bitkom

At a glance

DORA – Regulation on Digital Operational Resilience for the Financial Sector

Bitkom's view

Bitkom supports the EU's efforts in strengthening and harmonizing ICT security and digital resilience of financial services across Europe. We welcome the holistic approach targeting the financial services eco system along its entire value chain, including critical third-party providers (CTPPs). According to Bitkom, this allows to (a) allocate responsibilities among market participants across the value chain more efficiently and (b) facilitate scalability for CTPPs. In the light of ongoing negotiations, we ask to put the focus on resolving existing issues from the EU Commission's proposal rather than adding further complexity, which may run contrary to the very goals of DORA.

Core points

- **Criticality, Proportionality, and Scope**

  It is necessary to point out that DORA should exclusively focus on actual ICT risk. Whilst ongoing negotiations on criticality appear to be highly elaborated on processual matters – the HOW –, the WHAT, i.e. definitions of criticality, remains somewhat vague and the boundaries between critical vs. non-critical are blurred. Widening the scope of DORA, moreover, bears the risk of adding further legal uncertainties.

- **Overlaps with other regulations**

  The need for clarifying the lex specialis approach: Bitkom appreciates the approach of DORA to introduce a single rulebook to overcome fragmentation caused by diverging ICT frameworks at member state level. However, both financial entities as well as CTPPs are subject to other horizontal and sectoral regulation. Particularly the NIS(2)-Directive as well as the CER-Directive need more clarity, given that diverging national implementation laws bear the risk of creating regulatory uncertainties.

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

2021-May-21

Introduction

Bitkom supports the EU's efforts in strengthening and harmonizing ICT security and digital resilience of financial services across Europe. As outlined in our initial position paper on the EU Commission's proposal for a regulation on digital resilience for the financial sector (DORA), we welcome the holistic approach targeting the financial services eco system along its entire value chain. In fact, we believe that widening the scope to critical ICT third party providers (CTPPs) when dealing with digital resilience and cybersecurity threats provides the opportunity to (a) allocate responsibilities among market participants across the value chain more efficiently and (b) facilitate scalability for CTPPs. In doing so, DORA bears the potential to accelerate innovation and elevate security levels.

Having been following the developments regarding the EU Commission's proposal on DORA very closely, we want to take the opportunity to once more provide an assessment on current developments and contribute to the discussions with the EU Commission, the Council, as well as the European Parliament. Whilst we have seen substantial progress among key negotiators that is expected to render DORA more precise and clear, we have also observed certain developments that put the essence of DORA at risk. Thus, Bitkom invites the Council as well as the European Parliament to take the ensuing considerations into account in order to avoid market fragmentation and to tackle obstacles for financial entities as well as CTPPs, especially those operating across different geographies.

To attain a successful DORA proposal, it is essential to recalibrate the negotiators' focus on resolving and refining the EU Commission's initial proposal. Whilst this is definitely happening to a certain degree, we also observe that new issues are being brought to the table, e.g. by widening the scope of the proposal. According to Bitkom, adding complexity to the DORA proposal will much likely cause unintended, negative side effects. Against the background of an ambitious time frame, which Bitkom generally supports, the EU runs the risk of eventually undermining the very goals of DORA. Therefore, we ask to put the focus on resolving existing issues from the EU Commission's proposal rather than adding

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 +49 175 5848805
k.hackl@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

complexity. In that respect and to put it into entrepreneurial terms: Bitkom asks the Council and the European Parliament to focus on building a feasible regulatory MVP which maintains and furthers the competitiveness of European financial markets and their cybersecurity standards.

Specific Remarks and Key Considerations

Criticality, Proportionality, and Scope: It is necessary to point out that DORA should exclusively focus on actual ICT risk. Whilst ongoing negotiations on criticality appear to be highly elaborated on processual matters – the HOW –, the WHAT, i.e. definitions of criticality, remains somewhat vague and the boundaries between critical vs. non-critical are blurred. Article 28 DORA, for instance, falls short in providing concrete thresholds upon which criticality is to be assessed by the ESAs. In the ECON draft report – Amendment 87 (Article 27 (2b)) – a proper differentiation between critical and non-critical TPPs is even completely missing. Overall, Bitkom supports a risk-based approach that relies on financial entities identifying and managing risk and does not cause information overflow on the ends of supervisory bodies. Applying a more risk-based approach would also help to resolve the issue of proportionality. Instead of size, risk-profiles should be the key metric to assess whether an entity shall fall under DORA.

