International Cybersecurity Law Review (2023) 4:79–90
https://doi.org/10.1365/s43439-022-00076-5

Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)

Dirk Clausmeier

Received: 7 September 2022 / Accepted: 18 November 2022 / Published online: 16 December 2022

Abstract Cyber incidents in the financial sector are rising, and financial entities are increasingly outsourcing their IT infrastructure to third party service providers. The new Regulation on Digital Operational Resilience for the Financial Sector (DORA) addresses this trend and aims to strengthen the cyber resilience of financial entities, such as banks, insurance companies, investment firms and crypto-asset service providers. DORA creates a regulatory framework including requirements on Information and Communication Technology (ICT) risk management, ICT-related incident reporting and penetration testing. DORA entails provisions on ICT third-party risk management and introduces a European oversight framework for critical ICT third-party service providers. The requirements set out by DORA are homogenous across all EU member states. DORA follows a risk-based approach and requirements are applied in accordance with specific risk profiles and the size and nature of the financial entities. DORA also addresses the overlap with the horizontal Network and Information Security Directive (NIS) by introducing a *lex specialis* rule. This paper gives an overview on the key parts of DORA and analyses whether its rules are appropriate to prevent and better mitigate rising cyber threats in the financial sector in an efficient way for all stakeholders.

Keywords Oversight Framework · Incident Reporting · Third-Party Risk · Penetration Testing · TIBER · Financial Sector

✉ Dirk Clausmeier
Berlin, Germany
E-Mail: dirk.clausmeier@bmf.bund.de

Verordnung des Europäischen Parlamentes und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA)

1 Introduction

In September 2020 the European Commission published the digital finance package. It included the digital finance strategy[1] and the retail payment strategy[2], and two legislative proposals, the markets in crypto-assets (MiCA)[3] and the Digital Operational Resilience Act (DORA)[4]. The digital finance strategy builds on the Fin Tech Action Plan (2018)[5] and supports the digital transition of the financial sector and embraces technological innovations. However, the digital transformation of the financial sector can only be successful with resilient IT systems of all European financial entities. That is why the Digital Finance Package includes DORA.

The threat of cyber-attacks in the financial sector has dramatically increased in recent years. In comparison to other sectors, the financial sector presents an attractive target for cyber criminals. Cyber-attacks also have the potential to disturb or disrupt financial services which are important for the global financial system. According to *Kost* in just the first six months of 2021, phishing attacks in the financial sector increased by 22% since the same period in 2020.[6] On top of this, financial firms are facing rising ransomware and distributed denial-of-service (DDoS) attacks.[7] In the past, strong voices in the financial market predicted the next financial crisis could result from a systemic cyber-attack.[8]

The European Commission was alert to and addressed cyber risks in the DORA proposal[9] in order to strengthen the IT security of financial firms in the EU. After quick Council negotiations during the German, Portuguese and Slovenian Presidency, a general approach was reached in November 2021.[10] The European Parlia-

[1] COM (2020) 591 final.

[2] COM (2020) 592 final.

[3] COM (2020) 593 final.

[4] COM (2020) 595 final.

[5] COM (2018) 109/2.

[6] *Kost* focuses on different cyber threats in the financial sector and also analyses rising ransomware attacks, https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services.

[7] The timeline published by Carnegie Endowment chronicles ~200 cyber incidents targeting financial institutions since 2007: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

[8] *Lagarde* warned in February 2020 that cyber-attacks could cause the next financial crisis; https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecba9322556.html. In 2017, G20 Finance Ministers and Central Bank Governors agreed that the malicious use of Information and Communication Technologies (ICT) is an ongoing threat to the entire financial system; https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/world/G7-G20/G20-Documents/2017-11-03-g20-chairs-summary.pdf?__blob=publicationFile&v=3.

[9] COM (2020) 595 final.

[10] See https://www.consilium.europa.eu/media/53107/st14068-en21.pdf.

ment published its report in December 2021.[11] During the following French Presidencies, the European Parliament, Commission and Council negotiated in trialogue and reached a political agreement in June 2022.[12] DORA was formally adopted in November 2022 and will be applicable two years later. In the meantime, the European Supervisory Authorities (ESAs) will develop technical standards to provide further clarification and guidance.[13]

DORA includes new requirements for financial firms in the field of IT governance, reporting and also penetration testing. Critical ICT third-party service providers (CTPP) will be overseen by the three ESAs (EBA, EIOPA or ESMA[14]). After giving an overview on the general provisions of DORA, this publication will focus on the new requirements for financial firms and analyse whether its rules are appropriate to prevent and better mitigate rising cyber threats in the financial sector in an efficient way for all stakeholders.

