28 April 2021

EBF Position Paper on the European Commission's proposal for a Regulation on digital operational resilience for the financial sector (DORA)

COM (2020) 595 final

KEY MESSAGES

- The EBF calls for a risk-based approach and the consistent application of the proportionality principle across DORA consistently. (p. 8; p. 22; p. 23)
- The EBF calls for a fully harmonized cyber incident reporting framework. (p.16)
- The EBF calls for an EU-wide mutually recognized digital operational testing framework. (p.19)
- The EBF calls for an alignment of DORA's requirement for financial entities with existing supervisory guidance under the EBA guidelines on outsourcing and ICT and security risk management. (p. 23)
- The EBF emphasizes the need for close attention to the implicated additional burden for critical third-party providers' (CTPPs) customers under the proposed oversight framework. Access to innovation must not be detrimentally limited due to disproportionate obligations and limits for the provider selection. (p. 23, p.29)
- The EBF understands an appropriately designed oversight framework for CTPPs to be of added value for TPP customers. (p. 30)
- The EBF emphasizes that termination of the contractual arrangement by the competent authority should not be a standard enforcement tool, since it carries significant risk. (p. 31)
- The EBF calls for enabling the establishment of meaningful and voluntary cyber threat information-sharing arrangements among trusted circles. (p. 35)
- The EBF believes that the numerous Regulatory Technical Standards (RTS) delegated to the ESAs should not be too prescriptive, providing flexibility in the measures they adopt. (p.37)

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

INDEX

INTRODUCTION

The adoption of innovative technology by European banks requires a balance between a reliable and consistent framework of financial regulation and flexibility to adapt to changing business models. The inherently cross-border nature of digital service solutions needs to be addressed by banks, regulators, and digital service providers on a common ground, looking for the secure facilitation of financial service innovation across Europe. An appropriate and harmonized pan-European legal framework is key to facilitate adoption of innovative technology.

Consequently, the EBF welcomes the European Commission's aim to enhance operational resilience in Europe. The financial industry's own considerations will benefit from more harmonized ICT-related rules at the European level, aligned with the existing supervisory framework today. Detrimental fragmentation of the regulatory framework should be avoided, addressing risks consistently and proportionately across European jurisdictions without hampering the financial industry' ability to apply innovative services.

With this position paper, the EBF addresses the proposal for a Regulation on digital operational resilience for the financial sector, as published by the Commission in September 2020[1]. EBF positions in this document continue from established EBF key messages in the same year and build on the EBF consultation response to the Have-you-say procedure in February 2021. Concrete amendments aim to support the EU legislator, striving for proportionality and suitable ICT-related requirements. While the amendments not yet pick up on currently emerging compromise amendments by European Parliament and Council, they deliver the foundational understanding and positions of the European banks. Resting on the latter, the EBF will continue further analysis and engage in advocacy with EU institutions and stakeholders. Offering its expertise throughout the moving legislative process and reflecting on relevant questions in the advancing debate, the positions in the paper will guide the European banks' assessment of future amendments from institutions and stakeholders.

CHAPTER I: GENERAL PROVISIONS

A) Scope

Article 2: Being part of the financial services industry, consumer credit providers and intermediaries, as well as mortgage credit providers and intermediaries should be included in the scope of Article 2, based on the "same activity, same rules and same supervision" principle. This would also help to meet the overall aim of the DORA regulation – to increase cyber resilience across **the whole financial ecosystem**. To reflect a harmonized approach with PSD2, we propose the following amendment:

Art. 2 (1) (b) and (c) combined into new (b)

> ***"(b) ~~payment institutions~~ payment service providers as defined in Art. 1 (1) Directive 2366/2015 (PSD2)"***

[1]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

~~(c) electronic money institutions~~"

Additionally, creditors and credit intermediaries should be referenced by new *Art. 2 (1) (v) and (w)*

> ***"(v) Creditors, Credit intermediaries and appointed representatives providing credit agreements for consumers relating to residential immovable property under DIRECTIVE 2014/17/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 February 2014 on credit agreements for consumers relating to residential immovable property,***
>
> ***(w) Creditors and credit intermediaries providing credit agreements for consumers under DIRECTIVE 2008/48/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2008 on credit agreements for consumers."***

The EBF also notes that the implementation times of the proposal are unrealistic and that there are inconsistencies in the timetable for bringing the financial sector into conformity with the DORA stipulations, as it foresees a period of one year to comply with the regulation while the RTS are to be developed within 1 to 3 years after its entry into force. In order to ensure consistency of the different timelines and regulatory certainty needed for implementation and compliance, the EBF proposes that **this Regulation's provisions shall apply after a reasonable amount of time has passed after the publication of the RTS** (see also comments under Chapter IX).

B) Definitions

In general, there are number of terms in DORA which are undefined or the interaction of which creates confusions, for example the use of "information asset", "information" and "data" in chapter II. The text should be reviewed to ensure continuity, coherence and clarity of the terms and definitions used throughout.

The EBF also suggests mirroring the ISO 27000 definitions or other standards referred to in paragraph 258 of EBA Guidelines and methodologies for the supervisory review and evaluation process (SREP) EBA/GL/2014/13, to the extent possible.

Article 3 (7): We believe the definition of "major ICT-related incident" is too broad and will lead to significant over reporting of non-major incidents. The use of the word "potentially" creates a hypothetical that firms will not be able to predict, especially within the timelines currently required by DORA Article 17. In order to avoid breaching requirements firms will inevitably over report a significant number of non-major ICT-related incidents. This will reduce the value of the regime for supervision and create significant burden for firms. To correct this the phrase "with a potentially high" should be replaced by "likely to have a significant".

Article 3 (15 – 16): The current text **does not differentiate between ICT outsourcing arrangements as per the EBA Outsourcing Guidelines and one-off purchase of ICT services.** The "ICT Services" definition is very broad and generic, as it

does not distinguish between temporary services and continuative services. For temporary services and/ or planning, DORA provisions could be excessive and unnecessary, and they should be excluded from the scope. Furthermore, the perimeter of the ICT services is not aligned with the definition of service laid down in the EBA GLs on outsourcing rules. It does not foresee the same exclusions such as the provision of data that the DORA text explicitly mentions under the ICT services definition. Also, DORA does not exclude maintenance under license and telecommunications, which should also be excluded as they pertain more to licensing agreements than service ones.

The above would lead to a situation in which banks would have to undertake extensive due diligence and agree access and audit rights with providers of datasets or off-the-shelf software.

Where an ICT service provider is under oversight or supervision due to existing financial regulation, the introduction of an additional mandatory requirements does not enhance its risk mitigation capabilities. This is the case for **intra-group outsourcing of ICT services in banking groups. These entities are already subject under the scope of financial regulation. Their operational resilience risks are addressed and supervised. Consequently, they should not be covered by DORA**. **European banks welcome an explicit reference under DORA, acknowledging the differences in regard to risk by intro-group constellations. Governance and control within a group establish a very different setup from external ICT third-party service providers. Requirements of Chapter V should therefore not apply.** Different from external third-party providers, these entities are already subject under the chain of financial regulation and respective supervision processes. Risks to operational resilience are therefore not unaddressed and – in turn – no gap needs to be closed by DORA. For constellations including bank group structures inside and outside the EU, the group's dedication to comply with EU regulation today is already advancing operational resilience and operations in line with EU law. An introduction of additional mandatory governance requirements for such intra-group constellation would not add additional security, but rather increase regulatory workload by an additional rule set that may overlap or duplicate existing requirements.

To include the important differentiation of risk associated with external ICT provider vs. intra-group- providers, the following recital should be included under DORA:

Recital 25 a (new):

> **"Since the DORA initiative aims to fill gaps in rules on ICT risk and to introduce missing financial subsector legislation, existing regulatory approaches for ICT-relevant provider constellations – established already at EU level with harmonizing effect for financial entities – need to be considered to determine the scope of this initiative. Where ICT providers are not external operators but are established within a financial group, their particular risk profile should be taken into consideration for a risk-based application of the requirements in Chapter V in order to not prevent financial entities from efficient organisation and management of operations.**
>
> **The potential risk of the intra-group ICT service agreement is significantly different compared to the use of external ICT third party**

service providers for various reasons, predominantly due to their inclusion in the financial entities' governance and control framework or – in numerous cases – them being subject to financial supervision themselves. DORA aspires to address challenges of ICT risks under operational resilience, performance, and stability of the Union financial systems. Where intra-group providers are already operating under the financial services regulatory framework, legislative requirements, stability safeguards, performance measures and resilient processes are already established and monitored. In light of the proportionality principles, no duplicating or diverging requirements shall be established by DORA. Requirements such as Chapter V – in particular the oversight mechanism under Chapter V Section II - shall not apply to intra-group providers."

Art. 3 (17): The definition of "critical or important function" needs to be further aligned with the existing definition under EBA Guidelines on outsourcing section 4 para. 29 to 31. In particular, the EBA definition puts forward factors that should be considered for the designation (para. 31 a. to j.). Art. 3 (17) should pick up on these factors.

Article 3 (18): To include the correct editorial reference, the mentioned Art. 29 needs to be changed to Art. **28**. While Art. 28 addresses the designation of CTPPs, Art. 29 offers requirements for the structure of the oversight framework.

> *"'critical ICT third-party service provider' means an ICT third-party service provider designated in accordance with Article ~~**29**~~ **28** and subject to the Oversight Framework referred to in Articles 30 to 37;"*

The definition of critical third-party providers is an important gateway to target DORA's new regulatory safeguards (oversight) properly to those providers that currently are not addressed by EU level oversight. Intra-group ICT providers should not be considered to fall within this definition. To avoid this legal duplication, European banks propose an exclusion within Art. 28 (1) to reflect this, aligning DORA's approach with the proposed Recital 25 a new above.

Art. 28 (1) new letter c):

"c) the designation mechanism referred to in point (a) and (b) of paragraph 1 shall not apply in relation to intra-group ICT third party service providers."

This amendment prevents detrimental duplication of rules for intra-group subsidiaries, ultimately avoiding a disproportionate burden for European banks. Art. 28 (2) (a) to (f) do not sufficiently exclude the designation of an intra-group ICT provider as critical.

This amendment accompanies the EBF's call for inclusion of a Recital 25 a new (see above), intra-group ICT providers under in light of the DORA aspirations more generally.