In general, widening the scope of DORA, e.g. inclusion of payment infrastructures, hardware-as-a-service, or the reporting of "significant cyber threats", which lack adequate legal definitions, creates uncertainties in the market and causes new interdependencies which would need thorough analysis. Such additions to DORA are likely to be rendered counterproductive as they introduce additional complexity. Given the quite progressed stage of the decision making process we ask to focus on resolving the issues stemming from the EU Commission's proposal rather than adding "last mile complexity". Those legal uncertainties open the door for supervisory fragmentation.

We understand that currently discussed additions to the scope of DORA stem from the idea of trying to keep regulations up-to-date and future-proof. In our view, shorter review cycles for targeted adjustments of regulatory technical standards (RTSs) can help overcome this issue allowing to solve certain aspects with sufficient regulatory due diligence and the needed ongoing dialogue with market participants.

Overlaps with other regulations and the need for clarifying the *lex specialis* approach: Bitkom appreciates the approach of DORA to introduce a single rulebook to overcome fragmentation caused by diverging ICT frameworks at member state level. However, both financial entities as well as CTPPs are subject to other horizontal and sectoral regulation. Defining the *lex specialis* approach more stringent is thus crucial to overcome fragmentation and overlaps, particularly with the NIS(2)-Directive and CER-Directive.

Diverging national implementation laws of those directives bear the risk of creating regulatory uncertainty, hampering cross-border service distribution, and fueling regulatory arbitrage. Thus, the *lex specialis* approach should not only be mentioned in the recital of DORA but also in the legal text. Moreover, we suggest deleting the phrases "and where those requirements are at least equivalent in effect to the obligations laid down in this Directive", in NIS(2) (recitals (12), (13) and in Article 2(6)) and CER (Article 1(3)). This wording could lead to further fragmentation if the assessment was undertaken on national levels.

Moreover, Bitkom wants to point out that financial entities performing more than one financial function may be subject to multiple NCAs. For those entities it would be favorable if one NCA was designated to receive incident reporting or to at least ensure that forms and deadlines are aligned. Such alignment efforts are ideally also taken across member states to facilitate the uptake of cross boarder services. In addition to the financial entities, CTPPs (particularly those that are operating in a multi-tenant environment) face the challenge of operating "across" different authorities and geographies, which is why we suggest limiting DORA's supervisory powers over CTPPs to services critical to financial entities. Additionally, cooperation and coordination from the Lead Overseer not only with the Oversight Forum but also with other relevant competent authorities should be enforced. In the long run, Bitkom believes that DORA bears the potential to serve as blueprint for other sectors to manage ICT risk across value chains, facilitate access to/scalability of CTPPs, and eventually increase harmonization.

Sub-Outsourcing and Intra-Group Outsourcing: Selecting and on-boarding sub-contractors can take up to 24 months of due diligence and training for financial entities as well as ICT CTPPs. The established value chain between financial entities and ICT CTPPs is essential to uphold and guarantee business continuity. Under Article 31 DORA, the Lead Overseer is granted broad powers to request changes to subcontracting arrangements – including the termination of contractual arrangements – without any clear set of criteria. Those can be defined in the form of RTSs to ensure business continuity but the level 1 text must already provide a sufficient basis to do so.

The need for a multi-vendor strategy as foreseen in DORA (Article 5(9g)) should take into account the strategy, risk appetite, and risk assessment undertaken by a financial entity and not be required per default. Depending on the operational requirements of entities, they should be able to assess whether a multi-vendor strategy is appropriate. In this context, we would like to point out that an increased number of vendors will not just incur additional cost, but also add complexity to the IT estates as well as the risk and control frameworks financial entities need to have in place. Moreover, such an approach would undermine supervisory expectations – ECB included – to reduce the complexity of financial entities' organizational and IT infrastructures.

Harmonized requirements for testing: Bitkom welcomes the wording included in Recital 44 in the ECON draft report. A DORA testing regime should not come in addition to and should not be independent from the requirements on advanced testing included in the existing frameworks such as the TIBER-EU framework, as specified in the draft report. This will help avoiding any additional compliance costs which firms would incur as a consequence of having to fulfill duplicative requirements on testing. However, this does not mean that TIBER-EU should replace general threat led penetration testing (TLPT) in the long run as not all entities are obliged to fulfill these requirements due to proportionality. We also welcome the clarification in the ECON draft report that TPPs should be able to conduct their own pen-testing in case of client agreement and the provision of sufficient documentation. However, it is unclear why a TPP would need to enter into such testing contracts "on behalf of their clients". This constitutes a far-reaching intervention into contractual freedom, raises significant legal questions and may interfere with situations where a financial entity would not want the TPP to conduct separate testing.

