EU Digital Operational Resilience Regulation (DORA)

Barclays Position Paper

Barclays welcomes the European Commission's proposal for a 'Regulation on Digital Operational Resilience in the Financial Sector' (DORA).

Barclays recognises that an increasingly digital financial services sector raises the importance of ICT and security resilience for firms. We believe the Commission's proposal is a positive step towards a harmonised EU framework that will improve the digital operational resilience of financial services firms across the EU. However, we believe there are certain areas of the proposal which would benefit from further clarification or amendment to best achieve the desired objectives. Our high level views on the proposal are set out below, chapter by chapter. A detailed breakdown of suggested changes article by article is provided in the annex.

Barclays would welcome the opportunity to discuss these issues in more detail, as the proposal is negotiated by the EU institutions.

Key Issues

1. **Clarity that regulated entities providing ICT services exclusively to other entities within a consolidated financial services group do not fall under the definition of an "ICT third party service provider".**

Many international financial services groups are structured to have a group service company that provides certain services or functions (e.g. IT, HR) to other entities within the group. Indeed, this operating model is used extensively across the EU and international banking sector for recovery and resolution planning purposes as the operational continuity vehicle for the group. These intragroup service firms typically do not provide ICT services to any entities outside of their group.

Under the proposed DORA Regulation, it is not currently clear whether such intragroup service firms could fall under the definition of an 'ICT third party service provider', and subsequently, potentially as a 'critical third party provider'. We do not believe that is the intention of the draft legislation, but would kindly ask for clarification on this point.

Barclays believes that intra-group service firms should not be covered by the definition of an ICT third party service provider, for the following reasons:

- The broad policy intention of DORA is to ensure any ICT risks posed to a financial institution by an ICT third party service provider are effectively managed. The proposed measures in DORA are appropriate to manage third party ICT risk, where the service provider is a genuine third party entity i.e. a completely separate institution with its own commercial interests. However, in contrast, the interests of intragroup service firms are aligned with the other entities in the group to which they provide services in terms of effectively managing risk, and ensuring robust service provision. Intragroup service firms are ultimately subject to the same common senior management oversight at the group executive and board level. As such, intragroup service firms, even where providing ICT services, do not pose the same risk as genuine third party service providers.

- Further, intragroup services firms are already regulated and supervised by the relevant financial services national competent authority. They are also typically included in resolution and recovery plans at the group and subsidiary level to ensure operation continuity in times of group stress. If these regulated intragroup service firms are covered by the definition of an 'ICT third party service provider', they could theoretically also be deemed a 'critical ICT third party service provider' and therefore be subject to the new supervisory framework envisaged for these entities by DORA. This would result in intragroup service firms potentially subject to two supervisory frameworks intended for different types of firm: supervision by the financial services NCA as a regulated financial services entity; and separate supervision if deemed a critical ICT third party service provider under DORA. We understand the intention behind the new supervisory framework is to ensure major ICT third party providers deemed to be critical are subject to appropriate supervision in the EU. Barclays broadly supports this intention. However, the potential for regulated intragroup service firms providing services within a financial services group to be caught as an 'ICT third party service provider' creates an unintended consequence with implications that would conflict from a supervisory perspective.

Barclays therefore believes the Regulation should be amended to make clearer that regulated entities providing ICT services exclusively to other entities within a financial services group are not third party entities for the purpose of DORA. It should be expressly stated that such intra-group service entities do not fall within by the definition of an 'ICT third party service provider', nor the definition of a 'critical third party provider'.

2. Clarity on the criteria for determining 'Critical Third Party Service Providers'

Currently, the criteria to determine which ICT third party service providers are 'critical' - and therefore subject to the new supervisory oversight framework - are high level and overly vague, with DORA proposing that the Commission will supplement the criteria with more detail via subsequent technical standards (level 2). This lack of clarity regarding the precise nature of which providers are intended to be covered by this definition creates significant uncertainty for financial entities, who are required to determine subjectively which of their ICT third party service providers may or may not be deemed critical under the Regulation, across a broad spectrum of services these suppliers may provide.