Article 3 (20): We welcome clarification on what the criteria "has entered into a contractual arrangement either with an ICT third-party service provider, or with an ICT third-party service provider established in a third country" entails.

CHAPTER II: ICT RISK MANAGEMENT

The EBF calls for a risk-based approach and the consistent application of the proportionality principle in the ICT Risk Management provisions (Articles 4 – 14)

While the EBF welcomes the intention in the proposed Regulation to set a harmonised set of ICT risk management requirements for financial services firms operating in the EU, **the current text of the proposal is at times too prescriptive**. **Firms need the space to demonstrate capabilities and outcomes in order to allow for innovation, an evolving threat landscape, and changes in best practice.** The proposed requirements should not lock in practices that may soon be out of date, **thereby resulting in legislation that is not sufficiently future-proofed.** In line with the proportionality principle, any **additional requirements** should **only be used in a very targeted manner** in order to close clearly identified gaps. Greater emphasis on the capabilities expected of firms rather than how firms should achieve those capabilities would both give firms flexibility as well as allow regulators to exercise a greater level of proportionality.

The relevant articles in ICT risk management have a large focus on "all", e.g. "all processes", "all accounts", "all legacy ICT systems". This creates disproportionate efforts without any clear benefit for supervisory authorities, conflicts with a risk-based approach and even contradicts the Commission's aim to "[reduce] regulatory complexity, [foster] supervisory convergence, [increase] legal certainty, while also contributing to limiting compliance costs" (Recital 14). The requirements should therefore be limited to **critical aspects** (e.g. article 7(4-5, 7)). This introduction of more extensive mapping also seems not to be in line with the provisions of the EBA GL on ICT and security risk management (paras 15 and 16) which require the identification of only the assets that support their critical business functions and processes.

Finally, **the proposed ICT risk management framework requirements should be aligned with the EBA Guidelines on ICT and security risk management**, considering that the latter have only recently been adopted into national regulation and that the proposal sets out detailed requirements that could have a significant impact on current ICT processes and set-up. Core definitional items relating to operational and security risk management need to be aligned (i.e. incident management & reporting, interconnectedness, ICT asset/system/ services, information security, IT operations management, business continuity management).

A) Section I

The EBF is concerned that the role of the management body has been greatly expanded in DORA providing firms with limited flexibility to work within their existing governance structures. We see merit in allowing firms more flexibility to ensure that seniority of the management body is suitable for the activities being required. We would therefore recommend **an approach which gives firms flexibility to choose their own governance, and financial supervisors the ability to ensure that governance is appropriate.** This approach will allow a risk-based and proportionate application of the rules. More generally, as governance structures in financial institutions (FIs) vary and

there might coexist a Board of Directors and an Executive Board, there should be a possibility for the Board of Directors to mandate the Executive Board for certain responsibilities.

Article 4(2) (a): The meaning of the term "final responsibility" of the management body to manage the financial entity's ICT risks requires clarification as regards its exact meaning.

Article 4 (2) (c): ICT risk tolerance should not be set by a management board. It should be rather defined by the business units together with ICT SMEs to ensure that people closest to those risks set risk appetite and tolerances.

Article 4 (2) (e): The review of "audit plans" is assumed to refer to internal audit plans. If it does not, the term should be replaced by a clearer one. The audit function is independent from management and any of its boards.

Article 4 (2) (i): The DORA definition of ICT-related incident is so broad that reporting to the management body on every such incident would be unworkable. In line with the spirit of regulatory reporting, the text should be amended to require informing the management body of only "major ICT-related incidents". In addition, the text should be amended from a requirement to inform "duly" to inform on a "ad-hoc basis". This is in line with the existing requirement in the EBA ICT and Security Risk Management Guidelines (60.d.ii).

Article 4 (3): There should be a general possibility for the management body to delegate. The provision could be amended in a way that would allow the management body to delegate individual ICT risk management responsibilities to a committee of the management body or other appropriate members of senior management, while retaining accountability for their implementation.

B) Section II

The EBF is concerned that there appears to be a **confusion of terms, concepts and frameworks in the ICT Risk Management requirements**. The proposal currently **requires an extensive set of control frameworks plans and strategies**: firms must have an ICT Risk Management Framework (Art.5), a Digital Resilience Strategy (Art.5), an information security management system (Art.5) and ICT Business Continuity Plan (Art.10) and an ICT Disaster Recovery Plan (Art.10). **It is unclear how these frameworks work together**.

For instance, as resilience and risk management are different disciplines, it is not clear how the Digital Resilience Strategy could be included in the ICT Risk Management Framework or how the Strategy would set out how the Risk Management Framework would be implemented. It is also **not appropriate to include ICT Business Continuity Plan in an ICT Risk Management Framework**. As stated in 2019 EBA Guidelines on ICT Risk Management, "The ICT business continuity management processes are an integral part of the overall FI's business continuity management process and should not be separated."

The current requirements will create significant compliance burdens on EU banks and may be unworkable for smaller firms. They therefore add to a lack of proportionality within

DORA. **The EBF recommends that these requirements be adapted to capabilities that a firm must demonstrate**, e.g. a firm should be able to demonstrate that ICT has been appropriately considered as part of its business continuity and disaster recovery planning.

Article 5 (2): The **definition of the ICT Risk Management Framework** included in DORA is **not in line with the** definition of ICT and security risk management framework included in **the EBA Guidelines on ICT & Security Risk Management**. These GLs define an ICT risk framework managed by a second level function, while DORA gives a broad definition that includes "*strategies, policies, procedures, ICT protocols and tools*" for the de facto management of the entire information system.

Article 5 (4): The requirement for a specific information security management system is too prescriptive. It is also not appropriate for an ICT risk management framework to include an articulation of such a system. While ISO makes reference to a specific information security management system, not all firms or teams have access to ISO owing to its costs. Further, as we are not aware of any other standard which articulates an "information security management system" this appears to be a requirement to make use of a specific standard which we do not believe is in line with the Commission's intention to be standard agnostic.

Article 5 (9): There is no widely agreed definition of "digital resilience" nor is this defined in DORA. It is unclear whether the intention in this provision is to be different from "digital operational resilience" as defined in Art. 3 (1). Resilience within technology must be considered at a relatively detailed level in order to account for the variation in the technical design and risk of different systems, applications and the data they handle. Therefore, any articulation of a general "digital resilience" strategy would necessarily be at a very high level such that its value to the firm would be minimal.

The individual requirements for the digital resilience strategy in the rest of Art. 5 (9) could be included within the ICT risk management framework without the need for a digital resilience strategy which will add confusion, complexity, and compliance burden, especially for smaller or less sophisticated firms.

Article 5 (9) (d): An ICT reference architecture cannot be produced at the level of the firm or legal entity. If one were to be produced it would necessarily need to be at such a high level of abstraction as to be meaningless. If produced at the level of a specific technology service, which is the only level of detail that would be meaningful, it would result in thousands of pages of paperwork that no firm could keep up-to-date. This requirement therefore represents a disproportionate burden to firms that will add little to no value for risk management, nor will it provide regulators with realistic insight into the firm's ICT operations.

Article 5 (9) (g): **The mandatory adoption of a multi-vendor strategy is too prescriptive and should be removed**, as it is contrary to a proportionate and risk-based approach to ICT risk management and could lead to unintended outcomes.

In cases where 3-5 large vendors dominate an entire segment, **requiring firms to use more than 1 vendor from a very small pool does nothing to reduce the concentration risk systemically. It does however add cost and complexity for the firms using vendors - and makes it more difficult to access innovation**. The

innovative capabilities technology vendors offer are most often vendor-specific - so they cannot be "rotated", meaning the EU financial sector may lose access to state-of-the-art technology solutions. This can **harm the competitiveness** of the EU financial sector without reducing the concentration risk, entailing considerable cost for little benefit. Also, when applied to an EU legal entity within a group structure, the requirement could force the firm to shift from relying on an intra-group arrangement to depend on an external technology provider, increasing the concentration risk that the Regulation aims to reduce.

While **dependency on a single or a few vendors** may lead to concentration / lock-in risks, in practice this is **already managed** by pre-contractual risk assessments, exit plans and the integration of termination rights into the FIs' contracts. Concentration risk is not a new issue and therefore managing third party vendor concentration risk is an **integral part of banks' standard third-party risk management frameworks**.

European banks acknowledge the European Commission's **awareness of the facilitation of switching providers**, e.g. via technical requirements for data porting as mentioned in the EU Regulation on the free flow of non-personal data (Art.6), triggering industry work under SWIPO, or effective exit planning – which is already required by the EBA and will be required by the ESMA.

Article 5 (9) (i): The ICT-related incident communications strategy is too granular for an ICT Risk Management Framework. **The strategy will need to be tailored to markets, and incidents**. This requirement should be dealt with as part of the ICT-incident management chapter of DORA or in Art. 13 – Communication, to avoid confusion in the text.

Article 5 (10): The provision that financial entities may **delegate the tasks of verifying compliance with the ICT risk management requirements to intra-group or external undertakings upon approval of competent authorities** (CAs) will have **significant implications for centralised risk management and compliance functions**. For intra-group delegation, no CA approval should be required.

Article 7 (1): Regarding the provision that financial entities shall identify, classify and adequately document all ICT-related business functions, the EBF proposes to **clarify what constitutes an "adequate" mapping level** (e.g. recovery priorities of infrastructure and testing purposes). For instance, as regards Disaster Recovery (DR) purposes, DR solutions and procedures should cover all the production of ICT infrastructure, independently from functions' criticality and their underlining infrastructure. In line with the EBA Guidelines on ICT and security risk management and the recent BCBS Operational Resilience and Operational Risk revision proposals, the **mapping** should follow a risk-based approach and **only be required for critical functions**. This is both **practical** as mapping is an onerous task due to the amount of change in ICT systems and **proportionate** as it is more targeted at risk.

It is also not clear what an ICT-related business function is and a clarification would be welcome.

Article 7 (3): The **classification of major changes** as subject to risk assessment is subjective, therefore it **should be clarified** that it is for the firm to determine what constitutes a major change for the purpose of this requirement.

We also note that Art.10 (5) (a) uses the different phrase "substantive change". This should be amended for consistency.

