THE DIGITAL OPERATIONAL RESILIENCE ACT – CHALLENGES FOR A SAFER FINANCIAL INSTITUTIONS

MILOS MARYSKA, PETR DOUCEK, LEA NEDOMOVA

Prague University of Economics and Business, Faculty of Informatics and Statistics, Prague, Czech Republic
milos.maryska@ vse.cz, doucek@vse.cz, nedomova@vse.cz

The Digital Operational Resilience Act (DORA) is the latest regulation issued by the European Union to address the financial sector's growing reliance on technology and manage the associated cyber security risks. DORA sets the whole framework and extends the requirements for financial sector resilience not only to financial institutions themselves, but also extends the security requirements to suppliers of critical ICT services. This paper nalyses the main issues of implementation starting with just determining whether a company is subject to DORA through to the actual implementation and the impact of DORA on internal processes, capabilities and more. The key problems associated with the implementation of DORA can be clearly considered to be the financial and time complexity of the implementation, the short timeframe for implementation, the degree of impact of DORA on the internal processes of companies and the need for significant changes within IT, IT process, IT Risk Management and especially the lack of experts with adequate knowledge and experience.

Keywords:
DORA,
implementation,
risks,
security,
challenges

University of Maribor Press

DOI https://doi.org/10.18690/um.fov.3.2024.45
ISBN 978-961-286-842-0

1 Introduction

Digital transformation is a word that is bandied about in many ways in most companies and it could be argued that it is a phrase that is bandied about in all companies in the financial sector.
Digitisation affects many areas, including document processing, including the extraction of documents and their subsequent access to users, as well as the implementation of technologies that take over responsibility for routine tasks in which they replace living beings, and the implementation of various AI technologies to make companies more efficient. All of these areas are linked to one basic word - data - and it can be said that companies are collecting, storing and managing ever-increasing amounts of data to gain insight, make informed decisions and improve their operations.

At the same time, with the increasing use of digital technologies, businesses are becoming more and more dependent on data and are increasingly at risk of cyber-attacks, data breaches and other security threats. Therefore, it is essential to have a robust digital resilience strategy to protect data and maintain business continuity (EBA, 2019; EBA, 2019a).

The Digital Operational Resilience Act (DORA) is a regulation introduced by the European Union to address the financial sector's increasing reliance on technology and to manage the associated cyber security risks. This dependence is mainly driven by the drive to digitise companies mentioned above. In view of these efforts, attention is thus being paid at EU level to the cybersecurity aspect, which is closely linked to digitalisation.

DORA introduces specific and prescriptive requirements that are homogeneous across EU Member States, so companies have a simplified position as key parts of the regulation will be the same in all countries.

Compared to other regulations, the specific feature of DORA is that it does not only apply to the institution itself, but is binding on critical third-party ICT services that provide ICT-related services to financial institutions, such as cloud platforms, data analytics and auditing services, and of course the development and operation of companies' key information systems.

The first draft of DORA was published by the European Commission as part of the Digital Finance Package (DFP) on 24 September 2020. The law was approved by the European Parliament and entered into force on 16 January 2023. The European Supervisory Authorities (European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority (ESMA)) are preparing a set of policy products to enable the application of DORA (EU, 2023; EBA, 2019).

In the context of the above, the main objective of DORA is to strengthen the resilience of the financial sector to ICT-related incidents and to standardise a set of criteria, templates and guidelines that will determine how financial organisations manage ICT and cyber risks (EU, 2023; KPMG 2023; Cybersecurity Exchange, 2023).

The aim of this paper is both to identify the key issues associated with DORA and, based on the authors' practical experience, to outline the critical steps that need to be implemented in financial institutions to successfully implement DORA.

2 Methodology

The article is based on an analysis of current information from a number of information sources describing and defining various aspects of the Digital Operational Resilience Act and the authors' experience in practical implementation of the DORA standard in the financial institutions in which they are involved.

The main sources of information are the directives issued by the European Union and other sources describing the requirements for companies under the DORA Regulation.

For the purpose of this paper, we analyzed more than 37 information sources and 12 of them were used and cited in this paper.

3 Dora and its implementation

3.1 Self Assessment and Critical Areas

The first and fundamental step that needs to be taken in a DORA implementation is to determine whether or not the company is a DORA subject of interest. Unfortunately, there is no specific list of entities or types of companies that are subject to the standard, so it is necessary to analyse the entire set of DORA requirements and then compare them with the company's focus, turnover, number of employees and many other parameters (BCI, 2023).

The initial DORA self-assessment contains over 30 questions that determine whether or not a company is obliged to implement DORA.