Implementation timeline: DORA shall apply 12 months after entering into force. Bearing in mind that DORA contains more than 20 legal bases for RTSs to be developed and consulted by the ESAs as well as adopted by the Commission, the chosen implementation timeline is too short. According to the current draft of DORA, RTSs could be finalized 12 Months after DORA entering into force, meaning that there is not any time left for the industry to implement the RTSs and to amend contracts with CTPPs. Contrary to initial views, RTSs will not merely be a transposition of existing EBA-Guidelines but an introduction of a considerable amount of new requirements, creating significant implementation efforts. We therefore propose that DORA shall apply 12 months after all RTSs are adopted by the Commission.

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
Recital on international alignment (new) – The inclusion of a recital to clarify that the EU intends to cooperate with international regulatory authorities on harmonizing requirements and guidance on advanced testing frameworks would be beneficial.		
N/A	N/A	**In order to enable a smooth implementation of the requirements included in this Regulation and support those financial entities that operate across borders and in different jurisdictions, the Commission shall promote the cooperation with international regulatory Authorities on harmonising requirements and guidance on advanced testing frameworks.**
Amendment Article 3(51) (new) – The inclusion of a specification on how to define intragroup structures by using the definition in accordance with paragraph 11 of Article 2 of Directive 2013/34/EU in combination with recital 31 would be necessary.		
N/A	NA	**Intra-group relations should be differentiated via the shareholder structure in accordance Article 2 and Recital 31 of Directive 2013/34/EU.**
Amendment Article 5 (9g) – Deletion of a "multivendor strategy": As outlined above, a multi-veondor strategy should not become the default option but should take into account the risk assessment carried out by a financial entity. Thus, we are in support of the ECON draft to delete Article 5(9g). Alternatively, "multi-vendor strategy" should be replaced by "vendor strategy"		
The ICT risk management framework referred to in paragraph 1 shall include a digital resilience strategy setting out how the framework is implemented. To that effect it shall include the methods to address ICT risk and attain specific ICT objectives, by: [...] (g) defining a holistic ICT multi-vendor strategy at entity level showing key dependencies on ICT third-	The ICT risk management framework referred to in paragraph 1 shall include a digital resilience strategy setting out how the framework is implemented. To that effect it shall include the methods to address ICT risk and attain specific ICT objectives, by: [...] ~~(g) defining a holistic ICT multi-vendor strategy at entity level showing key dependencies on ICT third-~~	The ICT risk management framework referred to in paragraph 1 shall include a digital resilience strategy setting out how the framework is implemented. To that effect it shall include the methods to address ICT risk and attain specific ICT objectives, by: [...] ~~(g) defining a holistic ICT multi-vendor strategy at entity level showing key dependencies on ICT third-~~

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
party service providers and explaining the rationale behind the procurement mix of third-party service providers	~~party service providers and explaining the rationale behind the procurement mix of third-party service providers~~	~~party service providers and explaining the rationale behind the procurement mix of third-party service providers~~
Amendment Article 11(3) on backup systems – A clarification of the requirement to use ICT systems that have an operating environment different from the main one and aligning the wording to the PFMI Guidance on cyber resilience for financial market infrastructures seems appropriate.		
3. When restoring backup data using own systems, financial entities shall use ICT systems that have an operating environment different from the main one, that is not directly connected with the latter and that is securely protected from any unauthorized access or ICT corruption. For financial entities referred to in point (g) of Article 2(1), the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.	3. When restoring backup data using own systems, financial entities shall use ICT systems that have an operating environment different from the main one, that is not directly connected with the latter and that is securely protected from any unauthorized access or ICT corruption. For financial entities referred to in point (g) of Article 2(1), the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.	3. When restoring backup data using own systems, financial entities shall use, **if appropriate**, ICT systems that have an operating environment different from the main one~~**, that is not directly connected with the latter and that is securely protected from any unauthorized access or ICT corruption**~~. For financial entities referred to in point (g) of Article 2(1), the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date. **Financial entities shall exercise judgement when carrying out the recovery of the transactions so as to prevent a potential escalation of risks to the recovery operation or its related ecosystem**.
Deletion Article 11(5) – This requirement would create an unlevel playing field for CSDs, as this does not affect any other financial entity in scope of DORA. Further, the other requirements of DORA would provide for a decent level of security for CSDs.		
Financial entities referred to in point (f) of Article 2(1) shall maintain or ensure that their ICT third-party providers maintain at least one secondary processing site endowed with resources,	N/A	~~Financial entities referred to in point (f) of Article 2(1) shall maintain or ensure that their ICT third-party providers maintain at least one secondary processing site endowed with resources,~~