2 General provisions

DORA entails several general provisions. First, which financial entities are in the scope of DORA will be explained. The principle of proportionality also plays an important role for the application of DORA and will be discussed in a second step. Third, the relation to the horizontal Network and Information Security Directive (NIS) will be explained.

2.1 Personal scope of DORA

The broad personal scope of DORA is defined in Article 2 and includes all supervised financial entities, not only traditional financial institutes, such as banks, insurances and investment firms. DORA also applies to less traditional financial entities, such as credit rating agencies, trade repositories, payment and e-money institutions as well as trading venues. DORA also applies to crypto-asset service providers as authorized under MiCA and issuers of asset referenced tokens. It can only be supported that DORA has a large personal scope, given the omnipresent threat in the financial sector. New technology driven financial entities should maintain from the beginning some basic cyber hygiene rules. Even if especially younger FinTechs will be faced with DORA cyber regulation for the first-time, this does not

[11] EP report on the proposal for a regulation of the European Parliament and the Council on digital operational resilience for the financial sector (COM [2020] 0595 – 2020/0266(COD)).

[12] Consolidated version of the text available at https://data.consilium.europa.eu/doc/document/ST-10581-2022-INIT/en/pdf. Citations of articles in this text refer to this version of DORA.

[13] See also press release of the Council after the provisional agreement was reached on 11 May 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/.

[14] European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority.

seem excessive since DORA contains a simplified ICT risk management framework for such microenterprises, as well as for smaller and medium-sized businesses.[15]

DORA will not apply to audit firms. The inclusion of auditors was initially proposed by the European Commission and supported by the European Parliament.[16] However, the aim of DORA is to strengthen the cyber resilience of financial entities, and auditors are not financial firms and are also not supervised by financial supervisory authorities.[17] Therefore, rightfully so, auditors are not in the scope of DORA.

2.2 Proportionality principle

Article 3a DORA states that financial entities shall implement the rules in accordance with the principle of proportionality, considering their size, the nature, scale and complexity of their services, activities and operations, and their overall risk profile. Although the principle of proportionality is a general rule of law which should be applied throughout European law as such,[18] and therefore the specific article in DORA seems to be unnecessary, it is an important signal that the rules of DORA should not only be applied as such but in accordance to specific risk profiles and in order to keep the financial sector safe. The scope of DORA is very broad and some requirements are quite prescriptive. The consistent application of the principle of proportionality will correct an exhaustive application of the law.

2.3 Interaction between DORA and NIS

The European Parliament and Council adopted the horizontal NIS Directive in 2016 which aims to improve the overall level of cybersecurity in the EU for providers of critical infrastructure.[19] This directive applies to operators of essential services in seven sectors[20], including the financial sector. NIS makes the adoption of enhanced security measures obligatory for relevant operators in those sectors. The operators are identified on a national level by a mechanism set out in NIS. In the financial sector only larger credit institutions, trading venues, insurance firms and central counterparties fall within the scope of NIS.[21]

---

[15] See also the simplified ICT risk management framework in Article 14a DORA.

[16] EP report on the proposal for a regulation of the European Parliament and the Council on digital operational resilience for the financial sector (COM [2020] 0595 – 2020/0266[COD]); COM (2020) 595 final.

[17] The directive on statutory audits of annual accounts and consolidated accounts (2006/43/EC) will be under review and a possible future revision of the scope might be explored.

[18] About the principle of proportionality see *Streinz* [7], para 177 (in German).

[19] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.07.2016, p. 1.

[20] See *Stevens*, CR 12/2021 [6] p. 841 ff. (in German) who describes different providers of critical infrastructures (841–848).

[21] Overview of all the sectors and NIS-implementation in Germany (in German) *Beucher/Fromageau* in Kipker (Ed.), Cybersecurity, [4], pp. 355 (in German).