Given the implications of Article 28.9, as currently drafted, this creates a significant operational risk to international firms with suppliers located in different jurisdictions around the world – a model extensively employed in the financial services sector by both EU and non-EU headquartered operators alike. Legal and technical certainty would be much improved if policymakers provide more detailed and objective criteria to determine which ICT third party service providers are critical in the level 1 text. The key criteria to determine criticality should include: i) the number and significance of EU financial services firms being supplied by the provider; ii) the extent to which the ICT third party service provider is systemic to the operation of the EU's financial system (applying mature and transparent criteria such as that used to determine G-SIIs by the EBA); iii) the proportion of the ICT third party service providers' services which are provided to external clients and iv) the materiality of these services.

3. Ensuring that EU financial entities are able to rely on entities within their group, but located outside the EU, to demonstrate compliance with the requirements of DORA.

There are currently various, robust supervisory frameworks which apply to international financial institutions designed to ensure EU regulators and supervisors have appropriate oversight of digital operational resilience activities, both at jurisdictional and group level. For example, Barclays' own supervisory arrangements enable the SSM and the Central Bank of Ireland to monitor and enforce compliance by Barclays' European entity with various ECB/EBA/ESMA guidelines regarding ICT provision, delegation and outsourcing of services to our group service company (in the UK) which undertakes digital operational resilience activity for the entire group.

It is essential that global institutions are able to continue delegating/outsourcing certain digital operational resilience activities to group entities outside of the EU in order to ensure the operational effectiveness of centralised systems. Importantly, these arrangements are documented on robust, arms-length terms that comply with all relevant regulations.

While the Regulation includes specific provisions enabling firms to delegate/outsource certain obligations to intragroup or external undertakings (Art 5.10 on verifying compliance with the ICT risk management requirements, and Art 17.4 on reporting requirements), it is not clear as to whether EU financial entities are able to rely on entities within their group, but located outside the EU, to demonstrate compliance with the requirements of DORA. If EU based entities covered by the Regulation are prevented from such delegation or outsourcing, there is a risk that firms may be required to establish a local ICT resilience team to undertake activities within the EU, simply to comply with DORA. This would have the effect of fragmenting international firms' group-wide ICT risk management strategies, diluting efforts and resources from a single resilience approach, and ultimately delivering poorer operational resilience in the EU – the opposite of DORA's objective.

Policymakers should therefore ensure that EU firms may continue to delegate to, and rely on, entities within their group, but located outside the EU, to meet the requirements of DORA. Naturally, the EU firm would retain full responsibility for its compliance, enabling appropriate oversight capabilities for the relevant European competent supervisory authorities.

4. Mutual Recognition of TLPT test results, between EU Member States, as well as with third country jurisdictions.

Barclays supports the intention to introduce a strong and harmonised framework for the testing of firms' ICT systems across the EU. However, the proposal does not include any specific provisions facilitating the recognition of Threat Level Penetration Test (TLPT) results across different member states within the EU. Without an effective framework for mutual recognition of TLPT test results, firms will be required to undertake TLPT testing in each Member State in which they operate, which risks being duplicative, impractical and extremely resource intensive.

Furthermore, there are currently no provisions allowing recognition of TLPT testing undertaken in jurisdictions outside the EU. International financial services groups operating around the world may be subject to different digital operational resilience and testing frameworks in different jurisdictions. To avoid the risk of regulatory fragmentation and potentially costly requirements for separate tests to be undertaken in each jurisdiction, policymakers should include in the regulation a mutual recognition framework allowing TLPT tests undertaken in trusted third countries to be recognised

under this framework. In addition, policymakers should look to work with international partners to harmonise requirements wherever possible (e.g. TIBER-EU and CBEST).

Barclays Position - By Chapter

Chapter I – General Provisions

Support broad scope - Barclays supports the broad scope of financial services firms covered by the proposed legislation. It is important all financial services firms have a strong framework in place to ensure digital operational resilience.

Definitions inconsistent with international standards - The proposal introduces new definitions for certain terms that are inconsistent with internationally recognised definitions as part of the FSB Cyber lexicon. To avoid any regulatory uncertainty, these definitions should be amended to be consistent with the FSB Cyber Lexicon definitions where possible.

