German Banking Industry Committee

Die Deutsche
Kreditwirtschaft

Comments

Consultation on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

Lobby Register No R001459

EU Transparency Register No 52646912360-95

Contact:
Berit Schimm
Telephone: +49 30 2021- 2111
E-mail: b.schimm@bvr.de

Berlin, 2023-09-08

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
National Association of German
Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

Comments Consultation on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

		Comments GBIC
	General Drafting Princiles	
Q1	Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (Complexity and risks considerations)? If not, please provide detailed justifications and alternative wording as needed.	No, the principle of proportionality envisaged in article 4 (DORA) is not reflected in the draft RTS. Art. 29/ RTS only provides for the consideration of ICT-related elements of increasing complexity and risk, not as in article 15 DORA outlined "the size and overall risk profile of the financial undertaking and the nature, scope and complexity of its services, activities and operations". Among financial institutions that are not subject to the simplified ICT framework, significant differences in size and scope/complexity of activities and operations can be identified. Even small banks generally do not benefit from the simplified framework due to the EU definition. The possibility of using further opening clauses in the RTS should therefore be provided. Proportionality should be applied consistently. We suggest to add more opening clauses that allows a more risk-oriented approach as carried out in our comments to Question 3 –26. Financial entities must be able to prioritise resources to risk. If all ICT assets, systems and threats are considered equally serious, the financial entity will lose the ability to prioritise and as a result will be materially worse at managing its risk. By more fully incorporating the idea of proportionality and a risk-based approach, as was done in the EBA's 2019 Guidelines on ICT and security risk management, we believe DORA and these RTS will become better standards by which financial entities can manage their digital operational resilience.
Q2	Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.	Yes, in principle. Proportionality should be applied consistently.
	ICT security policies, procedures, protocols and tools	
Q3	Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.	• Art. 1.2 (c): Can you provide provide further guidance on "In case of exceptions the digital operational resilience of the financial entity shall be ensured"? • Art.1.2 (h): There exist also national standards. Add "national standards" in the following sentence: "Take into account leading practices and relevant international or national standards, as appropriate". • Art. 2: Regarding RTS-background paragraph 31 we believe the statements regarding the internal organisation of the three lines of defense (LoD) model are confusing both in the RTS and the level 1 text. Some of the statements in Art. 2 of the RTS could be interpreted as forcing financial entities to locate their cybersecurity functions within the 2nd line of defense. Prescriptive requirements regarding which functions in a financial entity are located in which LoD should be avoided as

		many financial entities take different approaches in this regard. Similar comments were made by the industry in response to the EBA's draft Guidelines on ICT and Security Risk Management 2019. We recognise that the intention of the level 1 text and the RTS is to ensure appropriate independence and avoid conflicts of interests according to the 3LoD model. The industry supports this and suggests that further clarity could be provided by making additional statements in the background paragraphs of the RTS which would provide legal clarity for financial entities who might otherwise feel compelled to interpret those statements literally. Article 19 covers this sufficiently. We suggest the following amendment to be added to the background paragraphs of the RTS: "These RTS are not intended to prescribe to financial entities how to implement the lines of defense model for ICT and security risk management purposes, or to prescribe the location of certain functions within the 3 lines of defense model. " • Art. 2.1(f): Financial entities should retain the freedom to determine which function develops training and awareness programmes. In many firms, these are developed by the cybersecurity function located within the 1LoD. This has benefits as it allows the financial entity to incorporate relevant threat intelligence more easily. It is rightly the role of a control function to monitor effective implementation. We therefore suggest the following amendment: "Monitor the effective implementation of ICT security awareness programmes and digital operational resilience training referred to in Article 13(6) of Regulation (EU) 2022/2554."
Q4	Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.	We suggest a more risk-oriented approach: • Art. 3.1 (d) iii: The term "accepted ICT risks" (plural) should be used instead of "the accepted ICT risk" (which suggests an aggregated quantification of the individual risks). Amendment: "the development of an inventory of accepted residual ICT risks, including an explanation of the reasons for which they were accepted" • Art. 3.1 (d) iv: Replace "any changes" by "relevant changes" in the sentence "provisions on the review of the accepted residual ICT risk at least once a year, including the identification of relevant changes to the residual ICT risk" due to a risk-orientated approach. • Art. 3.1 (e): Replace "any" by "relevant" und "promptly" by "appropriate" in the sentences: "provisions on the monitoring of relevant changes to their ICT landscape, internal and external vulnerabilities and threats and of ICT risk to detect changes in appropriate time that could affect the overall ICT risk profile." • Art. 3.3: The financial entity should consider whether such changes warrant any update to their policies and procedures, but these will not always be needed. We therefore suggest to add "as needed" in the sentence: "Financial entities shall update the ICT risk management policies and procedures as needed where material changes to the cyber threat landscape, to ICT services, or to ICT assets supporting the business functions occur.