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
capabilities, functionalities and staffing arrangements sufficient and appropriate to ensure business needs.		~~capabilities, functionalities and staffing arrangements sufficient and appropriate to ensure business needs.~~
The secondary processing site shall be:		~~The secondary processing site shall be:~~
(a) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;		~~(a) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;~~
(b) capable of ensuring the continuity of critical services identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;		~~(b) capable of ensuring the continuity of critical services identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;~~
(c) immediately accessible to the financial entity's staff to ensure continuity of critical services in case the primary processing site has become unavailable.		~~(c) immediately accessible to the financial entity's staff to ensure continuity of critical services in case the primary processing site has become unavailable.~~

Amendment to Article 23(2): While the possibility for the TPP to conduct own TLPT activities is an important step towards increasing resilience in a multi-tenant environment, there is no need to grant them the right to legally represent their financial customers when entering into contracts.

EC proposal	ECON Draft Report	Bitkom Proposal
(2) [...] For the purpose of the first subparagraph, financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical functions and services, including functions and services outsourced or	[...] Where the involvement of an ICT third-party service provider in the testing could have an impact on the quality, confidentiality or security of the ICT third-party provider's services to other customers not falling within the scope of this Regulation,	[...] Where the involvement of an ICT third-party service provider in the testing could have an impact on the quality, confidentiality or security of the ICT third-party provider's services to other customers not falling within the scope of this Regulation, the financial entity and the ICT

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
contracted to ICT third-party service providers. Where ICT third-party service providers are included in the remit of the threat led penetration testing, the financial entity shall take the necessary measures to ensure the participation of these providers.	the financial entity and the ICT third-party service provider may contractually agree that the ICT thirdparty service provider is permitted to directly enter into contractual arrangements with an external tester. ICT third-party service providers may enter into such arrangements on behalf of all their financial entity customers in order to conduct pooled testing.	third-party service provider may contractually agree that the ICT thirdparty service provider is permitted to directly enter into contractual arrangements with an external tester. ~~ICT third-party service providers may enter into such arrangements on behalf of all their financial entity customers in order to conduct pooled testing.~~
Deletion of Article 23.4(b i) as it would foresee the ESAs to define the scope of TLPTs in RTS		
4. EBA, ESMA and EIOPA shall, after consulting the ECB and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests, develop draft regulatory technical standards to specify further: [...]; (b) the requirements in relation to: (i) the scope of threat led penetration testing referred to in paragraph 2 of this Article; (ii) the testing methodology and approach to be followed for each specific phase of the testing process; (iii) the results, closure and remediation stages of the testing;	N/A	4. EBA, ESMA and EIOPA shall, after consulting the ECB and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests, develop draft regulatory technical standards to specify further: [...]; (b) the requirements in relation to: ~~(i) the scope of threat led penetration testing referred to in paragraph 2 of this Article;~~ ~~(ii)~~ **(i)** the testing methodology and approach to be followed for each specific phase of the testing process; ~~(iii)~~ **(ii)** the results, closure and remediation stages of the testing;
Amendment to Article 24(1) –Financial entities could be allowed to perform thread lead penetration tests by themselves if the criteria listed in Article 24.1 are met while agreeing with the proposal of the EP Draft report.		
1. Financial entities shall only use testers for the deployment of threat led penetration testing, which:	1. Financial entities **and ICT third-party service providers for the purposes of Article 23(2)** shall only use testers for	1. Financial entities **and ICT third-party service providers for the purposes of Article 23(2)** shall ~~**only use testers for**~~