Examples of issues are (Bousaissi, 2023; EU, 2023):

- Is the entity a payment institution, including payment institutions exempted in accordance with Article 32 (1) of Directive (EU) 2015/2366?
- Is the entity an account information service providers?
- Is the entity an electronic money institution, including electronic money institutions exempted in accordance with Article 9 (1) of Directive 2009/110/EC?
- Is the entity a credit institution?
- Is the entity a trading venue?
- Is the entity an investment firm?
- Is the entity an administrator of critical benchmarks?
- Is the entity a crypto-asset service providers as authorized under MiCA and issuers of asset-referenced tokens ?
- Is the entity an insurance and reinsurance undertaking?
- Is the entity a central securities depository?
- Is the entity a trade repositories?
- Is the entity a manager of alternative investment funds?
- Is the entity a crowdfunding service provider?

- Is the entity an insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediary?
- Is the entity an institution for occupational retirement provision?
- Is the entity a credit rating agency?
- Does the entity have more than 10 persons?
- Is the entity having annual turnover and/or annual balance sheet total > 2 million EUR
- Is the entity a payment system, other than referred to in the list above?
- Is the entity a card payment scheme?
- Is the entity a system operator, i.e. the entity or entities legally responsible for the operation of a system.?

It is clear from the above that almost all companies that touch the financial market in any way, have more than 10 employees, are affected by DORA implementation, thus it also applies to small financial organisations. The turnover does not need to be taken into account as 99% of the companies touching the financial market exceed the above-mentioned values.

If it is identified through self-assessment that a company is required to implement the DORA framework, it is advisable to be very structured and identify the key people and areas that need to be addressed within the company to implement DORA. In order to successfully implement DORA within a financial institution, a large number of steps and overall changes need to be implemented within the company and its processes. The critical areas that need to be implemented include (UK Finance, 2023; EU, 2023; ENISA, 2021; RSM, 2023):

- DORA can be considered a very large project, so a responsible project manager needs to be identified to deal with readiness and compliance within the organisation[2].
- Understand the five pillars of DORA: DORA divides digital operational resilience into five areas - risk management, incident reporting, digital operational resilience testing, third party ICT risk management and information sharing and intelligence[2].
- Significantly strengthen the area of ICT risk governance and management: the DORA places a strong emphasis on ensuring digital operational

resilience, and DORA is primarily the responsibility of risk management with compliance support with respect to the legal impact of impelment.

- Modify contracts with critical suppliers: DORA specifies requirements for contracts with third-party ICT providers that must be incorporated into financial institutions[1] contract management.
- ICT incident management and recording: the aim of DORA is to standardise the reporting obligations for serious ICT incidents across the European financial industry, i.e. companies must take this area into account in their internal processes.
- Control of third-party ICT risks: not only does the company oversee its own risks, but it must have processes and responses in place for third-party risks.
- Digital Operational Stability Testing:Regular testing of the operational stability and security of critical ICT systems is essential for the smooth operation of financial businesses[1].

A detailed analysis of the above critical elements is a prerequisite for the community to prepare for the full application of DORA and be able to meet all requirements. The above-mentioned critical areas are clearly linked to the problems associated with the implementation of DORA itself.

3.2 Key issues in DORA implementation

The implementation of the Digital Operational Resilience Regulation is quite a challenge for companies, especially compared to previous standards such as NIS2. The main reason for the challenge is the fact that a larger number of entities are subject to DORA - it is estimated that more than 6,000 companies in the Czech Republic will be affected by this regulation, mainly due to the transfer of DORA compliance responsibilities from financial institutions to suppliers of critical IT services. Of the many issues we have identified, we consider the following to be key issues (RSM, 2023; Norton Rose Fulbright, 2023; MorganFranklin Consulting, 2023):

- Preparedness, where smaller financial firms in particular may not be sufficiently prepared for the implementation of new requirements that are mandatory and failure to comply with them may be punishable by fines.
- Regular updating of ICT systems and elimination of threats.

- Process optimization of existing processes, the introduction of new processes and their description are key to meeting the requirements.
- Training of all relevant staff who must understand and comply with all new regulations.
- Timeframe: the planned timeframe for implementation is ambitious and requires organisations to take a more proactive approach to addressing these challenges.
- Design and implementation of complex security architecture.

All of the above points present challenges present a huge set of issues that are not only associated with the need for a significant knowledge base, but also funding, time etc. that companies do not have with respect to the launch date. The size of the company and its affiliation to a group of companies is an important aspect of the issue. If the company is part of a group of companies that use, for example, a group ICT service provider + other external suppliers, the implementation of DORA must also occur at the group level to ensure compliance.