Article 7 (4): As per Art.7(1) we recommend that the mapping requirement **be limited to critical systems**. In practice, mapping is a highly manual process that in this case would result in thousands of pages of flow charts with limited practical value and which would be incredibly burdensome to maintain accurately. Focusing on criticality of the firms' most important services allows for a more meaningful product that is focused on risk.

Article 7 (7): Obliging financial entities other than microenterprises to conduct a specific **ICT risk assessment on all legacy ICT systems is disproportionate**, as there is **no agreed definition of the term** "legacy systems" and **no justification provided for legacy systems being riskier** than new technologies. Sufficient integration and load testing of changes (for applications and infrastructure), coming in addition to monitoring and capacity management, help to foster resilience in a hybrid environment. The requirement to conduct a specific ICT risk assessment before and after connecting old and new technologies, applications or systems is of particular concern and lacks a risk-based approach that would allow for such assessment to be conducted only when there is significant risk involved. Moreover, this requirement is not in line with what is required by the EBA Guidelines on ICT and Security Risk Management. Unlike DORA, the EBA guidelines, despite specifically addressing ICT Risks, **do not mention at any point the need to carry out risk assessments on all legacy systems, but provide that systems must be classified according to their criticality**. In any case, a risk assessment should be performed before and not after a change, as any introduction of a new system should consider potential implications.

Article 8 (3): The **term "state-of-the-art"** for technologies to be used by financial entities **should be removed**, as its meaning is not commonly agreed and therefore subjective. It may also exceed smaller firms' ability to invest and force them to prioritise technology solutions that do not represent a good return on value in terms of their effect on risk. Taking into account that "state-of-the-art" does not mean "high-end", the term could be potentially replaced by the term "adequate" or "appropriate".

Article 8 (3) (a): It is **not possible to guarantee the security** of the means of transfer of information as prescribed in the article. The EBF recommends **rewording this provision,** including the term "minimize the risk" instead.

Article 8 (4) (a), **The wording in this provision should indicate that** requiring financial entities to develop and document an information security policy defining rules to protect the confidentiality, integrity and availability of their and their customers' ICT resources, data and information assets, **refers to customer data or any data related to the relationship with the financial entities' customers**. It is currently very generic, as banks are responsible for ICT resources and the information provided by clients or the information obtained through the contractual relationship with the client. As per current wording, it seems that banks bear further responsibility than this.

Article 8 (4) (b): The **requirements for how firms should design network connection infrastructure** are **too prescriptive**. The requirement should be limited to minimising and preventing contagion which is the objective that the provision is seeking to achieve. Also, even in high-risk instances, it **may not be appropriate to implement automated mechanisms for isolation**. Doing so could significantly increase the impact

of any cyber attack. The wording in this paragraph should be changed from "including" to "which may include".

Article 8 (4) (e): The definition of ICT Change Management, which differs from the one included in EBA guidelines on ICT and Security Risk Management, should better elaborate what within the ICT Change process should be based "*on a risk-assessment approach*".

Article 8 (4) (a) (c-f): The word "**policy" or "policies" seems to be used inconsistently**, which creates uncertainty as to what governance level different requirements should be captured and approved. The EBF would welcome a definition of "policy" and "procedure" in this regard. The EBF also highlights the number and granularity of new policies required, which will lead to increasing complexity.

Article 8 (4) (subpara.2): The expression "instantaneously severed" should be replaced with the term "severed as quickly as possible in case of incident" to more realistically reflect how this action can be taken in practice.

Article 9 (1): We recommend changing the text from "identify all potential" to "monitor known" single points of failure, as identifying every potential single point of failure seems unrealistic.

Article 9 (2): We do not believe detection mechanisms are the appropriate place to define alert thresholds and criteria for triggering ICT-related incident detection. We recommend that this requirement be removed or clarify what is intended by the word "mechanisms".

Article 10 (1), (3): **The EBF does not believe that the Business Continuity Policy or the Disaster Recovery Plan should be part of the ICT Risk Management Framework.** ICT should be integral parts **of the firmwide disaster recovery and business continuity plans**. The requirements should also be changed to reflect that ICT need to be fully considered and integral to both, but that this may not require separate ICT policies or plans. Doing so would be to remove ICT from consideration within wider policies and plans. Business Continuity Policies, often already refer to Disaster Recovery Policies and Cyber Policies as "specialistic" components of Business Continuity Planning (e.g. Disaster Recovery Plan, Cyber-Attack Plan).

Article 10 (2) (a-c): DORA requires the ICT business continuity plan to include elements of response and recovery which we do not consider appropriate:

- (a) recording all ICT incidents should not be done as part of business continuity. Both aspects – while important in their own – are unrelated;
- (b) ensuring continuity of critical functions is not specific to ICT;
- (c) responding to incidents is not typically managed through a business continuity policy. This requirement would be more appropriate in Chapter III and creates confusion for firms who will need to try to determine where they should record the governance of incident response.

Article 10 (3): As per our comments on Art. 10 (1) it is not appropriate to create dedicated ICT disaster recovery plans, or to include these as part of the ICT risk management framework. In the event of a disaster the firm should consider the impact to its operations, and in particular its critical or important functions, holistically. Disaster recovery plans specific to ICT risk creating confusion regarding how a firm should handle a disaster. They also encourage compartmentalisation which would likely result in a worse

overall response from the firm. As with business continuity, it is important that the firm's disaster recovery plans fully consider ICT. However, that is not the same as creating dedicated ICT disaster recovery plans owned by the firm's ICT risk managers by virtue of inclusion in the ICT risk management framework.

Article 10 (5)(a): For complex ICT infrastructure (e.g. spread through several data centres), it is **very difficult to annually test the whole infrastructure**. For these environments, this requirement could be rephrased, by introducing the principle that **some tests shall be performed yearly, and the whole infrastructure could be tested in a larger time horizon** (e.g. 3 years). This would also take into account that these environments do not share the same risk level and/or scenario for the whole infrastructure. We also note that Art.7 (3) uses the phrase "major change", while here the term "substantive changes" is used. It should be clarified whether there is an intentional distinction being made between these two terms which are not defined.

Article 10 (7): **The obligation to keep records of activities before disruption events** would mean that all activities shall be recorded, as it cannot be known beforehand which activity would lead to disruptions. This **goes against a risk-based approach**. Also, **the requirement to make records readily available is disproportionate**, as supervisors are already able to access these records as needed. As they could contain sensitive information regarding a firm's operations, their circulation should be limited.

Article 10 (9): In line with the general limitation of incident reporting to major incidents**, the obligation to report to CAs all costs and losses** caused by ICT disruptions and ICT-related incidents should be limited to major incidents, as well. It is also important to bear in mind that it is not always possible to clearly attribute costs and losses to single incidents or they may only be visible over time.

Article 11: **There is disproportionate focus on backup** in the first paragraphs. Backups, as described in this proposal, are related to solutions that should be used in extreme scenarios, like disaster recovery. However, backup (the process of safeguarding data) is not used in the primary recovery methods. Backup management constitutes a running ICT management process that is focused to recover normal operations in case of data loss or corruption due to component failures, IT procedure and application failures, operative errors, intentional or unintentional misconduct. Therefore, **this provision should be amended to reflect the aforementioned meaning of the term "backup"**.

Article 11 (3): In the provision regarding the operating environment to be used when restoring backup data using the financial entities' own systems, **it should be clarified whether an operating environment different from the main one and not directly connected refers to a complete production environment replicated in a stand-by status to be used only in case of a contingency event.** It should also be clarified whether the bank will be able to reload on the same server if the data is healthy and whether this provision requires financial entities to have a recovery environment that is completely independent of their IS (bunker type). In case this is the intention of the provision, the wording "different from the main one" should be rephrased into "separate from the affected one". If the requirement is indeed to have a separate, offline store of data, then firms will be unlikely to make use of this for the purpose described in Art. 11(1), as recovering from an unconnected offline environment will not allow firms to minimise disruption nor to make their RTO objectives. Additionally, **the provision lacks a risk-**

based approach, as it is **not restricted to critical systems and includes all transactions**; Therefore, it should be limited only to critical systems.

Article 11 (4): The approach taken is **too prescriptive**, as maintaining redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs is a practice that might be effective in certain scenarios but not all. Sometimes it is best to restore in the same operating environment. We suggest that the proposal **allow that recovery can also be performed in the primary environment after the identification and blocking phases of the attack**. At a minimum, the segregation constraint should be limited to ICT assets supporting critical business functions.

In general, it is important that the proposed text **only targets IT assets that underpin critical functions**. A backup policy is needed depending on the criticality of the information or the sensitivity of the data.

Article 11 (6): The **EBF proposes that term "market efficiency" be deleted, as it does not have specific meaning regarding risk assessment (risk approach)** and efficiency is not part of operational risk. Further, "**extreme scenarios" are not a defined category** that firms could validate against. We suggest **changing the term to "severe" scenarios**, in line with existing international and US approaches.

Article 11 (7): The requirement to perform multiple checks to ensure that the level of data integrity is of the highest level might be effective in certain scenarios but not all and therefore **lacks a risk-based approach**. Additionally, ensuring that all data is consistent between systems does not mean that it is accurate or complete.

Article 12 (2): Rules on how to classify changes to be communicated to CAs should be defined, as **requiring financial entities to communicate to the CAs the changes they implement seems disproportionate** and it could be interpreted that it entails all changes, even minor ones. It should be clarified that that this provision only covers changes in the sense of mitigating measures – changes to address root causes of major ICT-related incidents affecting their core activities (if needed). Further, the EBF is concerned that the requirement to report could be interpreted as a requirement to seek approval. In the event of an incident firms must have the freedom to make immediate changes to address the cause or effects of an incident.

Additionally, the wording "significant ICT disruptions" should be changed, in alignment with the proposal's part in reporting, using the term "major incidents".

Article 12 (6): This provision should be amended to clarify that training obligations shall be proportionate to the function of the personnel and the degree of its involvement in digital operational resilience, besides the general ICT security awareness programmes and digital operational resilience trainings included in training schemes for all staff.

