Position Paper

Bitkom Position Paper on the Proposal for a Regulation on Digital Resilience for the Financial Sector (DORA)

2020 October 16

Introduction

By publishing the Digital Finance Package, the EU Commission has provided an unprecedented cornerstone with regards to the harmonization and digitization of EU's financial markets. Bitkom welcomes the package that builds upon developments during recent years and approaches an increasingly diverse market with the needed depth and scrutiny to achieve the goals of a) building an ecosystem of trust that promotes innovation and b) ensuring the interests of consumers by relying on high security standards.

Bitkom appreciates the opportunity to comment on the Digital Finance Package and is committed to partake in the political and societal discourse during the legislative processes in the upcoming months. As the first milestone on the way to a revised legislative financial ecosystem, we value the recently published proposal for a regulation on digital resilience for the financial sector, and we appreciate the opportunity to share our first perception and general positions with the German Ministry of Finance at an early stage of the legislative process.

Proposal for a Regulation on Digital Resilience for the Financial Sector (DORA)

As in past years, Bitkom strongly endorses the EU in its efforts to substantially and sustainably strengthen the resilience of networks and systems against cybersecurity risks across Europe. We welcome the integrated approach of targeting the entire financial services eco system along the value chain, i.e. widening the scope to ICT third party service providers, such as cloud service providers. With clear standards and responsibilities for and among market participants as well as supervision, respectively, also lies the opportunity to increase scalability for infrastructure service providers.

Implementing EU-wide security standards as well as harmonized testing and reporting structures are critical to deepen the harmonization of the European Digital Single Market, i.e. to avoid market fragmentation and to tackle challenges for cross-border service providers. Eradicating national inconsistencies with regards to the implementation of security standards or supervision will be key to drive EU-wide innovation. We welcome that DORA sets out to become the central reference document for ICT security in the financial sector. According to the proposal, DORA will not impact the NIS Directive but rather build on it and address possible overlaps via a *Lex Specialis*. In this context, we

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Kevin Hackl
Digital Banking & Financial Services
P +49 30 27576-126
k.hackl@bitkom.org

Sebastian Artz
IT Security
P +49 151 27631531
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

have to explicitly highlight the importance of a seamless interplay between the DORA and NIS regulation – any kind of double regulation must be avoided.

Overall, Bitkom is in strong support of the EU Commission's idea of reaching an optimum equilibrium between setting security standards and increasing innovation-friendliness while adhering to the principle of technological neutrality. Having said this, we would like to comment on some aspects of the regulation in greater detail.

Specific Remarks

At this stage, we consider the draft being highly elaborated on processual matters while lacking some clarity with regards to security obligations, testing requirements, reporting mechanisms, and outsourcing for financial service providers and third parties. Please find below our thoughts and comments on particular sections of the legislative proposal:

Art 11(3): the proposal states that "financial entities shall use ICT systems that have an operating environment different from the main one, that is not directly connected with the latter". A backup system, however, needs to be directly connected to the main system to e.g. replicate data. The wording "operating environment different from main one" should be more precise. It should be clear that a second location from the same entity is fulfilling this requirement.

Art 17-20: **on streamlining ICT-related incident reporting and addressing overlapping reporting requirements:** we welcome the intention that the European Commission wants to streamline and harmonize reporting duties which would be highly beneficial to the eco-system. Financial service providers are currently bearing high costs due to fragmented member states provisions. Where/if new reporting structures apply, it should be ensured that no "double reporting" increases the existing burden.

Art 21 (4) on general requirements for the performance of digital operational resilience testing: the proposal states that "[f]inancial entities shall ensure that tests are undertaken by independent parties, whether internal or external". From our perspective, there must be a possibility that tests are to be performed by the staff operating the system. We thus suggest exchanging the term "undertaken" by "overseen".

Art 22 (1) on Testing of ICT tools and systems: the listed methods are lacking the needed clarity as definitions and distinctions are missing.