Chapter II - ICT Risk Management Framework

Rules overly prescriptive - We note the proposal is intended to be principle based in its approach, however many of the requirements in this section are, in our view, overly prescriptive, for example setting out detailed, specific requirements on firms across each ICT risk management area. We believe the proposal should ensure its approach is principle / outcome based, providing firms with flexibility to achieve the desired outcomes through their own approach rather than setting out specific operational measures to be taken by firms.

Interaction with EBA ICT guidelines - It is currently unclear how the requirements in Article 5 (ICT Risk Management) interact with the EBA ICT guidelines which are applicable to financial services firms. Further clarity on this interplay would be welcomed to avoid duplication or inconsistency, ahead of the proposal entering into force.

Chapter III - ICT Incident Reporting

Interaction with FSB Toolkit on CIRR - The recently developed FSB toolkit on Cyber Incident Response and Recovery set outs best practice for incident reporting. It is currently unclear how the requirements in the proposal interact with those in the FSB toolkit. In order to avoid regulatory uncertainty, policymakers should look to ensure that these are consistent.

Definition of Major ICT-related incidents – we note this definition is linked to '*potential*' impact and broader in scope than analogous definitions under other regulatory frameworks such as NISD and GDPR, which tend to peg requirements to a '*likely*' impact. Such a distinction, without a clear materiality threshold, seems disproportionate and will likely lead to firms over-reporting, contrary to the stated objectives of DORA.

Timing of reports - Barclays recognises the desire for regulators to be provided with detailed information on incidents as soon as possible. However, Barclays would stress the importance of firms having the flexibility to appropriately manage and respond to incidents, without having to divert critical time and resource to meet overly onerous reporting requirements. Policymakers should provide greater flexibility for firms in the timing of reporting requirements. This includes in relation to any final reports, where imposing a fixed one month deadline (where analysis and mitigation may still be ongoing) may not drive the best incident management culture.

Sharing of reports between authorities - Barclays supports the intention for incident reports to be shared with other EU authorities, however it is important this is undertaken securely and confidentially given the potentially sensitive nature of major incident reports. Further, policymakers should consider the extent to which incident reports could be reciprocally shared with authorities in trusted third countries outside of the EU, for example the UK following the potential agreement of a UK-EU MOU for financial services.

Single reporting hub - Barclays supports the intention to create a single EU hub for reporting of major incidents. Such a hub can improve efficiency of incident reporting and sharing of reports across the EU.

Feedback from authorities - Barclays supports the proposals' intention for authorities to provide feedback to a financial entity following an incident report. Policymakers should consider whether there could be an obligation for the authorities to provide feedback, insight and intelligence to all relevant firms where it could be beneficial, based on any major incident reports they receive. Such a provision could support the broader financial services sector in its preparedness and response to any industry-wide threats.

Chapter IV - Digital Operational Resilience Testing

Mutual recognition of test results across the EU - Barclays supports the intention to introduce a strong and harmonised framework for the testing of firms' ICT systems across the EU. We note that in the Explanatory Memorandum and the Recitals there are multiple references to the need for mutual recognition of testing results across the EU. However, we would note that the proposal does not include any specific provisions facilitating the recognition of Threat Level Penetration Test (TLPT) results across different member states within the EU. Without an effective framework for mutual recognition of TLPT test results, firms will be required to undertake TLPT testing in each Member State in which they operate, which risks being duplicative, impractical and extremely resource intensive.

Mutual recognition of test results from third country jurisdictions - Furthermore, there are currently no provisions allowing recognition of TLPT testing undertaken in jurisdictions outside the EU. International financial services groups operating around the world may be subject to different digital operational resilience and testing frameworks in different jurisdictions. To avoid the risk of regulatory fragmentation and potentially costly requirements for separate tests to be undertaken in each jurisdiction, policymakers should include in the regulation a mutual recognition framework allowing TLPT tests undertaken in trusted third countries to be recognised under this framework. In addition, policymakers should look to work with international partners to harmonise requirements wherever possible (e.g. TIBER-EU and CBEST).