Article 13 (1): It is **not considered appropriate to expose major vulnerabilities - which are not defined in DORA- as this would represent an extreme risk to the bank. Major vulnerabilities should be removed from this requirement**. Further, the text should be amended to require plans to be developed for only major ICT-related incidents. Mass disclosure of relatively minor and inconsequential incidents **could erode confidence in the EU financial sector.**

Article 14 (b-c): While the EBF agrees with the principle of "security by design", this should be included in products. **Procedures and tools** as well as the **methods, techniques and protocols should not be prescribed**. These provisions should be **replaced with a requirement to "incorporate security controls into systems from inception**".

CHAPTER III: ICT-RELATED INCIDENTS, MANAGEMENT, CLASSIFICATION and REPORTING

The EBF calls for a fully harmonized ICT- incident reporting framework (Articles 15 – 20)

The EBF is encouraged by the steps to harmonise cyber incident reporting requirements in the proposed Regulation vis-à-vis the NIS Directive (and the proposed NISD2, as mentioned in its proposed text), as well as vis-à-vis the PSD2 with the amendment via the accompanying Directive.

Regarding the PSD2, however, harmonizing reporting only for ICT-related incidents would retain the divergencies with the reporting of non-ICT-related incidents and, therefore, the fragmentation in incident reporting will remain. Moreover, additional complexity could arise, also due to the overlapping definitions contained within the two pieces of legislation, and the use of different terminology (e.g. Operational Incident, Security Incident, ICT Related Incident, Cyber attack). The EBF's view is that it will not be possible for firms to distinguish between ICT and non-ICT incidents at the earliest stages of analysis and therefore the current approach will likely result in significant duplication of reporting. Given also that in the PSD2 text there is no mention of ICT and non-ICT incidents but only of security and operational ones, while DORA covers aspects of physical security as well, a clarification of the definition of non-ICT related incidents and its importance in practice is deemed necessary. For these reasons, the current proposal should be **amended to also include reporting of all major incidents under PSD2**.

While these steps are decisive towards removing the obligation of FIs to report multiple times, **there are still several other intra-sector and cross-sector provisions in EU legislation that set out different timeframes, taxonomy, and thresholds,** such as the GDPR, the eIDAS Regulation and the SSM requirements. To this end, a fully harmonized cyber incident reporting regime across all EU legislation is yet to be introduced upon entry into force of DORA and the EBF urges policymakers to further build upon the initiative taken into the proposal until full harmonization is achieved[2].

The EBF is of the view that to be effective and practical, **reporting requirements** must be focused **on incidents exceeding a relatively high threshold**, (we also note the recent consultation from the EBA regarding PSD2 incident reporting which aims to raise the threshold for reporting precisely in order to reduce the number of non-material incidents reported). In particular, it is proposed to refer to thresholds that do not only

[2] For a detailed presentation of the multiple incident reporting requirements in EU legislation and the EBF proposal for harmonization see the EBF position on cyber incident reporting.

have an absolute amount but refer also to the percentage threshold so that the achievement of that threshold is not linked to the size of the operations of the bank.

We urge policy makers to **set a high bar for reporting initially and to adjust in the future if it is determined that material incidents are not being captured by the requirements.**

Additionally, as **public sector authorities are able to aggregate and gather reported information from firms and could provide anonymised feedback** to support sector preparedness and response, **further actions should be taken** to encourage the sharing of this information.

As regards exploring the possibility of further centralisation of incident reporting via a central hub, the EBF welcomes this initiative. However, as described in the relevant EBF position[3], **establishing a central reporting and coordination hub in each Member State** is deemed more feasible in the short term than designating one at EU level. A centralised hub at national level could work as a one-stop shop mechanism, where all incidents, including sector-specific ones, can be reported. The national entity operating this hub would be the one responsible for the sound delivery of the requested information to each regulator, supervisor and/or law enforcement.

Setting up an EU level hub for major ICT-related incident reporting in order to identify trends and avoid duplications in reporting could be explored on a medium to long term basis. In such case, the EBF particularly stresses the need for more clarity in the role and the function of this mechanism, ensuring also maximum security conditions in terms of resilience, feedback, and data security, as it would entail concentrating all major incidents reporting from European financial institutions and would represent a highly sensitive source of information. Therefore, the requirements in terms of resilience, feedback, and data security of the hub would have to be carefully laid down, especially as regards security of exchanges, security of information storage (back up), control of persons having access to information and adopting a consistent method of reporting.

The EBF also recommends alignment with international best practices in incident management. In its 2020 toolkit [4]on Cyber Incident Response and Recovery (CIRR) the Financial Stability Board (FSB) provides best practices for incident reporting as part of cyber incident response and recovery. Alignment with a global standard, for example considered by a FSB standard global approach, would reduce regulatory uncertainty and the regulatory burden for cyber incident responses for financial entities; especially those operating cross-border.

Article 15 (2): The provision should be amended to clarify that firms can organise their management of this process as they see fit assuming they are able to achieve the stated objectives.

Article 15 (3) (d): The word "major" should be added in the last reference of ICT-related incidents, in line with the previous relevant mentions in the sentence.

[3] Ibid
[4] https://www.fsb.org/wp-content/uploads/P191020-1.pdf

Article 16: The EBF believes that regulators and financial entities should work together to promote standardisation and effective implementation for ICT-related incident criteria, for instance on the following topics:

- How to assess reputational damage (Art. 16.1.a),
- When to consider that downtime has started (Art. 16.1.b),
- Whether geographical spread should include EU Member States, or European countries or other jurisdictions with critical operations (Art. 16.1.c),
- How severity (Art 16.1.1) and criticality (Art. 16.1.f) are defined, and
- How to determine economic impact (Art. 16.1.g).

We recommend that the criteria for incident classification are developed jointly with industry input, and that it is aligned with the FSB toolkit for CIRR.

Article 16 (2) (b): In line with the provision's objective, the missing word "major" should be added in the second reference to ICT-related incidents.

Article 17: In general, the **incident management requirements are too strict and too prescriptive** regarding the classification of incidents and the frequency of reports, including submission templates.

It is imperative that the unification of incident reporting is considered as soon as the legislation comes into force. We welcome an understanding of the timeframe "without delay" under Art. 17 (1), (3) (a) as "without **undue** delay", offering at least one business day in the responder's national state, since (a) refers explicitly to the end of such business day.

Article 17 (2): The requirement to inform stakeholders **when an incident "may" have an impact is too broad**. This could lead to **excessive reporting which could have negative impacts on market and consumer confidence**. For the same reason a qualifier, such as "material", should be added before impact. Finally, a literal reading of the requirement to inform on "all measures" taken would include root cause analysis and other highly sensitive information. **We recommend the word "all" is removed and replaced with "within reason of measures".**

Article 17 (3) (a): The EBF believes **that two hours is far too little time** to produce meaningful information regarding an incident. Without further time to determine impact firms will be forced to report non-major incidents but with little clarifying or actionable information. We note that in some EU jurisdictions the requirement is to report within two hours of the point when the incident is determined to be significant. We believe this is a more productive approach that will result in higher quality incident reporting.

Article 17 (4): The EBF believes that delegating the reporting obligations **upon notification of the CA should suffice**, instead of the latter's approval, especially in the case of delegation within a group structure.

Article 20 (2): In the first subparagraph of the article, the word "major" should be added in the first reference to ICT-related incidents, in line with the meaning of the provision.

CHAPTER IV: DIGITAL OPERATIONAL RESILIENCE TESTING

The EBF calls for an EU-wide mutually recognized digital operational testing framework that is proportionate to the financial institutions' size (Articles 21 -24)

Digital operational resilience testing is an important part of banks' resilience strategies and efforts to ensure consistency across the EU financial sector in the Regulation are welcome. The proposal will have a direct impact on the amount of effort, resources and costs needed to develop, implement and maintain systems that support critical functions, due to the annual testing and the security initiative requirements. Therefore, a **risk-based approach should be taken into account in devising which FIs qualify as significant** in order to carry out threat led penetration testing (TLPT), **with the criteria focusing on the criticality of the service and the size, scale or systemic character of the financial institution, in line with the TIBER framework.** FIs have identified their critical processes, defined by the criteria established by the existing EBA Guidelines and in Art. 3 (17) of this proposal, while Supervision Authorities also have established entities of Systemic Importance. The criteria should be built on both these identification processes. A level-playing field among all financial entities should be ensured, as well as the approach that customers of smaller entities should also be equally protected.

Intra-EU, **and international mutual recognition of testing results is vital to reducing risk and ensuring the smooth functioning of the Single Market** and to avoid cost increases for financial entities operating cross-border. We would recommend including an explicit mention of the mutual recognition effects of digital operational resilience testing in the Regulation.

Article 21 (5): We recommend the text be amended **to require that all issues be "dispositioned" rather than remedied**. Firms will take a risk-based approach and may determine that a vulnerability is within risk appetite or can be mitigated through compensating controls. Additionally, it would be highly inefficient to re-test for validation and would distract significant resources from more valuable work. The EBF recommends that **firms be given the flexibility to target validation based on criticality or to gain confidence in the actions taken through alternative means**. In case this is the intention of the text, further clarity to that end would be welcomed.

Article 21 (6): The EBF is of the view that the **requirement to test all critical systems and applications annually is not scalable to large firms**. It must be recalled that testing is only one tool among many and not always the most appropriate. Testing all systems as currently proposed, without allowing firms to in some way prioritise for risk, **does not fit with modern best practices and does not take into account what other controls firms may put in place**. The EBF recommends allowing firms to test the main critical systems following a risk-based approach allowing the consideration of sensible (multi-year) windows of time in light of the level of criticality. Complexity and size of the environment for the critical system should filter into this approach, being aware of systems and applications' set-up, e.g. multiple data centres with possibly unique risk scenario considerations.

Article 22 (1): It is **unclear from the text whether it is expected that all of these tests be performed** or for this to be a list of possible tests that can satisfy digital operational resilience testing requirements. While the tests listed in this paragraph are all valid, they would **not all be appropriate on all occasions**. Attempting to do so would not only be extremely burdensome for firms, but it would also yield significant duplication

and therefore no improvement in risk management. Instead, these options shall be applied according to the risk-based approach.

Art. 22 (2): The requirement to perform vulnerability assessments for all existing or new services supporting critical functions, rather than only those services that are themselves deemed critical, is challenging and assumes indefinite capabilities. Acknowledging the insights that such assessments can bring, its scope should nevertheless focus on the **essential** support services, as identified by the financial entities, for the critical services.