The upcoming NIS 2.0 Directive (NIS2) which was finally adopted in November 2022 broadens the scope of the current NIS by covering more firms in existing sectors.[22] The scope of NIS2 is broader but the DORA requirements are by far more prescriptive and detailed than the NIS2 requirements. In addition, the scope of DORA includes all financial entities regardless of their criticality for the financial sector. That is why a *lex specialis* clause was introduced into NIS2 stating that DORA takes precedence over the NIS Directive as a *lex generalis*.[23] In case of overlaps the NIS2 requirements will not apply to financial entities. Nevertheless, competent supervisory authorities shall exchange information on incidents with NIS authorities.[24] The importance that DORA's and NIS' ecosystems interconnect is convincing given the overlapping aims, scopes and rules.

3 Specific provisions

DORA entails requirements for financial firms in the field of ICT risk management, incident reporting and testing. DORA will also introduce a new oversight framework for CTPP.

3.1 ICT risk management

DORA includes requirements for internal risk management and third-party risk management.

3.1.1 Management of internal ICT risks

To improve their cyber resilience financial firms are required by Article 4 DORA to set-up an internal governance and control framework to ensure effective and prudent management of all ICT risks. This includes establishing a management body to define, approve and oversee the implementation of all arrangements related to an ICT risk management framework. The ICT risk management framework must include strategies, policies, procedures, ICT protocols and tools necessary to adequately protect all information and ICT assets[25], and pursuant to Article 7 identify, classify and adequately document all ICT–supported business functions, roles and responsibilities, and the information assets and ICT assets supporting these functions, and their roles and dependencies with ICT risk.

[22] Proposal for a Directive of the European Parliament and of the Council on measures for high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – EU doc. COM (2020) 823 final, 16 December 2020, see also *Sievers*, Cybersecurity Law Review [5], pp. 223 who focuses on the new categories of important and essential entities to broaden the scope. https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

[23] Cf. Recital 13 NIS2.

[24] About overlapping reporting requirements see *Clausmeier*, WM [1], pp. 1397 (in German).

[25] See Article 5 DORA.

Article 9 DORA obliges financial entities to have in place mechanisms to promptly detect anomalous activities. Entities shall put in place a comprehensive ICT Business Continuity Policy.[26] For the purpose of ensuring the restoration of ICT systems and data with minimum downtime, limited disruption and loss, as part of their ICT risk management framework, financial entities shall develop and document backup policies and recovery methods[27] as well as a communication strategy.[28]

The above-described requirements are very prescriptive.[29] Risk management is an important element but always needs to be implemented by measures that are appropriate to the financial entities' level of risk. Clear guidance from ESAs on how to put this into practice will surely be appreciated by the affected financial entities.

3.1.2 Management of ICT third-party risks

In recent years, the extent and nature of financial entities with third-party service providers have evolved, particularly in the field of technology. The "G7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector (2018)"[30] states that entities' governing bodies are responsible and accountable for effective oversight and implementation of third-party cyber risk management. Although by DORA entities cannot outsource their responsibilities to a third-party, DORA entails key principles for a sound management of ICT third-party risk and considers the complexity of ICT-related dependencies. This might help governing bodies to get a better understanding of their third-party risks.

Financial entities shall be aware of the nature, scale complexity and importance of ICT-related dependencies. That is why financial entities shall maintain a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.[31] The register must distinguish between services that cover critical or important functions and those that do not. The register is a key element to the proper management of third-party related risks.

Article 27 DORA entails key contractual provisions to ensure a more balanced playing field between the financial entity and the third-party service provider. The contractual arrangement shall include at least provisions on accessibility, availability and integrity, as well as provisions on ensuring access, recovery, service level descriptions and termination right, and also the obligation of the ICT third party

[26] See Article 10 DORA.

[27] See Article 11 DORA.

[28] See Article 13 DORA; on coordination and communication see also FSB report (2020), effective practices for cyber incident response and recovery: https://www.fsb.org/wp-content/uploads/P191020-1.pdf.

[29] Article 14 instructs the ESAs inter alia to specify further elements to be included in the ICT security policies and to develop further components of the controls of access management rights.

[30] https://www.bundesbank.de/resource/blob/764692/01503c2cb8a58e44a862bee170d34545/mL/2018-10-24-g-7-fundamental-elements-for-third-party-cyber-risk-data.pdf.

[31] See Article 25 DORA.

service to help in case of an ICT–related incident.[32] The contractual clauses should strengthen especially smaller financial entities while negotiating contracts with the most prosperous and dominant technology companies, so called BigTechs.