Interaction with TIBER–EU - Regarding the requirements for firms to have independent testing firms undertake TLPT on critical live ICT systems, there is no mention of the ECB's TIBER-EU testing framework. Policymakers should clarify how the requirements in the proposal relate to and interact with the ECB's existing framework.

Testing firm requirements - Regarding the use of external testers for TLPT testing, the recitals state that TLPT testing can be undertaken by either internal or external testers, providing they are independent. However, articles in the proposal suggest testing must be outsourced to external testers. Many firms may have their own independent testing teams, with a comprehensive

understanding of the firm's ICT infrastructure and therefore the abilities to undertake rigorous testing. Policymakers should therefore clarify in the proposal's articles that TLPT testing can be undertaken by internal testing teams, providing they are independent.

Chapter V – Managing ICT Third Party Risk

Interaction with EBA Outsourcing Guidelines - EU financial services firms are currently required to comply with the EBA's 2019 Outsourcing Guidelines, when managing third party risk. It is not clear exactly how the new provisions in this proposal interact with the EBA Guidelines, creating regulatory uncertainty and the risk of duplication or a conflict in approach. The EBA Guidelines are relatively new and many firms are still in the process of transitioning fully to the new requirements. Policymakers should clarify whether Chapter V is intended to replace these wholesale, or sit alongside the existing EBA Guidelines in some way. In either scenario, the relationship between the existing contract requirements in the EBA Guidelines and Art 25.11.a of DORA needs to be reconciled and the impact (cost/benefit analysis) of transitioning any existing contractual arrangements from EBA Guidelines to DORA compliance properly assessed.

Oversight of CTPPs - Barclays recognises policymakers' desire for stronger oversight over critical third party providers that provide services to firms in the EU, and we support the intentions behind the proposal.

Restrictions on use of non-EU CTPPs (Art28.9) - However, we would caution against provisions prohibiting the use of third party providers based outside the EU, if they are deemed to provide critical services to firms within the EU. While we understand this provision may be intended to reduce potential risks posed to the system due to a lack of supervisory oversight, reducing access to advanced technology and services from non-EU ICT third party providers that support firms' resilience would not only lead to lesser choice (and therefore impact risk diversification), but also create other adverse impacts (e.g. operational complexity for firms that may need to amend their supplier arrangements). If it is the intention that critical TPPs would be required to establish EU subsidiaries, there would need to be much greater clarity surrounding whether a particular provider meets the criteria for criticality under Article 28. The current test appears overly subjective and places an undue onus on the recipient of the services to determine whether a particular TPP, which may have many touchpoints with a financial services organisation, in multiple jurisdictions, is 'critical' in relation to any or all services it provides.

We also note that Article 28.9 as drafted does not appear to be in line with the recent EBA Guidelines on outsourcing arrangements. This provision therefore risks further global fragmentation of ICT providers and risk management frameworks, contrary to the objectives of DORA

Ability to contract on a global basis - Large global financial entities typically procure services through enterprise wide agreements, which may support multiple group companies situated in different jurisdictions and a number of distinct services, some of which may be more material than others. Such an enterprise-wide approach helps to manage legal risk and improves operational resilience, by providing better group-level oversight of suppliers and contractual consistency in terms of managing any ICT-related risks. It is important that DORA does not require EU entities within a multinational group to contract for critical ICT services separately to these enterprise –wide agreements. This would cause unnecessary fragmentation and introduce operational risks, contrary to the stated purposes of DORA. It would also require unwinding a large volume of existing

agreements, many of which will have been repapered very recently in light of the EBA Guidelines, and risks arbitrarily constraining supplier selection and access to the most innovative technologies, to the detriment of the financial services sector and our clients and customers.