Art 23 (2) (sub.para. 2): An **adequate level of mapping** underlying ICT processes, systems and technologies supporting critical processes and services should be defined, as **too granular mapping could be disproportionate and not easily manageable**. Moreover, the requirement for financial entities to ensure a TPP's participation in a TLPT should be replaced by the requirement to include a contractual requirement for critical providers to conduct TLPT. This could either be done via the FI's TLPT or organised by the TPP itself if evidenced via adequate documentation, as it is already market standard. Especially in a multi-tenant environment, the inclusion of a TPP in multiple TLPTs by various financial entities does not only increase operational risk per se, but also raises significant questions with regards to liability, e.g. what should be considered "adequate measures" by the financial entity or who would be held liable in case a TLPT causes an operational incident, such as a data leakage. It should be clarified that, **in case that ICT third-party service providers are included in the remit of TLPT, banks cannot be held accountable** for their participation. The relevant accountability/liability should be clarified, and multi-tenant environments should be considered, while always taking a risk-based approach as to which TPPs have to be included in the TLPT.

Article 23 (4): This provision refers to "intelligence-based penetration tests". We recommend this be edited to "threat-led penetration tests", to bring it in line with the rest of the chapter. If a different form of testing is meant, this needs to be clarified and the industry given time to consider potential impacts.

The EBF suggests that the audit rules for Testers for TLPT be uniform at European level to avoid discrepancies and respect the level playing field.

Article 23 (4) (c): The provision for the **mutual recognition of testing results is too limited**. The EBF recommends the inclusion of a **specific mechanism** to allow for the mutual recognition of tests among EU authorities that would be attested by the host MS, as well as for the potential of recognition of tests performed in other jurisdictions, assuming they meet regulatory expectations. The obligation to perform these TLPT should be limited to critical functions, making use of the TIBER-EU framework to define the methods of carrying out this type of TLPTs. Also, the relevant RTS to be developed by the ESAs should be based on TIBER-EU.

Article 24 (1) (c): When a reference is made to testers' certification, we would welcome **clarifications on the certification requirements**. When adhesion to a formal code of conduct or ethical framework is mentioned, it would be beneficial to clarify the requirements that those codes or frameworks should have.

Article 24 (1) (d): The **audit rules for external testers** performing TLPT should be **uniform at European level**, in order to avoid discrepancies and to respect the level playing field.

CHAPTER V: MANAGING OF ICT THIRD-PARTY RISK

The EBF understands the importance of resilience and risk awareness when it comes to the interactions with third-party providers. Dedicated to providing the highest level of service quality to customers and investors, European banks keenly focus on the adequate management of third-party relationships, mitigating risk to provide a convenient, innovative and secure service experience. Additionally, committed to the accountability under the financial regulatory framework, European banks vigorously secure compliance to the existing legal requirements.

Where DORA interacts with obligations and requirements for financial entities, European banks want to highlight the importance of aligning these newly proposed requirements with existing regulation and supervisory guidance. Following the **principle of proportionality**, additional regulation should only come into play where there is an existing gap in the framework, then to be addressed by DORA. The proposal's expectations for the financial entities should not diverge from the EBA Guidelines on ICT and security risk management – as demonstrated above in the relevant provisions on the proposal's ICT Risk Management provisions – and the EBA Guidelines on outsourcing, which are implemented in member states and have triggered substantial efforts by the banks to be compliant. The established Guidelines have created an effective framework for supervision in European Member States. Any divergence of DORA from established pillars of this framework creates disproportionate burden on the banks and endangers the security gained by the supervisory approach in the first place. Considering the only recently implemented Guidelines on outsourcing (entered into force in September 2019), the financial sector should gain sufficient time for initiated changes to be impactful. A too early addition or possible deviation due to DORA requirements needs to be avoided. Otherwise, the ability for European banks to safely innovate financial services is seriously put in peril.

European banks would like to highlight that the requirements for engagement and access to TPPs have **direct impact on the availability of innovative service solutions** for banks. Where financial entities are faced with additional or possibly misaligned legal requirements under DORA, the fragmentation will be a burden. Ultimately, this could detrimentally impact the availability of innovative financial service to banks, their ability to strategically take them up and effectively offer them to customers in Europe. European banks commit themselves to secure digital transformation, satisfying the needs and demands of consumers and investors while contributing effectively to a digital leadership role for Europe. In turn, a proportionate approach, meaning a firm commitment of the regulatory framework to the **risk-based approach** for digital operational resilience, must be the foundation of the management of ICT third-party risks by financial entities.

A) SECTION 1 – Key principles for a sound management of ICT third party risk (Articles 25 – 27)

The EBF calls for alignment of DORA with the existing European supervisory framework

In order to ensure that concentration risk is properly monitored and managed, European banks generally see value in a more specific oversight of CTPPs, taking into special consideration critical Cloud Service Providers (CSPs).

An approach by means of a Regulation can help to provide legal clarity and necessary harmonization across the EU for individual legal requirements regarding the engagement of financial entities with TPPs. Considering the inherently cross-border nature of innovative third-party solutions, such as cloud computing, a detrimental fragmentation of the regulatory approach in member states' jurisdictions must be avoided. Innovative service solutions and cooperation with TPPs need to aim for economically viable and scalable solutions for European banks.

DORA's advancement of the framework for digital operational resilience should reflect the existing regulatory safeguards and supervisory guidance and expectations in Europe. The existing EBA Guidelines on outsourcing and ICT and security risk management are of essential importance, having triggered extensive compliance efforts by the financial sector in the recent past. DORA should allow the financial entities to continue operations under this established governance, which prove to be effective. Thus, DORA should align with established GL requirements, without adding additional obligations for banks.

To secure alignment of the approaches under EBA Guidelines and DORA regarding financial entities, we welcome a clarification as to the scope of the DORA principles. They only refer to the ICT third-party services, while EBA Guidelines broadly address all outsourcing. Where DORA aspires for more harmonization, the EBA Guidelines already provide for the right framework, without need for changing requirements. To that end, **Art. 3 DORA should be amended**, aligning the DORA definitions stronger with the important criteria applied under the definition applied by EBA GL para. 12,26, 27 and 28[5]. Enhanced regulatory requirements under DORA should focus on ICT critical or important functions.

Equally important, the EU legislator should ensure financial entities via explicit reference that the established definition of "critical or important function" under the EBA GL (para. 20 and following) is matching the concept of DORA's understanding of "critical or important function" for financial entities under Art 3 (17)[6]. Even though the EBA GL on outsourcing cover more than ICT services, DORA should not create legal uncertainty and disproportionate burden for banks by creating a diverging understanding of this central definition.

[5] See above Chapter I, B) Definitions.
[6] Ibid.

The EBF calls for a consistent application of a risk-based approach across DORA

We welcome the European Commissions' dedication to the principle of proportionality for the DORA proposal. European banks agree that this fundamental principle for EU legislation should be thoroughly reflected across the proposal's concepts and wording. Legal requirements and obligations must be based on a **risk-based approach**. It allows banks' access to digital innovation while safeguarding systemic stability as well as consumer/investor protection.

Art. 25 (2) DORA refers to the principle of proportionality but fails to establish a risk-based approach explicitly, to be applied by financial entities under the included requirements. We invite the EU legislator to clarify accordingly and to add explicit references to the risk-based approach in all Articles 25 to 27, with specific attention to:

- Art. 25 (2) – general principle for management of ICT third-party risk
- Art. 25 (4), (10) – provision of a template for the register of information[7]
- Art. 25 (6) – specification of information security standards
- Art. 25 (9) – minimum content of exit plans

The EBF calls for avoidance of additional burden by regulatory fragmentation or legal uncertainty for CTPPs' customers

European banks welcome the European Commission's proposal to foster harmonization and more centralized oversight for CTPPs. However, **the ability of financial entities - as customers of CTPPs – to adopt technological solutions depends on balancing access to innovative CTPP services with burdens imposed by legal requirements for digital operational resilience**. Should the new oversight add, either directly or indirectly, to the burden on financial entities in terms of due diligence, compliance or assistance of oversight's later enforcement, the timely uptake of innovative service solutions by the European financial sector will be at risk. Ultimately, this could prove detrimental to customers in the EU and the European leadership position in digital transformation of the economy. As correctly assessed by the Commission, the fragmented and in parts inefficient regulatory framework for ICT risk management applicable to financial entities is one of the key challenges for the creation of a true single market for financial services in the EU. We therefore welcome the intention expressed in Recital 14 of the proposal to **reduce regulatory complexity, foster supervisory convergence, increase legal certainty, while also contributing to limiting compliance costs, especially for financial entities operating cross-border, and to reducing competitive distortions.**

European banks operate under a comprehensive regulatory framework. While they are committed to their obligations – especially vis-a-vis the protection of consumers and financial stability – they should not be faced with additional regulatory requirements to secure operational resilience on the side of third-party providers. **Banks already**

[7] The **EBF Cloud Banking Forum developed a guiding register template** to foster harmonization, focusing on cloud services (only). Please find the template here: https://www.ebf.eu/wp-content/uploads/2020/06/200604-EBF-Cloud-Banking-Forum_Outsourcing-Register-cloud-specific-guidance_final.xlsx.

implement the thorough framework of the EBA Guidelines on outsourcing and the EBA Guidelines on ICT and security risk management, following their national implementation in Europe**.** Thereby, banks' interaction with TPPs is already addressed comprehensively in EU regulation. We therefore do not see the need for DORA to establish additional requirements. Where DORA introduces requirements that overlap with or reiterate parts of existing requirements, for example under Art. 27 regarding contractual arrangements, there needs to be alignment with the Guidelines already in place. Any direct or indirect deviation would create legal uncertainty and disproportionate burden for banks that would need to operate under multiple regulatory and supervisory expectations, and, for example, implement two different types of outsourcing registers for ICT and non-ICT-related arrangements.

Detailed risk assessments and minimum content for contractual arrangements, such as access and audit rights should be limited to the outsourcing of critical or important functions as outlined already in the EBA Guidelines on Outsourcing and ICT Risk Management.