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
	the	~~**the deployment of**~~ […]
Amendment of Article 25 (8) – Remedies and Contract Termination: To provide some flexibility to the regulated financial entities based on existing requirements instead of mandating the termination requirements		
Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under the following circumstances:	Financial entities shall ensure that contractual arrangements on the use of ICT services are **able to be** terminated**, after all other remedies have been exhausted,** at least under the following circumstances:	Financial entities shall ensure that contractual arrangements on the use of ICT services are able to be terminated**,** ~~after all other remedies have been exhausted,~~ **in line with applicable national law,** at least under the following circumstances:
Deletion of Article 27(2b) – Key contractual provisions on the use of ICT services: To avoid the unintentional ban of third country outsourcing of non-critical services. As non-critical services can also be carried out by CTPPs Article 27(2b) is misleading. The intention proposed in Amendment 95 of the ECON draft report (Article 28(9)) would be sufficient and, thus, allow for the deletion Article 27(2b). Moreover, Amendment 87 would not limit the requirement to CTPPs: given the fact that only 27 (b) is limited to "ICT third party service providers […] designated as critical", 27 (a) would refer to all ICT third parties regardless of the criticality. As a result, third party offerings in the EU could become so expensive that access to innovative technology for EU financial entities could be limited. Especially smaller tech providers which often offer niche products would be affected as well as their European clients.		
the locations where the contracted or sub-contracted functions and services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity if it envisages changing such locations;	The contractual arrangements for the provision of ICT services by an ICT third-party service provider established in a third country shall, in addition to the provisions set out in paragraphs 2 and 2a of this Article: (a) be concluded with a legal entity in the Union of that ICT third-party service provider; and, (b) guarantee that, in the event the ICT third-party service provider is designated as critical pursuant to Article 28(9), the Joint Oversight Executive Body can carry out its duties specified in Article 30	~~The contractual arrangements for the provision of ICT services by an ICT third-party service provider established in a third country shall, in addition to the provisions set out in paragraphs 2 and 2a of this Article:~~ ~~(a) be concluded with a legal entity in the Union of that ICT third-party service provider; and,~~ ~~(b) guarantee that, in the event the ICT third-party service provider is designated as critical pursuant to Article 28(9), the Joint Oversight Executive Body can carry out its duties specified in Article 30~~

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
	on the basis of its competences set out in Article 31.	~~on the basis of its competences set out in Article 31.~~
Amendment Article 27.2(h i) – making sure to have access to the information but not the actual copies		
2. The contractual arrangements on the use of ICT services shall include at least the following: (h)the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes: i)rights of access, inspection and audit by the financial entity or by an appointed third-party, and the right to take copies of relevant documentation, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;	Art. 27.2(a) (new) - 2a. The contractual arrangements for the provision of critical or important functions shall, in addition to the provisions set out in paragraph 2, include at least the following: [...] (b) the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes: i) rights of access, inspection and audit by the financial entity or by an appointed third party, and the right to take copies of relevant documentation, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;	2. The contractual arrangements on the use of ICT services shall include at least the following: (h)the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes: i)rights of access, inspection and audit by the financial entity or by an appointed third-party, and the right to ~~take copies~~ of **consult** relevant documentation, **which shall be made available in a secure, non-proliferating way**, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;
Amendment Article 28.9 – Localization policy: It is crucial to not impose data localization requirements and to follow the intention of the EP draft report.		
Financial entities shall not make use of an ICT thirdparty service provider established in a third country that would be designated as critical pursuant to point (a) of paragraph 1 if it were established in the Union.	Financial entities shall not make use of an ICT third party service provider established in a third country **for a** critical **or important function unless that ICT third-party service provider has a legal entity in the Union and has concluded contractual arrangements in accordance with Article 27(2b).** **The Joint Oversight Executive Body shall, in a recommendation, consider the criticality of third country ICT third-party service providers in accordance with**	Financial entities shall not make use of an ICT third party service provider established in a third country **for a** critical **or important function unless that ICT third-party service provider has a legal entity in the Union ~~and has concluded contractual arrangements in accordance with Article 27(2b).~~** **~~The Joint Oversight Executive Body shall, in a recommendation, consider the criticality of third-country ICT third-party service providers in~~**