Powers of the Lead Overseer and National Competent Authorities:

- **Termination powers of national competent authorities** – The DORA proposal grants national competent authorities further intervention powers to require firms to temporarily suspend (or terminate) the use of a critical ICT third party provider until recommendations made by their lead overseer have been addressed. This could have a severe impact on firms' ability to serve their clients and customers as well as their operational resilience. Barclays would therefore urge that this power should only be considered as an extreme last resort option, where concerns of the Lead Overseer cannot be addressed by alternative means. We would also urge that in such circumstances impacted firms are given sufficient notice and time to make necessary arrangements for a controlled and secure transition to alternative providers, and consider any other additional fall-back options.
- **Powers to make recommendations on contractual terms –** DORA provides the Lead Overseer with the power to make recommendations on the contractual terms and conditions under which Critical TPPs provide services to financial entities. While we appreciate the Commission's intention is to manage risk, the power to intervene on the terms of contractual agreements risks undermining firms' approaches to managing supplier relationships, by making standard agreements very difficult to manage, and potentially conflicting with supplier management in other jurisdictions.
- **Monitoring and enforcement by the national competent authority –** DORA requires that national competent authorities monitor whether financial entities take into account the risks identified in the recommendations addressed to critical TPP by the Lead Overseer. More detail should be provided as to how this would work in practice.

Chapter VI – Information Sharing Arrangements

Support for information sharing - Barclays supports the proposals' intentions to enable cyber threat intelligence sharing between firms. Given many data sharing frameworks already exist across the sector, Barclays believes that participation in any particular framework should be voluntary, and should be a strategic decision for individual firms.

Clarity on sharing of IP addresses - Barclays notes the proposal would require any information sharing arrangement to be governed by rules respecting the protection of data i.e. GDPR. Policymakers should clarify whether firms are permitted to share potentially personal data such as IP addresses with other firms, for the purpose of preventing cyber threats.

Chapter IX – Transitional and Final Provisions

Date of application – DORA currently proposes that the requirements of the Regulation will start to apply 12 months after the date of entry into force. Given the technical complexity of DORA's requirements, and the significant change they will require from firms, for example, re-contracting with suppliers, the time between entry into force and the date of application of the rules should be extended to provide firms with greater time for implementation.

Annex – Detailed Article Breakdown

Chapter I – General Provisions

Article	Description / Text	Problem / Change Required
Art 3 Definitions	• Network and information system (Art. 3.2); • Information asset (Art. 3.5); • ICT-related incident (Art. 3.6); • Cyber threat (Art. 3.8); • Cyber-attack (Art. 3.9); • Threat intelligence (Art. 3.10); • Defence-in-depth (Art. 3.11); • Vulnerability (Art. 3.12); • Threat led penetration testing (Art. 3.13)).	**Problem** - Definitions are inconsistent with existing globally recognised terms, e.g. FSB Cyber Lexicon[1] **Change required** - Definitions should be amended to be consistent with the FSB Cyber Lexicon.

Chapter II - ICT Risk Management Framework

Article	Description / Text	Problem / Change Required (Clarification, Amend, Remove)
Art 4.2 Governance and Organisation	*The **management body** of the financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework…* • *Lists various requirements for the management body*	**Problem** – The provisions are too prescriptive in their requirements for the management body – actions like this should be taken by the appropriate governance management function. **Change** – Activities in 4.2 should be undertaken by the appropriate governance management function, with a flexible requirement for firms to ensure the management body is included as appropriate.
Art 7 Identification	*Proposal lists specific requirements of firms regarding the identification of business functions and supporting data and systems.*	**Problem** – The requirements proposed are overly prescriptive. **Change required –** Proposal should take a principle / outcome based approach, providing firms with flexibility to achieve the desired outcomes through their own approach.
Art 7.1 Identification	*As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all **ICT-related business functions**,…*	**Problem** - Unclear what is meant by 'ICT-related business function'. **Change** - Further clarity required.
Art 8.3 Protection and Prevention	*To achieve the objectives referred to in paragraph 2, financial entities shall use **state-of-the-art** ICT technology and processes which…*	**Problem** – Unclear what is meant by state-of-the-art. Removes flexibility to utilise the most suitable tool. **Change** – Amend 'state of the art' to 'suitable' or 'appropriate' technology.