3.2 ICT-related incidents management, classification and reporting

3.2.1 Harmonizing of reporting requirements

Reporting of ICT-related incidents to the supervisory authority is a key element of cybersecurity. The notification gives a higher chance to better understand and identify the source of the incident, to analyse the potential for repercussions and to seek assistance. A quick notification of an incident might also help other institutes to better get prepared for similar attacks. Hackers are often using similar networks or widely used software vulnerabilities.[33] Informed authorities are in the position to publicly warn against and prevent other attacks.

Unfortunately, reporting rules are fragmented. The Financial Stability Board (FSB) found in its 2021 report that fragmentation exists across sectors and jurisdictions in the scope of what should be reported for a cyber incident. Also, time frames for reporting cyber incidents, and how cyber incident information is used, differ in most jurisdictions. This is especially a challenge for financial institutions that operate in multiple countries. Those firms face several different reporting requirements for a single cyber incident. In addition, also financial supervisory authorities receive heterogeneous incident information.[34]

DORA harmonizes reporting requirements for all EU based financial institutions. Financial entities shall establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.[35] While all incidents shall be recorded, financial entities shall only report major incidents to the financial supervisory authority.[36] Relevant criteria to determine a major incident are among others the relevance of the incident on the criticality of the services affected, the duration of the incident and the economic impact. The ESAs are instructed to develop regulatory technical standards in order to establish the content of the notification for significant cyber threats and uniform templates.[37] As a result, the competent authorities should receive homogenous incident information from the whole industry in the future.

Article 17 al. 3 (a) DORA obliges financial entities to produce in a first phase an initial notification. This should include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess

[32] See also (in German) *Ferstl* in: IT-Outsourcing [2, pp. 621]. He describes German requirements on outsourcing contracts. See also (in German) *Kian*, Cloud Computing [3, p. 33] dealing with the specific requirements on cloud contracts.

[33] About the motivation of cyber-attackers see *Ülgen*, Governing Cyberspace [8], pp. 50.

[34] The Financial Stability Board (FSB) in 2021, https://www.fsb.org/wp-content/uploads/P191021.pdf.

[35] See Article 15 DORA.

[36] See Article 17 DORA.

[37] See Article 18 DORA.

possible cross-border impacts. In case the status of the original incident has changed significantly an intermediate report should be produced[38]. A final report should be delivered, when the root cause analysis has been completed, regardless of whether or not mitigation measures have already been implemented.[39]

DORA is not directly introducing a timeframe for financial institutions to report major incidents to the competent authorities. This is left to the ESAs and the European Union Agency for Cybersecurity (ENISA) having to consult and come up with a consistent time frame in line with the time frame planned under the upcoming NIS 2 Directive.[40] Initially, the European Commission proposed strict time limits in DORA that were not consistent with the longer time limits in NIS2.[41] In order to avoid fragmentation, it was the right trialogue decision to let the time limits be defined by regulatory technical standards at a later stage.

3.2.2 Sharing of incident information

Information sharing is key to achieving cyber resilience and preventing further harm from cyber-attacks. Thus, it will also be important that the financial supervisory authority shares relevant information with the NIS authority. Both authorities have different roles.[42] The financial supervisory authority focuses on potential impacts of an incident on the financial system. The NIS authority should analyse potential impacts on providers of critical infrastructures of all branches that are essential for the functioning of a society and economy.[43]

Information of incidents will also be shared by national competent authorities with the ESAs. ESAs will gain an overview of all major cyber incidents in the European financial sector. DORA also invites ESAs to prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The establishment of such an EU Hub can only be supported as it would give the possibility to gain a threat landscape of potential and identified cyber threats affecting the European financial sector. ENISA and NIS authorities could also benefit from the threat analyses of such a centralised data pool.

[38] See Art. 17 al 3 (b) DORA.

[39] See Article 17 al. 3 (c) DORA.

[40] ENISA does not receive any incident reports. However, ENISA is the most competent authority to advice on different NIS2 reporting requirements. For the tasks of ENISA see *Kipker*, Cybersecurity [4], Chap. 1.

[41] COM (2020) 595 final (09/2020).

[42] *Clausmeier*, ibid.

[43] *Beucher/Fromageau*, ibid.