Considering the deviation between DORA proposal and EBA Guidelines, European banks recommend the following changes to DORA:

- **Amendment to Article 25 (3):** In line with the comment made on Article 5 (9) (g), the mandatory adoption of a multi-vendor strategy is too prescriptive and could lead to unintended outcomes. We recommended that this requirement is removed, so that the use of multi-vendor strategies remains a risk-based and business decision of financial entities.
- **Amendment to Article 25 (4):** In order to avoid disproportionate burden to banks due to diverging or extending legal obligations, the register on contractual arrangements should not go beyond the register reporting obligations on outsourcing, already existing under EBA Guidelines para. 52. A single repository is essential for effective reporting operations.
  Where the EBA register calls for register entries *only* for critical or important functions, Art. 25 (4) DORA should not compel the financial entity to create a separate, workload-intensive register for non-critical ICT services regarding the identical service solution. It is important to assess the register scope in light of the intended purpose of the register for the competent authority. An excessive scope can trigger an information overflow, rather distorting than helping to identify concentration risks. Hence, European banks recommend a register scope as selected by the EBA GL[8]. Applying a two-tier system, certain reporting information are only to be provided in case of criticality.
  The register scope under DORA should not exceed the already implemented register requirements under the EBA GL. Where the EBA register calls for register entries only for critical or important functions, Art. 25 (4) DORA should not compel the financial entity to create a separate, workload-intensive register for non-critical ICT services regarding the identical service solution. It is important to assess the register scope in light of the intended purpose

[8] The EBF Cloud Banking Forum created a template to fill out the EBA register requirements under para. 54 and following for cloud-specific outsourcing. Its structure shows the advantage of an advanced reporting with distinction of critical or important services, providing a necessary filter function for the reader of the register.
https://www.ebf.eu/wp-content/uploads/2020/06/200604-EBF-Cloud-Banking-Forum_Outsourcing-Register-cloud-specific-guidance_final.xlsx

of the register for the competent authority. An excessive scope can trigger an information overflow, rather distorting than helping to identify concentration risks. Hence, European banks recommend a register scope as selected by the EBA GL, allowing for a single register.

- **Amendment to Article 25 (5):** Following of a risk-based approach by financial entities, the listed actions prior to entering the contractual arrangements should be limited to critical services. To that end, points (b) to (e) should be dependent on the confirmation of criticality or importance by the financial entity's assessment under (a).
- **Amendment to Article 25 (6):** We call for amendment of the wording "latest information security standards". Designated point of time, frequency of reconsideration and entity responsible for designation of this status are not clear. Neither are detailed factors to consider in the assessment of "latest". Generally speaking, the "latest" standards are not necessarily the most secure, since testing is an essential part of the IT security development. Without sufficient guidance, the interpretation of this requirements can trigger detrimental fragmentation in the application the Regulation across European jurisdictions. We suggest amending the wording to:

  "*Financial entities ~~may only enter into contractual arrangements with ICT third-party service providers that comply with high, appropriate and the latest~~* ***should ensure that their ICT third-party service providers comply with appropriately high information security standards.***"

  We invite the legislator to consider that firms should only be required to limit their contractual relationships when those relationships will not allow them to meet their own risk appetites or regulatory requirements. Art.25 (6) creates precedents for interference in what should be market decisions.

- **Amendment to Article 25 (7):** Regarding sub.para. 2, targeting auditor skills in case of "high level of technological complexity" is both unnecessary and confusing, given the difficulty in determining what qualifies as having a high level of technological complexity. We suggest deleting this unspecific reference, without questioning the need for appropriate skills for auditors itself.
- **Addition to Art. 25 (8) (c):** We encourage the Commission to clarify that the contractual arrangement should include a termination *right* for constellations of evidenced major/material weakness by the ICT third-party provider under point (c). Mitigating actions by both TPP and customer should be taken into considerations before execution of such right is called for. European banks support an incorporation of the proportionate wording included under EBA Guidelines para. 105:

  "Institutions should take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, institutions and payment institutions should follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, institutions and payment institutions should take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary."

  Since Art. 25 (8) (c) aims to ensure the right for termination of contractual arrangements with cause, it should include an explicit prevention for providers to

make such termination subject to penalty payments or other negative consequences for service provision to the financial entities prior to the triggered exit.

- **Amendment to Article 25 (9) sub.para. 3 (following (c)):** In line with a proportionate risk-based approach and EBA GL para. 106, such requirement should not address all third-party services but be limited to critical or important functions provided by ICT third-party providers.
  Further, it may not always be possible to identify an alternative in the case where the third-party dominates the market in a particular jurisdiction or where the service is based on proprietary information or technology. In such an instance a firm may choose to step in (in the event of failure). The paragraph 9 should be amended to allow firms the flexibility to find the most appropriate way to continue operating or providing the service. The recovery of data in the event of outage or failure is important but should be distinguished from the ability to continue providing the service or resilience targets.

  "Exit plans shall be comprehensive, documented and, where appropriate, sufficiently tested. **The exit strategies shall be commensurate to the risk profile of the third-party ICT service providers.**
  Exit strategies shall not be necessary for those third-party service providers within the scope of prudential requirements in a consolidated situation as defined in point (47) of Article 4(1) of Regulation (EU) No 575/2013 when their risk mitigation strategy is already taken into consideration within the ICT risk management framework of Article 5 of this Regulation."
- **Article 25 (10):** Intended technical standards by the ESAs on a standard template for the Register under Art. 25 (4) should pick up the EBA GL's distinctions in critical and non/critical services[9].
- **Article 26 (1):** DORA should clarify that the definition of "*easily substitutable*" should be for the firm to define. The latter will best be suited to consider factors such as provider availability and time required for migration. Further, the consideration of multiple contractual arrangements should be focused on critical and important functions.
- **Article 27:** Key contractual provisions should be aligned to the EBA Guidelines on Outsourcing Arrangements and apply only to critical ICT services.
- **Article 27 (2) (e):** We propose an addition of the phrase "including major ICT-related incidents" to the text following the word "development". For financial entities to comply with their reporting requirements, including those set out in Art 17 (3), they require timely information from their ICT third-party service providers. This has in the past been difficult for firms to negotiate owing to the range of different reporting requirements and the lack of a clear regulatory mandate for the ICT TPPs. Inclusion of the phrase suggested above will help clarify the regulatory requirements to which financial entities are subject and reduce a friction in contractual negotiation between financial entities and providers.
- **Article 27 (2) (j):** In the interest of legal certainty, the provision should abstain from using ambivalent wording that is expected to trigger diverging interpretations

[9] The EBF Cloud Banking Forum developed a guiding reporting template under the EBA GL for cloud-specific services. Aiming for a harmonized approach across European jurisdictions by NCAs, the template operates on EBA's distinction of reporting obligations for critical or important services.
https://www.ebf.eu/wp-content/uploads/2020/06/200604-EBF-Cloud-Banking-Forum_Outsourcing-Register-cloud-specific-guidance_final.xlsx

by national competent authorities and – in turn – facilitate detrimental fragmentation of the framework instead of providing valuable harmonization. Art. 27 (2) (j) introduces the expectations of competent authorities as relevant factor for termination rights and notification periods. This reference invites deliberately fragmentation and prevents banks' from negotiating contractual arrangements effectively for inherently cross-border solutions beyond individual jurisdictions. We invite clarification as to what expectations would need to be satisfied and how to ensure the harmonized arrangements across the EU. Looking at contractual practices today, contracts might be signed for periods of 3 to 5 years. Where competent authorities' expectations change, contractual updates on termination and notices cannot be easily achieved right away. We recommend a harmonized understanding of supervisory expectations under (j) at level of the European Supervisory Authority (ESA).

The EBF welcomes the reference to standard contractual clauses under Art. 27 (3) DORA

In the field of cloud computing, the EBF observes that the legal and regulatory constraints and the higher compliance risk derived from the use, management and storage of customer information constrain the adoption of cloud service models by a strictly (and comprehensively) regulated banking industry. These constraints also create significant frictions in ensuring that regulatory compliance is achieved in contractual negotiations between banks as Cloud Service Customers and Cloud Service Providers. In order to address these frictions for cloud computing services specifically, **standard contractual clauses (SCCs) for cloud use are an appropriate tool to safeguard the proportionate implementation of requirements of the regulatory framework regarding cloud.**

The EBF welcomes the activities by the European Commission to develop voluntary SCCs for the use of cloud computing. The reference under Art. 27 (3) helps to highlight the potential of a use of SCCs, calling for a deliberate consideration. We support the requested attention by both financial entities and providers, aiming to support reliable compliance with the regulatory framework, including DORA, in contractual arrangements.

The EBF invites the European Commission to continue its engagement with European banks, securing SCCs with high practical relevance for banks' negotiations with providers. We encourage alignment with GDPR Articles 28 and 46 and with the new standard contractual clauses between controllers and processors located in the EU and the new standard contractual clauses for transfer of data to third countries (contractual wording under Art. 28 and 46 GDPR and the SCCs for international data transfer).

B) SECTION 2 - Oversight framework for critical third-party providers (Articles 28 – 39)

The EBF supports the Commission's focus on oversight for only critical third-party providers

In line with the key principle of **proportionality**, we welcome the European Commission's approach to apply the oversight framework only to **critical** ICT third party service providers.

We welcome the Commission's approach to **determine "criticality" for TPPs based on mixed qualitative and quantitative criteria, which should be clear and cumulative.** Size of a TPP alone will not provide for an exhaustive criterion. We welcome the consideration of subcontracting under Art. 28 (2) c), since criteria should focus both on characteristics of the service in question as well as entity qualities, including the role of the TPP (e.g. within a supply chain). To properly monitor and reflect the effect of concentration, it is important to cover sub-outsourcing constellations, either involving multiple layers of TPPs (for example for cloud services) within one service contract or a "fourth party" involvement of a TPP by a service vendor of the financial institution.

In order to avoid detrimental duplication of rules for intra-group subsidiaries (ICT providers), European banks suggest an amendment to Art. 28 (1) to exclude these constellations from the oversight framework under DORA.

Art. 28 (1): new letter

> "**c) the designation mechanism referred to in point (a) and (b) of paragraph 1 shall not apply in relation to Intra group ICT Third party service providers.**"

We welcome the suggested clarification for intra-group ICT providers exclusion from DORA's Chapter V by means of an additional recital. [10]

Publication of a yearly list of CTPPs under Art. 28 (6)
European banks welcome the intended yearly update by the ESAs, through the Joint Committee, on critical ICT third-party service providers at Union level. However, there must be a delay between the designation of an ICT TPP as critical and that status coming into effect in order to allow firms time to adjust their contractual relationship or find an alternative provider.