While DORA is intended to strengthen the IT security of financial entities, its implementation may present many more challenges for smaller organizations, which have their own challenges of being subject to DORA compared to large corporations (MorganFranklin Consulting, 2023):

- Small businesses may face limited resources in terms of budget and staff to implement new requirements.
- They may lack the necessary technical knowledge to understand and implement complex DORA requirements.
- Small organisations often rely on third party ICT providers and managing relationships with third parties can be problematic.
- The regulatory burden of complying with DORA and other standards and regulations can be significant, and even small companies must meet defined requirements to augment staff with specific job functions.

3.3 EU norms related to IT security for financial institutions

With regard to the previous, let us give a brief overview of how many binding standards have been issued in recent years for the IT Security:

- Directive 2013/36/EU (CRD): this directive requires the EBA to further harmonise the internal governance arrangements, processes and mechanisms of financial institutions across the EU.
- Directive (EU) 2015/2366 (PSD2): this directive mandates the establishment, implementation and monitoring of security measures for operational and security risks.
- ICT and Security Risk Management Guidelines: these guidelines set out requirements for credit institutions, investment firms and payment service providers (PSPs) to mitigate and manage their information and communication technology (ICT) and security risks.
- EU Cybersecurity Law: the EU framework for cybersecurity certification for ICT products allows for the creation of tailored and risk-based EU certification schemes. The NIS2 Directive is the EU legislation on cybersecurity. It provides legal measures to strengthen the overall level of cybersecurity in the EU.
- DORA

In terms of content, these standards and directives seek to ensure a consistent and robust approach to IT security across the EU financial sector, but their number and range is significant and they impose a significant burden on companies.

4 Summary and conclusion

On the one hand, the implementation of dora represents a significant progress in setting rules and requirements for ICT security of various types of financial institutions, which can be considered a very positive factor, especially from the perspective of the clients of these companies. On the other hand, however, there are many problems associated with this regulation and its implementation, including in particular the lack of stability of the legislation, which is still under development, the volume of changes that companies have to implement even in their key processes.

Acknowledgements (optional)

Paper was processed with support from institutional-support fund for long-term conceptual development of science and research at the Faculty of Informatics and Statistics of the Prague University of Economics and Business (IP400040).

References

BCI. (2023). What we know about DORA: The Digital Operational Resilience Act. https://www.thebci.org/news/what-we-know-about-dora-the-digital-operational-resilience-act.html

Bousaissi, K. (2023). How will DORA impact the financial sector? https://www.ey.com/en_lu/wealth-asset-management/luxembourg-market-pulse/how-will-dora-impact-the-financial-sector-

Cybersecurity Exchange. (2023). Securing the Future of Finance: Top Cybersecurity Best Practice for Financial Institutions. https://www.eccouncil.org/cybersecurity-exchange/whitepaper/securing-the-future-of-finance-top-cybersecurity-best-practices-for-financial-institutions/

EBA. (2019). European Banking Authority. EBA publishes guidelines on ICT and security risk management. https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-guidelines-ict-and-security-risk-management

EBA. (2019a). European Banking Authority. EBA Guidelines on ICT and Security Risk Management. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

ENISA. (2021). EU CYBERSECURITY INITIATIVES IN THE FINANCE SECTOR - ENISA. https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector/@@download/fullReport

EU. (2023) Shaping Europe's digital future. The EU Cybersecurity Act. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

KPMG. (2023). KPMG Global. Digital Operational Resilience Act. https://kpmg.com/xx/en/home/insights/2023/10/digital-operational-resilience-act.html

MorganFranklin Consulting. (2023). What US Financial Service Providers Should Do to Prepare for the DORA Regulation. https://www.morganfranklin.com/insights/what-us-financial-service-providers-should-do-to-prepare-for-the-dora-regulation/

Norton Rose Fulbright. (2023). Digital Operational Resilience for the Financial Sector (DORA): 10 things to know. https://www.nortonrosefulbright.com/en/knowledge/publications/251c1837/digital-operational-resilience-for-the-financial-sector-dora-10-things-to-know

RSM. (2023). Demystifying the Digital Operational Resilience Act (DORA) for middle market Businesses. https://www.rsm.global/insights/demystifying-digital-operational-resilience-act-dora-middle-market-businesses

UK Finance. (2023). Complying with DORA – steps for financial institutions to take. https://www.ukfinance.org.uk/news-and-insight/blog/complying-dora-steps-financial-institutions-take