[1] FSB Cyber Lexicon (November 2018)

Art 8.4 Protection and Prevention	*Proposal lists specific requirements of firms regarding the protection of ICT systems.*	**Problem** – The requirements proposed are overly prescriptive. **Change required –** Proposal should take a principle / outcome based approach, providing firms with flexibility to achieve the desired outcomes through their own approach.
Art 8.4.a Protection and Prevention	*As part of the ICT risk management framework referred to in Article 5(1), financial entities shall:* *(a) develop and document an information security policy defining rules to protect the confidentiality, integrity and availability of theirs, and* ***their customers' ICT resources****, data and information assets;*	**Problem** – While firms can protect against customers' ICT impacting on the security of the bank, firms should not be responsible for ensuring the protection of customers' own devices. **Change required** – Clarity required on what is meant by 'customers' ICT resources'. Should be removed if it is the case that firms would be responsible for protecting customers' ICT devices.
Art 10.9 Response and Recovery	*Financial entities other than microenterprises shall report to competent authorities* ***all costs and losses caused by ICT disruptions and ICT-related incidents.***	**Problem –** it is not practical for firms to identify all 'costs' of incidents. **Change required –** provision should be removed.
Art 11.4 Backup Policies and Recovery methods	*Financial entities* ***shall maintain redundant ICT capacities*** *equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs.*	**Problem –** requirement is overly prescriptive. **Change required –** provision should be removed. Proposal should provide firms with flexibility to manage their approach.
Art 12.2 Learning and Evolving	*When implementing changes, financial entities other than microenterprises shall communicate those changes to the competent authorities.*	**Problem –** Reporting all changes made following an incident to the competent authorities would be impractical, and potentially unhelpful, given the potential number of changes made. **Change required –** Provision should be amended to clarify that only significant or fundamental changes should be reported.
Art 13.1 Communication	*Financial entities shall have in place communication plans enabling a responsible disclosure of ICT-related incidents or* ***major vulnerabilities*** *to clients and counterparts as well as to the public, as appropriate.*	**Problem –** Firms should not be required to disclose major vulnerabilities publicly. This creates unnecessary risk. **Change required –** delete 'major vulnerabilities'.

Chapter III - ICT Incident Reporting

Article	Description / Text	Problem / Change Required (Clarification, Amend, Remove)
Art 17.2, 17.3 Reporting of major	**17.2 -** *Where a major ICT-related incident has or may have an impact on the financial interests of service users and clients, financial entities shall, without undue delay, inform their service users*	**Problem –** Requirements of action to take during/following an incident are too prescriptive and risk diverting critical attention and resource away from appropriate management and response to the incident.

ICT-related incidents	*and clients about the major ICT-related incident and shall as soon as possible inform them of all measures which have been taken to mitigate the adverse effects of such incident.* **17.3** - *Financial entities shall submit …: (a) an initial notification, without delay, but no later than the end of the business day, or, in case of a major ICT-related incident that took place later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day…*	No clear materiality threshold for either the significance of the impact or likelihood of occurrence, risking unnecessary over-reporting. **Change required –** provisions should be amended to make clear that firms should, as a best practice, look to take the action at an appropriate time, subject to management of the incident being in hand. It should also be clarified that any timeframes should run from when a financial entity becomes aware of the incident, not when the incident 'took place', which may be different in practice.
Art 20.1 Supervisory Feedback	*…the competent authority shall acknowledge receipt of notification and shall as quickly as possible provide all necessary feedback or guidance to the financial entity…*	**Problem –** Feedback is only to the firm providing the incident report. **Change required –** to support broader industry preparedness for incidents, consider whether there could be an obligation for the authorities to provide appropriately anonymised feedback, insight and intelligence to all relevant firms where it could be beneficial, based on any major incident reports they receive.

Chapter IV - Digital Operational Resilience Testing

Article	Description / Text	Problem / Change Required (Clarification, Amend, Remove)
Art 23	*Advanced testing of ICT tools, systems and processes based on threat led penetration testing*	**Problem –** article includes no mention of the TIBER-EU framework. **Change required –** should clarify how these TLPT provisions relate to TIBER-EU
Art 23	*Advanced testing of ICT tools, systems and processes based on threat led penetration testing*	**Problem –** article does not allow for mutual recognition of TLPT test results. **Change required –** should include provisions enabling mutual recognition of TLPT test results, both within the EU, and with trusted third country jurisdictions.
Art 23.2 Advanced testing of ICT tools, systems and processes based on TLPT	*… financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical functions and services, including functions and services outsourced or* ***contracted to ICT third-party service providers. Where ICT third-party service providers are included in the remit of the threat led penetration testing, the financial entity shall take the necessary measures to ensure the participation of these providers****.*	**Problem –** proposal requires firms to include third party providers in TLPT exercises where they support critical services. There is potential for a third party provider to provide services to many FS firms. They may then be required to participate in all firms' TLPT exercises, thus duplicating efforts and potentially putting their service provision at risk. **Change required** – requirement to include third party providers in TLPT exercises should be removed.

Art 23.3 Advanced testing of ICT tools, systems and processes based on TLPT	*Financial entities shall contract testers in accordance with Article 24 for the purposes of undertaking threat led penetration testing*	**Problem –** While article 21.4 states that testing should be undertaken by either internal or external testers, this provision appears to suggest testing must be outsourced to external testers. **Change required –** clarify that TLPT can be undertaken by internal testing teams, providing they are independent.

Chapter V – Managing ICT Third Party Risk

Article	Description and Problem	Change Required (Clarification, Amend, Remove)
Art 25.1 *General principles*	*Financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation.*	**Problem –** It is not clear how the new provisions in this proposal interact with the EBA Guidelines, therefore creating regulatory uncertainty. **Change required –** clarify whether/how the proposal is intended to replace or sit alongside the EBA Guidelines, including with respect to intra-group outsourcings.
Art 25.4 General principles	*As part of their ICT risk management framework, financial entities shall maintain and update at entity level and, at sub-consolidated and consolidated levels, a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.* *The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover critical or important functions and those that do not.* *Financial entities shall report at least yearly to the competent authorities information on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided.*	**Problem –** requirements to log and report to authorities' details of all uses of ICT third party providers is overly burdensome and disproportionate. **Change required –** provision should focus only on critical services.
Art 25.8.c General principles	*Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under the following circumstances:* *…ICT third-party service provider's* ***evidenced weaknesses*** *in its overall ICT risk management and in particular in the way it ensures the security and integrity of confidential, personal or otherwise*	**Problem –** requirements to log and report to authorities' details of all uses of ICT third party providers is too burdensome. Currently unclear what 'evidenced weakness' means i.e. whether it is specific to the services being provided under a contract, or broader.

	sensitive data or non-personal information	**Change required –**clarify what "evidenced weakness" means
Art 27 .2 Key contractual provisions	*Sets out detailed requirements for terms of contracts*	**Problem –** certain provisions are overly prescriptive and also extend to all contractual arrangements for ICT services and not just those supporting critical or important functions. **Change required –** provide greater flexibility and proportionality.
Art 28.9 Designation of critical ICT third-party service providers	*Financial entities shall 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.*	**Problem –** Provision potentially limits the availability of third party providers available to firms, and risks creating difficulties for firms with a cross-border operating model. It is also challenging for individual firms to assess whether a third country third party provider would be deemed critical if it were based in the EU. **Change required –** provision should be deleted, or at a minimum expressly exclude from its scope intra-group ICT service providers established in a third country
Art 37.3 Follow-up by competent authorities	*Competent authorities may, in accordance with Article 44, 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 to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers.*	**Problem** – this could have a significant impact on firms' service delivery and operational resilience. There is also a risk that different competent authorities across the EU might take divergent approaches in following up lead overseer recommendations. **Change required –** proposal should clarify that such powers are a last resort, and that firms would be provided with sufficient notice to transition to alternative providers. Policymakers should consider what guidance or mechanisms could be introduced to ensure national competent authorities are broadly aligned.

Chapter VI – Information Sharing Arrangements

Article	Description and Problem	Change Required (Clarification, Amend, Remove)
Art 40.1.c Information-sharing arrangements on cyber threat information and intelligence	*…is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct* ***in full respect of business confidentiality, protection of personal data*** *and guidelines on competition policy.*	**Problem** - any information sharing arrangement is to be governed by rules respecting the protection of data i.e. GDPR. **Change required –** Policymakers should clarify whether firms are permitted to share potentially personal data such as IP addresses with other firms, for the purpose of preventing cyber threats.