Art 23 (3, 4) and Article 24 on threat led penetration testing: we appreciate that testing methods like "penetration testing" and "red team testing" are foreseen in the proposal. The proposal states that "[c]ompetent authorities shall identify financial entities to perform threat led penetration testing in a manner that is proportionate to the size, scale,

activity and overall risk profile of the financial entity". Large scale threat led penetration testing is not only a costly but also potentially threatening to a financial institution's critical infrastructure – the worst-case scenario: breakdown of an entire critical infrastructure environment. With regards to ICT third party providers, it needs to be understood that testing for a single financial services unit may harm and impact other financial service providers given the multi-tenant environment.

We welcome that the proposal's Explanatory Memorandum states that "[t]he proposed rules do not go beyond what is necessary in order to achieve the objectives of the proposal". However, the qualitative and quantitative criteria have to be evaluated carefully, given that different companies have different sizes and inherent risk exposures. A "one-size fits all" approach may disproportionally increase the burden for certain companies.

A careful risk-based approach shall thus clarify what entities and what parts of an entity apply for threat led penetration testing. Qualified testers reduce the risks of tests: in Germany, for instance, the Federal Office for Information Security runs a certification program for pen testers. However, testing capacities are limited and appropriate external testers are lacking, which is why it should be explicitly allowed for a financial entity to perform e.g. thread led penetration tests by itself, if certain criteria are met (e.g. Art 24 a) and b)). As financial entities' IT architectures are very heterogeneous and sometimes very complex, it would be very inefficient to rely solely on external service providers. This holds also true for other advanced security testing methods. From our understanding of the proposal, the European Commission does not explicitly forbid firms to use their internal resources to test their systems themselves. Yet, we kindly ask the European Commission to explicitly allow for it and define the terms and conditions.

Art 25(8) on general principles contractual arrangements on the use of ICT services: the wording "ensure that contractual arrangements on the use of ICT services are terminated" appears too strict and does not represent a risk-based approach, especially as a "lead overseer" (article 30f.) "shall assess whether each critical ICT third-party service provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks which it may pose to financial entities". Financial entities shall thus be required to evaluate the possibility of termination in case of contractual breaches, but should not be required to automatically do so, especially when there is a prospect for remedy.

Art 27(2)h-i on ICT third-party provider should be obliged to make high risk evidence available: for high risk evidence, e.g. non remedied vulnerabilities, ICT third-party provider has legitimate interest maximize security and impede the spread of information, e.g. by means of a secure reading room and keep copy in there that customers can access whenever required.

Art 31 (1) iv on Conditions on sub-outsourcing in third countries are disproportionate: in general, we support the Commission's approach but the current state of the proposal would mean that financial entities cannot outsource any critical functions to ICT provid-

ers, as long as they cannot ensure that there is no sub-outsourcing to third countries. This is not proportional and would effectively rule out outsourcing for critical functions and may impact the quality and number of services a global ICT provider can provide to its EU based clients vs. how it services clients outside the EU. Thus we suggest not ruling out subcontracting to third countries under the precondition that existing European laws, in particular GDPR, data storage, and the respective financial services regulation, are met. In this context, we would also like to suggest to build upon existing guidelines for outsourcing (such as by EBA, EIOPA or ESMA's draft guidelines) and not introduce additional or conflicting guidelines.

Art 34 and 35 on the inspection and oversight of ICT third party provider: Requirements that may seem appropriate for a certain type of provider may not be suitable for others. For instance, the provision that would require providers to give hardcopies of records and procedures (Article 34.2.b) as well as the ability to seal premises (Article 35.2) would not be suitable to a cloud environment as this could compromise the highly secure environment inherent to this type of provider.

Art 37 (3) on the request to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party: this section lacks the focus of needed exit plans and transition phases. Thus the section should be amended to consider and assess specific exit plans and timelines per service, ensuring a safe transition before a specific service is suspended. Putting the use of an ICT third-party or certain services to a sudden halt may heavily impact a financial institution's operations which rely on a functioning third party infrastructure. Furthermore, risk-mitigating measures implemented by the outsourcing financial institution should be considered in the competent authority's decision as to whether a suspension or termination is actually required.

Art 40 on information sharing arrangements among financial entities: we welcome the take on enabling cooperation among financial entities but also want to point out the importance of confidentiality to rule out operational as well as reputational risks.