The EBF welcomes the ESAs' understanding of a designation of a single supervisory authority as Lead Overseer

In their letter from 9 February 2021, the ESAs expressed their support for a joint-ESA executive body, integrating the role of the Oversight Forum and being responsible for the overall oversight work for cross-sectorial CTPPs. A legislative clarification is invited to

[10] See above under Chapter I, B) Definitions.

designate CTPPs to a single ESA. European banks welcome the dedicated assignment of EBA to the service oversight by CTPPs that are located within the remit of financial entities.

The EBF is concerned of DORA limiting the available selection of innovative CTPPs by financial entities

We call upon the EU legislator to delete Art. 28 (9) since it will prevent European banks from offering cutting-edge service innovation to consumers and investors. The paragraph calls upon financial entities to "*not make use of an ICT third-party 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*". European banks believe that this geographical restriction, executed as a single factor for elimination of CTPP-usage, is disproportionately limiting banks' options in selecting innovative providers. While we understand that the oversight framework seeks to anchor authorities' monitoring and enforcement powers by providers' establishment in Europe, such "in-or-out" limitation due to geographical establishment eliminates the global potential of service innovation for the benefit of consumers and investors. Technological innovation is developing in non-European regions and relevant providers are emerging in various jurisdictions. An establishment within the EU, which may not be feasible for every innovator with potential to become critical, can hamper or even altogether exclude the access of European banks' customers to new and beneficial services. Not every new technological innovation will automatically have an equivalent provider in the EU, offering the same service solution under the same timeline. Even more concerning is the targeted ban on the financial sector only under DORA, creating an imbalance in terms of innovation access across different sectors. This feels counterproductive when aiming for a European level playing field in digital innovation.

We believe that the EBA guidelines on outsourcing already set a sufficient framework to ensure a sound management of the additional risks and the supervisory expectations regarding outsourcing to service providers located in third countries, without limiting the use of these providers by financial entities. We call upon the EU legislator to take the same approach in DORA. The criteria for designation of criticality under Art. 28 (2) DORA clearly address factors beyond the size of a provider. In turn, Art. 28 (9) will not only effect large critical provider companies. Small, upcoming non-EU TPPs offering quality-enhancing, and in the future potentially critical, services will be heavily affected by the requirement of an EU establishment for reasons related to business development and available resources. This can include business process management providers, account aggregation and payment initiation services, or providers of collaboration tools.

Before considering an outright ban, a call for a legal representation of the CTPP within the EU could allowing later public enforcement actions to target the provider. However, at a minimum, the EBF calls for clarification that business presence/representation should not be understood as a requirement to have the central or even the operating legal entity based in the EU.

Furthermore, additional clarity is welcomed regarding the effect and expected timeline for actions by financial entities, should a previously non-critical provider without EU-establishment become critical throughout a running contractual arrangement. Considering

the potentially complex migration of service solutions, European banks would like to warn against any disproportionate expectations in terms of rapid termination and migration decisions. Based on a risk-based approach, TPP-customers require necessary flexibility to adjust in such case, upholding their commitment to established accountability and compliance.

Since Art. 28 (9) introduces a serious barrier to continued cooperation with CTPPs covered, the requirement should not be introduced abruptly, with little or no warning to financial entities. To avoid detrimental impact on the complex, hence often long-term planned and prepared, usage of CTPP services by financial entities, there should be a specific transition phase of at least 36 months granted for Art. 28 (9), allowing financial entities to act in line with its defined exit strategies.

The EBF understands an appropriately designed oversight framework for CTPPs to be of added value for CTPP-customers

The DORA proposal aims to establish coordinated oversight of CTPPs, introducing a Lead Overseer who executes market powers in coordination with national competent authorities. The Commission proposes significant monitoring obligations and respective overseer powers to ensure the collection of data important to ensure digital operation resilience. Under the current framework, financial entities as customers are already dedicated to compliance with requirements securing operational resilience, engaging in information collection and dialogue with the CTPPs themselves. European banks believe there to be synergies in this workstreams and information flow with the DORA proposal. Where the latter would advance the information flow not only between CTPPs and public authorities, but also considering the providers' clients, all sides can benefit from more efficient exchanges, reducing burdens on personnel and operations.

CTPP-customer firms should be able to leverage DORA, supporting further the effectiveness of processes. As part of a synergy gain, this could avoid duplications of monitoring activities by banks, that have already been conducted by the Lead Overseer. By gaining access to the information provided by critical ICT TPPs to authorities in the context of their new oversight, banks' own monitoring processes could benefit from organization efficiency, and avoid unnecessary costs without reducing the commitment to security or accountability. The information collected by authorities could not only help to address concentration risk and its management at a system level but help to avoid workload-intensive duplication of the same monitoring activities by a large number of banks under individual obligations. This enhances sector efficiency and frees up means for investment in further important technological innovation.

Access to the Lead Overseer's recommendations

TPP customers should learn about the issued recommendations by the Lead Overseer to address identified shortcomings in a timely manner. Art. 37 (2) expects national competent authorities to monitor whether financial entities take into account the risks identified in the recommendations addressed to CTPPs. However, financial entities are not included in the distribution of the issued recommendations in the first place. We call upon the EU legislator to amend Art. 35 (5) sub-para. 1, adding the financial entities who are

customers of the CTPP in question, to the list of recipients of the Lead Overseer' recommendations for the relevant services they consume.

For financial entities to take risks into account, early awareness building – based on available information – is important. The timely access to the recommendations would be a helpful step to support financial entities appropriate risk mitigation. The communication of monitoring findings and supervisory reactions with CTPPs' customers under the oversight framework can provide actionable intelligence to financial entities. Ultimately, access to the recommendations can help to avoid unnecessary steps in information sharing due to different layers in the communication process.

We believe that the proposed access to the recommendations is compatible with the ESAs' support for market transparency by publication of the recommendations. As expressed in the letter from 9 February, the ESAs' support a publication of high-level information on the number and types of recommendations issued to each CTPP. While the full recommendations should not be indiscriminately published due to confidentiality and competition aspects, they should still be shared in full with the CTPP customers in question, as they could leverage the previous work by the Lead Overseer to further adapt their risk management framework. A public intention by each CTPP to follow the recommendations, though without apparent enforcement capability, appears to be a useful tool to enhance transparency at the market. We encourage a notification of CTPPs' customers by the provider, once it has issued such intention.

Receiving information about on-site inspections
Art. 34 (3) calls for information of national competent authorities (NCAs) by the Lead Overseer in good time before an on-site inspection. Those financial entities which are customers of the CTPP should be informed in addition to the NCA. To that end, Article 34 (3) should be amended:

> "In good time before the inspection, Lead Overseers shall inform the competent authorities and of the financial entities using that ICT third-party provider. **Where information is requested from the provider, the financial entities using that provider shall be informed by the Lead Overseer that a request was issued**."

The EBF emphasizes that termination of the contractual arrangement by the competent authority should not be a standard enforcement tool, since it carries significant risk

Art. 37 (3) grants the competence to NCAs to require a financial entity to terminate, in part or completely, the contractual arrangement. This option appears to insufficiently consider the detrimental effect that such termination can have on the business operation of the CTPP's customer. A termination of service provision by a CTPP is a complex endeavour, requiring a strategic retraction of data and shift towards in-house or alternative service providers so as not to disrupt the business operations in question. Business continuity is key. **Considering the relevance of the CTTP's service, demonstrated by the designation of criticality in the first place, an abrupt termination can carry significant risk to the operational resilience and business continuity of a financial entity.** Termination and exit require security and control under

a financial entity's exit strategy. In turn, it cannot become a standard enforcement tool, to be frivolously applied. Considering EBA GL on outsourcing para. 105, an outsourcing agreement *may* be terminated only *if necessary*. Remedial actions and corrections shall be *appropriate*. Art. 37 (3) DORA should align with this evaluation of appropriateness prior to any consideration of termination.

Therefore, we urge the EU legislator to explicitly include a reference under Art. 37 (3) outlining the right to call for (partial) termination only as an action of last resort. There are considerable alternatives and less-intrusive measures available, providing for a more proportionate reaction while avoiding detrimental burden for CTPP customers in the earlier escalation process. At a first stage, a severe warning should be issued to the financial entity, indicating in detail the identified risk and failure of the CTPP to comply with recommendations of the Lead Overseer. In line with the point made earlier in this paper, these recommendations should be communicated to the financial entity. Should this prove insufficient to trigger a risk mitigation, a temporary freeze could be issued for the ICT-service provider: no signing of new contracts and no extension or renewal of existing contracts. Such freeze could be upheld until the CTPP has proven the remediation of shortcoming impacting the consuming parties. It should be part of the annual published report from the Lead Overseer, clearly stating the announced freeze periods or already effective freeze sanctions.

In its current form, Art. 37 (3) does not reflect the reality of multiple innovative services being consumed by a financial entity under a shared contractual arrangement. In turn, the partial or complete termination is not a proportionately tailored approach to mitigate individual risks identified for a single service under such umbrella contract.

We propose the amendment of Art. 37 (3) in the following way:

> **"Where regulatory objectives cannot be ensured by other measures, subject to approval by the Oversight Forum**, competent authorities may, in accordance with Article 44**, issue warnings to financial entities regarding the risks identified as a result of the oversight process. Following a warning, competent authorities may** require financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party provider until the risks identified in the recommendations addressed to critical ICT third-party providers have been addressed. Where necessary, they may require financial entities **– as a matter of last resort -** to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers. **Before such decision, the competent authority shall hear the financial entity in question and consider the detrimental impact of the potential request of termination for business continuity and additional burden on the financial entity. Once a decision has been taken, the competent authority shall allow sufficient time for financial entities addressed by the decision to adjust their outsourcing arrangements in such a way as to not jeopardise digital operational resilience."**

The competence to terminate under Art. 37 (3) is based on the Art 25 (8), introducing an obligation for financial entities to ensure designated termination rights under the

contractual arrangements. Already this provision should clarify that termination will only be required if remediation of the identified concern is not possible. Such analysis by the NCA needs to consider measures proposed and implemented by the financial entity in question, possibly mitigation identified risks to the point where termination (or even a suspension) is no longer an appropriate action to request. Without such important framing, paragraph 8 introduces market uncertainty over the continuous use of ICT TPPs in Europe.