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
	paragraphs 1 and 2 of this Article. **The recommendation of the Joint Oversight Executive Body shall be communicated to the legal entity in the Union of the ICT third-party service provider. That legal entity shall have the right to comment on the recommendation in accordance with the second subparagraph** of paragraph **7a.** **Upon designation as critical, all correspondence from the Joint Oversight Executive Body shall be with the legal entity** in the Union **of the ICT thirdparty service provider**.	~~**accordance with paragraphs 1 and 2 of this Article.**~~ ~~**The recommendation of the Joint Oversight Executive Body shall be communicated to the legal entity in the Union of the ICT third-party service provider. That legal entity shall have the right to comment on the recommendation in accordance with the second subparagraph** of paragraph **7a.**~~ ~~**Upon designation as critical, all correspondence from the Joint Oversight Executive Body shall be with the legal entity** in the Union **of the ICT third-party service provider**.~~
Deletion Article 31 (1d)(iv) – This requirement would hinder financial entities use third-country service providers, which is a common practice.		
31(1) For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers: [...] (d) to address recommendations on the areas referred to in Article 30(2), in particular concerning the following: [...] (iv) refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met: - the envisaged subcontractor is an ICT third-party service provider or an ICT sub-contractor established in a third country; - the subcontracting concerns a critical or important function of the financial entity.	31(1) For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers: [...] (d) to address recommendations on the areas referred to in Article 30(2), in particular concerning the following: [...] (iv) refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met: - the envisaged subcontractor is an ICT third-party service provider or an ICT sub-contractor established in a third country **and does not have a legal entity in the Union**; - the subcontracting concerns a critical or important function of the financial entity.	31(1) For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers: [...] (d) to address recommendations on the areas referred to in Article 30(2), in particular concerning the following: [...] ~~(iv) refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met:~~ ~~- the envisaged subcontractor is an ICT third-party service provider or an ICT sub-contractor established in a third country;~~ ~~- the subcontracting concerns a critical or important function of the financial entity.~~
Deletion of Article 37 (4a) (new) – The requirement for an exit strategy is already known from EBA requirements, wherein the authority refrained from introducing any timeframe. It is not fully clear what the provision is trying to achieve or who the addressee is (competent authorities or the CTPPs) and it could lead to a rushed exit which may create new operational risk. If the intention behind the		

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
proposal is to ensure that financial entities have sufficient time to execute their exit strategies, no timeframe should be referenced as supervisory practice may lead to using the minimum timeline as a benchmark. If the intention is to ensure that financial entities initiate their exit strategies without undue delay, we suggest replacing the word "execute" with "initiate" to avoid any misinterpretation. If kept, the timeline should be extended to 90 days.		
N/A	31 (4a): The decisions provided for in paragraph 3 shall only be implemented once all affected financial entity customers have been duly informed. The affected financial entity customers shall be afforded at least 30 calendar days to conclude and operationalise alternative arrangements, and to execute their exit strategies and transition plans referred to in Article 25. The critical ICT third-party service providers subject to the decisions provided for in paragraph 3 of this Article, shall fully cooperate with their financial entity customers.	~~31 (4a): The decisions provided for in paragraph 3 shall only be implemented once all affected financial entity customers have been duly informed. The affected financial entity customers shall be afforded at least 30 calendar days to conclude and operationalise alternative arrangements, and to execute their exit strategies and transition plans referred to in Article 25.~~ ~~The critical ICT third-party service providers subject to the decisions provided for in paragraph 3 of this Article, shall fully cooperate with their financial entity customers.~~
Amendment Article 44.4 – It seems appropriate to apply the measures mentioned in a commensurate way corresponding to the breaches to DORA		
44(4): Member States shall confer on competent authorities the power to apply at least the following administrative penalties or remedial measures for breaches of this Regulation: (a) issue an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct; (b) require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that	44(4): **Powers are conferred on the Joint Oversight Executive Body and on relevant** competent authorities to apply at least the following administrative penalties or remedial measures for breaches of this Regulation: (a) issue an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct; (b) require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation	44(4): Member States shall confer on competent authorities the power to apply at least the following administrative penalties or remedial measures for breaches of this Regulation: (a) issue an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct; (b) require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that

Suggested Amendments to DORA

EC Proposal	ECON Draft Report	Bitkom Proposal
practice or conduct; (c) adopt any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements; (d) require, in so far as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and (e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.	and prevent repetition of that practice or conduct; (c) adopt any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements; (d) require, in so far as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and (e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.	practice or conduct; (c) adopt any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements; (d) require, in so far as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and (e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach. **The application of the aforementioned measures shall be commensurate with the extent of the breaches to this Regulation.**

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.