3.3 Testing

3.3.1 Requirements of threat led penetration tests

Once a financial entity has reached cyber maturity, because it has developed and implemented both an effective, actionable plan and an infrastructure to keep its business resilient, it should be tested. DORA obliges financial entities to regularly test their operational resilience and it defines common standards for testing programs.[44] Tests should also include vulnerability assessments, open-source analysis and source code reviews. DORA requires larger financial entities to carry out at least every three years a threat led penetration test ("TLPT").[45] The TLPT may be carried out in a manner proportionate to the size, scale, activity and overall risk of the financial entity.

The G7 Fundamental Elements[46] define TLPT as follows: "TLPT is a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. The purpose of TLPT is to assess and provide insights on entities' resilience capabilities against a real world simulated cyber incident. TLPT should be conducted within a set scope and incorporate a risk management process to ensure a controlled test that minimizes risk to entities."

3.3.2 Internal or external testers

The G7 Fundamental Elements do not advise if a test should be performed by an internal or external tester. In 2018 the European Central Bank (ECB) published TIBER-EU, a European framework for threat intelligence-based ethical red-teaming. It is the first EU-wide guide on how authorities, entities, and threat intelligence and red-team providers should work together to test and improve the cyber resilience of entities by carrying out a controlled cyber-attack. The framework foresees only external testers.[47]

An external tester is more neutral and independent than an in-house testing team. On the other hand, contracts with external companies are costive. The European Commission and Parliament wanted to leave the decision whether to use an internal or external tester to the financial entity itself.[48] The Council had a strong opinion to only allow external testers.[49] As a compromise, DORA requires larger financial institutes that are supervised by the European Central Bank (ECB) to instruct external testers only. All other financial entities are authorized to perform in-house

[44] See Chapter IV DORA.

[45] Art. 23 requests advanced testing by means of threat lead penetration testing.

[46] https://www.bundesbank.de/resource/blob/764690/792725ab3e779617a2fe28a03c303940/mL/2018-10-24-g-7-fundamental-elements-for-threat-led-penetration-testing-data.pdf.

[47] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

[48] COM (2020) 595 final (09/2020).

[49] General Approach of the Council see https://www.consilium.europa.eu/media/53107/st14068-en21.pdf.

tests. The ESAs will develop a regulatory technical standard to specify further the requirements and standards governing the use of internal testers.[50] ESAs should also specify further the requirements and standards regarding the scope of the test and the testing methodology. As quite a lot of Member States have already implemented the TIBER-EU Framework it will be important that the standards will be developed in accordance with this framework.

It is important to know that NIS2 will not require any TLPT for entities falling under its scope. That means that there is no risk of overlapping regulation regarding testing obligations with DORA. Still, DORA testing standards are quite high, regardless of the type of tester. Also, smaller entities are not obliged to perform expensive TLPTs. They should rather first invest their limited budget in a robust IT infrastructure before investing to comply with higher testing standards.

TLPTs should be carried out at least every three years.[51] Based on the risk profile of the financial entity and considering operational circumstances, the competent authority may in accordance with Article 23 DORA, where needed, request the financial entity to reduce or extend this frequency. TLPTs are expensive and time consuming. Therefore, authorities should make use of the exception to extend the time period in case the operational circumstances allow for it.

3.4 Oversight framework for critical ICT service providers

The FSB considers in its report on BigTechs (2019) financial stability implications of BigTech in finance.[52] Financial entities rely on advanced ICT services often provided by BigTechs. DORA addresses this problem and the ongoing trend of financial entities to outsource their IT-infrastructure to third-party service providers in Chapter V.

IT architectures have been becoming more complex over the last years, and it can only be welcomed that DORA takes a more holistic approach beyond internal processes and systems. As a new model of European oversight, DORA foresees an oversight framework for CTPP, such as cloud services, under a joint oversight regime, appointing either EBA, ESMA or EIOPA as lead overseer.

3.4.1 The architecture of the European oversight framework

First, ICT third-party service providers that are critical for financial entities will be designated by the ESAs. The designation process is regulated in Article 28 DORA and will be based on the systemic impact on the stability of the financial system, continuity or quality of financial services in case the relevant CTPP would face a large-scale operational failure. On that basis it can be assumed that mostly larger ICT service providers will be designated, depending on the number of global systemically important banks and insurances relying on their services.

[50] See Article 23 al. 4 aa DORA.

[51] See Article 23 DORA.

[52] FSB report see https://www.fsb.org/wp-content/uploads/P121020-1.pdf. This report examines the provision of financial services by BigTech firms in finance.