Furthermore, European banks call upon the EU legislator to amend Art. 37 (4), to reflect better the necessary proportionality in a NCA's decision on termination. Adding to the list of existing criteria (a) to (d), we propose a new (e): "*whether the suspension or termination introduces a risk for the business operations of the customer of the critical third-party provider*". Considerations of risk by the NCA should specifically consider necessary time for a customer to migrate complex service solutions safely, since disproportionally short timeframes for suspension or termination create new, and unnecessary, risk for operational resilience.

In order to secure a harmonized approach of follow-up actions under Art. 37, we suggest including a mandatory *coordination* of the NCA with the Lead Overseer under Art. 37 (5). Rather than just *informing* the Overseer regularly, NCAs should receive the latter's feedback on the measure considered by the NCA before the action is enforced. This coordination should explicitly consider the fragmentation that such action would create for financial entities service provision across borders and in different jurisdictions.

The EBF recommends enhanced promotion of certification schemes for ICT providers

Leveraging the Cybersecurity Act, the Commission is advised to explore the possibility to promote certification schemes for ICT providers, in line with initiatives such as the ENISA Working Group on a cloud security certification scheme, which is applicable to the financial sector. This could help towards a more efficient process of assessing TPP risks. Such certification schemes should take note of existing industry initiatives and standards established in the market. Looking at a shared controls landscape with technology solutions such as cloud computing, standards applied by the financial industry can help to address central issues from an established best practice perspective. Additionally, the Third-Party Statements in SOCII already give insight into the operational effectiveness of agreed controls in a shared controls landscape (e.g. for cloud computing).

Among relevant best practices and internationally recognized standards, the Commission is invited to consider references such as the Cloud Security Alliance Cloud Security Matrix (CSA CCM), security standards ISO 27001/27002/27017/27018, NIST SP 880-43, COBIT, CIS Critical Security Controls and Business Continuity Planning standard ISO 22301.

The EBF invites clarification and amendments for the oversight framework of CTPPs

In order to benefit from operational resilience based on stronger harmonization of applicable oversight powers, we welcome a strong legal certainty in the Art. 28 to 35. In

the following, individual aspects are highlighted due to the need of clarification or amendment.

Article 28 (6): A yearly publication frequency cannot determine the reaction time of financial entities to these published changes in designation. There needs to be time allowed for FIs to react to changes to the list of CTPPs as banks will need to adjust their contracts and potentially security arrangements. In some circumstances, banks may need to reconsider the relationship with the provider. In addition, the providers themselves will need an implementation period in order to allow for them to change their compliance to meet heightened expectations from their FI customers that result from their updated designation. We suggest an appropriate period of time, aiming at 12 months, between the identification of an ICT TPP as critical and that designation coming into effect. Financial entities require such timeframe to react to the changed provider determination, and we welcome necessary flexibility of the competent authorities by way of extensions for customers to react in time (waiver option). Without impact on the financial entities' dedication to a risk-based approach, such waiver could help catering to the complexities related to a provider being determined as critical.

Article 30 (2) (e): The word "major" should be added before "ICT-related incident".

Article 31 (1) (a): appropriate safeguards are needed to ensure the confidentiality of the CTPP's clients' data.

Article 31 (1) (d) (iv): The requirement should be changed to notification rather than refrain as there is no justification for forbidding sub-contracting based purely on the legal residence of the provider. This requirement moves very closely to a prescription against extra-EU supply chains. If this were repeated in other jurisdictions it could cause significant damage to the global operating model of EU banks. Please consider our suggestion to clarify the definition of the ÏCT sub-contractor established in a third country under Art. 3 (20).

Article 32 (1), (2): limits must be put in place to ensure confidentiality and security of client data held by the CTPP. At a minimum FIs need to be notified of any such request pertaining to their data. We believe that a reference to a "simple request" is not a stringent enough legal basis for obtaining such information. We welcome a clarifying reference to the request based on a concrete power of the Lead Overseer under Art. 31, stating clearly the purpose of information use only for oversight of the provider, not for separate compliance investigations targeting the CTPP customers. Alternatively, 32 (2) (b) could clarify that such requests will be limited to the data of the CTPP and not their clients.

Article 32 (5): The following text should be added to the first paragraph:

> "The Lead Overseer shall, without delay, send a copy of the decision to supply information to the competent authorities of the financial entities using the critical ICT third-party providers' services. **The critical ICT third-party provider shall without delay notify their clients of the Recommendations received from the Lead Overseer."**

It is desirable that financial entities be made aware of risks identified by the Lead Overseer and recommendations made to the CTPP so that they can assess the findings and make any necessary changes to the security controls they have in place or their contractual arrangements. Financial entities must also be informed of the Recommendations in order to comply with DORA, notably Art. 37(2). The proposed amendment facilitates a direct

discussion between the CTPP and the financial entity, ensuring that the risks and mitigations are properly communicated and understood.

CHAPTER VI: INFORMATION SHARING ARRANGEMENTS

The EBF calls for enabling the establishment of meaningful and voluntary cyber threat information-sharing arrangements among trusted circles (Article 40)

While the provision in the proposed Regulation for facilitating the establishment of cyber threat information sharing arrangements among financial institutions is welcome and in line with calls from industry, **it needs to be formulated in a way that ensures the voluntary nature of such arrangements**.

Involving public authorities in cyber threat information-sharing mechanisms that are meant to be a tool for the industry and for timely exchange of crucial information to efficiently identify, prevent and address threats within trusted circles does not seem to be opportune. There is need to clarify **the rationale of the public authorities' involvement**, as well as **the conditions** under which this would be realized.

Authorities in their capacity as regulators, overseers and/or supervisors should not have access to the info-sharing network. Regulatory reporting on cyber incidents and data breaches should be outside the scope of the intelligence sharing within the European community. The ECRB, central banks, as well as other ESAs could be involved in the form of periodic (quarterly or biannually) meetings between the circle of trust group and public authorities as a path to foster collaboration and transparency, maintaining a highly trusted cybersecurity ecosystem and enforcing the Public Private Partnerships (PPPs) that have been created over the years. On such occasions, it is fundamental that the ECB ensure that an internal "Chinese Wall" separates its Security Operating Centre and its system operator function from its regulatory, oversight and supervisory functions.

It is not clear what is the objective of introducing an **obligation for financial entities to notify competent authorities** of their participation in information sharing arrangements, and it **creates a new and unnecessary burden, while also jeopardizing the voluntary nature of such schemes**. There could be strategic considerations behind the decision to participate in info-sharing schemes, and the arrangements among FIs (or between the FI and other institutions/other sector operators/TPs/FinTechs, etc.) could be large in terms of number, or dynamic in terms of validation/cessation. Therefore, the notification requirement should be removed.

Additionally, the proposal needs to include **amendments to the EU data protection legislation** when it comes to establishing such schemes in order to lift existing obstacles of legal uncertainty that often impede an efficient cyber threat information-sharing, especially when these involve personally identifiable information (PII). More specifically, it is important to define cases of exception when information-sharing can lead to high benefits, e.g. in the anti-fraud context, in which difficulties related to the presence of data associated to physical persons may be encountered.

The EBF is of the view that information-sharing should be **implemented through information-sharing arrangements that protect the potentially sensitive nature** of the information shared, such as via CERTs or using MISP.

CHAPTER VII: COMPETENT AUTHORITIES

Article 46: Regarding the provisions on criminal penalties, since the accomplice of the offense is punished like the main "actor", a bank linked to a failing service provider, in particular in terms of personal data protection, would risk being called into question.

Another issue to be highlighted is the cumulation of the sanctions provided for in articles 44 in DORA with the sanctions provided for elsewhere (e.g. GDPR and national legislations).

Article 48 (1), (2): The EBF believes that certain information should remain confidential or should be published only in a restricted circle. Therefore, the nature of the incident and the identity of the individuals should not be published on a public website.

Article 49 (3): Information covered by professional secrecy should not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national legislation.

CHAPTER IX: TRANSITIONAL AND FINAL PROVISIONS

Article 56: The application times of the proposal are unrealistic, as previous experience with other comparable regulations has demonstrated. A period of 3 years to comply will be more realistic.

The EBF underlines the inconsistencies in the timetable for bringing the financial sector into conformity with the DORA stipulations. The proposal foresees one year for application of the regulation and, at the same time, it mandates European agencies to develop RTS within 1 to 3 years after its entry into force. However, the use of these elements by financial institutions is required by DORA. **Firms cannot comply within one year with the proposal's provisions and then review their processes with regard to the new requirements in RTS**. Also, a period of one year to apply this proposal as it stands is not possible, especially if the text prohibits the use of non-EU established critical ICT TPPs.

Therefore, the EBF proposes that **this Regulation's provisions shall apply after a reasonable amount of time has passed after the publication of the RTS.** For orientation, we suggest a period of three years for the EU legislator's consideration, understanding well the need to balance the need for timely action with proportional expectations.

FURTHER REMARKS:

The EBF believes that the numerous Regulatory Technical Standards (RTS) delegated to the ESAs should not be too prescriptive, providing flexibility in the measures they adopt

It is crucial that the **future RTS be directed towards harmonisation, providing flexibility** for financial institutions. They should leave room for FIs to follow their own risk-based approaches and be rightly aligned so as to be implemented in a sound way.

The EBF remains committed to further contribute to shaping the RTS in a way that they address the industry needs and avoid unnecessary burdens and excessive prescriptiveness that would lead to the opposite results than those intended by the proposed Regulation.

It is also essential that FIs are provided with sufficient implementation time between the publication of the RTS and the compliance date. In particular the changes to reporting processes and formats and the complex requirements for policies and internal governance arrangements will take time to implement. Also, as highlighted above, the RTS should be released at the time when the proposal shall apply, which the EBF suggests being in 3 to 5 years after entering into force.

For more information:

Alexandra Maniati
Director of Innovation & Cybersecurity
a.maniati@ebf.eu

Julian Schmücker
Senior Policy Adviser – Digital Innovation
j.schmucker@ebf.eu

Dimos Karalis
Policy Adviser – Innovation & Cybersecurity
d.karalis@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu