Innowacyjna bankowość. Gazeta Bankowa. https://www.gb.pl/innowacyjna-bankowosc-pnews-1401.html
Zaleska, M., & Kondraciuk, P. (2019). Theory and practice of innovation development in the banking sector. Financial Sciences, 24(2), 76–88. https://doi.org/10.15611/fins.2019.2.06
Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej, i bezpieczeństwa środowiska teleinformatycznego w bankach, KNF, Warszawa 2013
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (PE/32/2022/REV/2)
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (PE/41/2022/INIT)
https://www.pwc.pl/pl/artykuly/dora-dlaczego-to-jest-dla-ciebie-istotne.html
https://bank.pl/jak-dora-zmieni-funkcjonowanie-polskiego-sektora-finansowego-od-2025-roku/
Rekomendacje Zarządu Związku Banków Polskich z dnia 9 października 2024 r. ws. zgodnych z Rozporządzeniem DORA wzorów aneksów do umów o świadczenie usług ICT, Warszawa 2024
https://www.knf.gov.pl/?articleId=91834&p_id=18