In a second step, for each designated CTPP a lead overseer will be appointed. Either EBA, ESMA or EIOPA will oversee the identified CTPPs. Instead of having three acting agencies in this new field it might have been advisable to only appoint one European agency as overseeing body.[53] It will be a challenge to quickly build up competencies and new administrative infrastructures for three agencies. Otherwise, it can probably be assumed that in most cases the EBA will be acting as lead overseer, because banks will be the largest and systemically most relevant group of clients of CTPPs.

3.4.2 The oversight process

The lead overseer will be in the position to request relevant information, conduct general investigations and to address recommendations to the CTPP.[54] CTPPs need to ensure that they do not pose undue operational risks for the financial sector and comply with basic ICT requirements. CTPPs need among others to ensure the security, availability and continuity of services provided to financial entities.[55] The lead overseer will also assess the physical security, the risk management process, governance arrangements, mechanisms for data portability and testing programs of ICT systems. Although the powers seem to be extensive the lead overseer could follow a risk-based approach and focus on critical and important functions of CTPPs and evaluate the potential level of systemic risk. Not all outsourced tasks have the same level of risk.[56]

After the assessment the lead overseer will issue recommendations to the CTPP. While recommendations will be issued by a European body, national competent authorities will be responsible for following them up.[57] The national financial supervisory authorities shall inform relevant financial entities of the risks identified in the recommendations. The competent authorities will also be able to take actions against their supervised financial entities when the recommendations are not endorsed by the CTPP. As a measure of last resort competent authorities will have the right to require the supervised financial entities to temporarily suspend the use or deployment of a service provided by their CTPP until the risks identified have been addressed or where necessary to terminate their contracts with the CTPP concerned.[58]

Although the regulatory supervisory intervention in relation to CTPPs still takes place indirectly through the regulated financial entities using their services, the oversight regime is a big step forward to better monitor potential risks stemming

[53] ENISA as a horizontal European Agency does not have the mandate for executive powers.

[54] See Article 31 DORA.

[55] See Article 30 al. 2 DORA.

[56] The Proposed Interagency Guidance on Third-Party Relationships issued in 2021 by the US Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) offers for instance a framework based on sound risk management principles, https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210713a1.pdf.

[57] See Article 37 DORA.

[58] See Article 37 al. 3 DORA.

from BigTechs, including potential concentration and contagion risks that could impact the financial system.

4 Conclusion

The timing for DORA could not be better. The cyber threat situation is alarming, not only for the financial sector. DORA's main emphasis is to prevent or at least to better mitigate rising cyber threats in the financial sector. To achieve this goal the DORA framework sets the right priorities on ICT governance, reporting and testing. Although some parts of DORA are quite prescriptive, the risk-based approach of DORA will lead to a balanced application of the requirements. Some parts of the regulatory framework, such as incident reporting deadlines have still to be developed by the ESAs in the form of common regulatory technical standards. These standards should put emphasis on providing better guidance for financial institutes. The European oversight framework on critical ICT third-party service providers is the right answer to the ongoing trend of financial entities to outsource their IT infrastructure. If this oversight model is successful, it could have a pioneering role for other sectors.

Conflict of interest D. Clausmeier declares that he has no competing interests. The author is a deputy head of division at the German Federal Finance Ministry. All views and opinions expressed in this article are those of the author.

References

1. Clausmeier D (2020) Die Umsetzung der NIS- und PSD-II-Richtlinien in Deutschland: Doppelte Meldewege für die Finanzindustrie bei schwerwiegenden Cybervorfällen, Wertpapiermitteilungen (WM), p 1397
2. Ferstl M (2009) Aufsichtsrechtliche Besonderheiten für Kredit- und Finanzdienstleistungsinstitute. In: Bräutigam P (ed) IT-Oursourcing Berlin, p 621
3. Kian B (2016) Cloud Computing Baden-Baden
4. Kipker D-K, Beucher K, Fromageau M (eds) (2020) Cybersecurity München
5. Sievers T (2021) Proposal for a NIS Directive 2.0. Cybersecur Law Rev 2(2):223
6. Stevens J (2021) Regelungsvielfalt im IT-Sicherheitsrecht. Comput Recht (cr) 37(12):841
7. Streinz R (2019) Europarecht München
8. Ülgen S (2016) Governing Cyberspace. Washington DC