Q5	Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.	Generally: We believe that in this it is important for financial entities to take a proportionate and risk-based approach to the mapping of ICT assets. Taken literally, DORA could imply the mapping of absolutely every ICT asset, including, for instance, computer headsets, computer mice and keyboards, every laptop or corporate phone, and a great number of other ICT assets which are immaterial to the functioning of financial entity or its ICT risk. To do so would overwhelm any system of record. A large number of ICT assets are similar. Therefore, also appropriate grouping of ICT assets as a whole should be allowed. Considered to the assets of ICT third party providers the assets should be limited to the interfaces to third parties. Therefore we suggest the following amendment for Art. 4.1 (a): "In line with the proportionality principles in Article 4 of Regulation (EU) 2022/2554, the policy on management of ICT assets shall:". Furthermore we suggest to add the following sentence to Art. 4.1 (1): "In the management of ICT assets, ICT assets may be appropriately grouped." Art. 4.2 (a) We believe that it is helpful to clarify that the RTS not demands the creation of a single inventory or system of records. Such a clarification was given for the EBA ICT Risk Management Guidelines (page 94). We therefore recommend the following supplement: "This article does not require a financial entity to keep the inventory in a single system. The way the inventory is maintained is to be determined by the financial entity." Art 4.2 (b) We propose that the described items should be limited to meaningful details in the context of the single ICT asset. We suggest to replace "of all of the following" with "in principle": "prescribe that the financial entity keeps records that contains in principle". • Art. 4.2 (b) i: "unique identifier of each ICT asset": The requirement lead to enormous administrative and redundant effort with little benefit. The implementation should be designed or limited to a manageable extent. An adjustment or addition is necessary here so that an grouping of the documentation of ICT assets of the same kind is sufficient. A unique identifier for each single asset is not manageable and not appropriate. • Art. 4.2 (b) ii: Some new technologies cannot easily be located to a specific jurisdiction. For instance, some cloud assets are dynamic in nature and have server-less architecture. An example of this could be batch job processing code. It would be difficult and often meaningless from a risk management perspective, to record the location of such an ICT asset. • Article 4.2 (b) vii: Some ICT assets such as computer key boards have no RPO or RTO, whereas the recovery objectives for critical applications are of top concern for a financial entity's resilience. Amendment: "the ICT business continuity requirements, including recovery time objectives and recovery points objectives where applicable." • Art. 4.2 (b) ix: It may not always be possible for a financial entity to document the links of all ICT assets to business functions. For example, traffic is routed through network routers and switches on a dynamic basis. Those ICT assets

		could therefore support any number of business services at a given time, or none at all.
Q6	Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?	The institute should be able to determine for itself to record the date, if relevant.
Q7	Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.	The rules for encryption are protecting authenticity, integrity and confidentiality but not availability. Availability should be excluded from this recommandation. • Art. 6.2 (a): Encryption of data in use remains an emerging field of cryptographic technology. We understand it to mean techniques such as homomorphic encryption. However, these remain niche capabilities that are not supported by the vast majority of data processes. Art 6.2 (a) would therefore de-facto require the use of separate environments for all, or the vast majority of, data processing. While there are variations on the kind of environments this could refer to, we are not aware of any solution which would scale to the level required by this citation. We also do not believe it is necessary to use a separate environment in order to process data in use in a safe and secure way. We therefore suggest it be removed or amended to allow firms to apply this according to their own risk-based approach: "If encryption of data in use is not possible, financial entities shall consider, using a risk-based approach, whether to process data in use in a separated and protected environment to ensure the confidentiality, integrity and availability of data." • Art. 7.3: To our knowledge, it is not yet technically possible to recover lost keys. This is why Art. 7.2 is an important area of any firm's ICT risk management. The financial entity could, alternatively, develop methods for recovering data that was protected by a lost key. For instance, backup data could be protected with a different key. We therefore suggest the following amendment: "Financial entities shall develop and implement methods to recover the data in the case of lost, compromised or damaged keys." • Art. 7.4 register for certificates: A restriction should be made that this requirement should only be fulfilled for certain sensitive certificates and devices and could be decentral organized. For instance, all certificates would require the firm to have a register for certificates embedded in browsers, the scale of which is hard to calculate. While we are aware that some firms are exploring a more complete approach to certificate registry, this is an area of theoretical research for highly funding firms, not something that could be currently expected across the industry. We therefore recommend the following amendment: „Financial entities shall create and maintain registers for all certificates and certificate storing devices deemed to be material to is digital operational resilience. The register shall be kept up-to date."

Q8	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.	No.
Q9	Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.	Regarding background paragraph 53, the approach given in Art. 8 and 9 covers areas that are typically the responsibility of teams wider than the security function. For instance, ICT operating policies and procedures and capacity management are typically be owned by the technology function, rather than the cybersecurity or ICT controls functions. Some of the requirements given in Art. 8, while appropriate capabilities for a financial entity to have, are classified in a way which implies a too limited purpose. The way financial entities choose to complete and maintain their ICT operations documentation may vary between organisations. For these reasons, we suggest adding a clarification to the background paragraphs that confirms that financial entities are expected to develop policies and procedures for ICT operations, but not prescribe how these should be achieved or exactly which documents they are contained in. We therefore suggest the following amendment be added to background paragraphs: "This regulatory technical standard does not prescribe exactly where these policies and procedures should be maintained with the financial entity or which functions are responsible for individual requirements within this RTS." • Art. 8.2 (c) ii: If troubleshooting is within the competence of the organisation, external support is not needed. Proposal for the sentence: "support and escalation contacts, including external support contacts if required in case of unexpected operational or technical issues" - Art. 8.2 (c) iii.: These should not be limited to "error handling", nor would a financial entity want to develop separate recovery procedures for specific causes of disruption such as errors as this would introduce unnecessary complexity and likely result in inferior capabilities. The requirement should be formulated more comprehensively: "adequate ICT service continuity procedures in the event of ICT system disruption". • Art.10. 2 (c): The vulnerability management (VM) of financial entities is already challenged by the volume of vulnerabilities being disclosed. Tracking disclosures and prioritising patching based on the criticality of the vulnerability are vital tasks to security operations. We believe the article should reference the need for ICT TPP to manage their own vulnerabilities, patch them as appropriate, and adequately assure financial entities that this has been done. Financial entities should prioritize assessing the VM/ patching programmes of their third-parties to ensure they are adequate, rather than verifying the activity against any one vulnerability. Amendment: "ensure that ICT third-party service providers appropriately address any vulnerabilities related to the ICT services provided to the financial entity and provide adequate assurance on the state of their

		vulnerability management and patching programmes to the financial entity.” This article should also be limited to only ICT TPP with tasks on critical or important functions or processes to focus on the critical processes. • Art. 10.2(d): clarify, that the tracking of the usage of third-party libraries, including open source relates to software development in the bank - not for licensed software, SaaS etc. • Art. 10.2 (f): Addition of a risk-based provision of patches. Proposal: "deploy patches risk-based to address identified vulnerabilities". • Art. 10.2 (i): Adaptation of the wording from "any" to "relevant": prescribe the recording of relevante detected vulnerabilities affecting ICT systems and the monitoring of their resolution. • Art. 11.2 (b): We note that in the EBA Guidelines on ICT and security risk, this requirement was limited to network components. Secure configuration may not be a relevant control for some ICT assets such as non-connected devices or very low risk assets. Financial entities will therefore need to apply a risk-based approach to this requirement. Amendment: “identification of secure configuration baseline for ICT assets taking into account a risk-based approach, leading practices, …”. • Art. 11.2 (f): The inclusion of private end devices should be dispensed because this could lead to a legally problematic depth of intervention. If the bank allows the use of private devices for business, then there should be adequate measures, e.g. an enclosed environment on the private endpoint-device. • Art. 12.2 (c) The wording "all of the follwing" should be changed to a risk-based approach because not every ICT system enables extensive logging. Proposal: "the requirement to log events risk-based related to the following:" • Art. 12.2 (g): Synchronisation of the clocks of all ICT systems with a single reliable reference time source is not possible about the cooperation of different service providers and can only be implemented under their own sovereignty. Delete or adjust: “the synchronisation of the clocks of all the financial entity's ICT systems in their sphere of influence upon a single reliable reference time source.”
Q10	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.	No.

Q11	What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.	Vulnerability scans for all used ICT assets do not consider a risk oriented approach neither a approach of proportionality or avoiding unnecessary regulatory and reporting burden. There will be additional costs for the scans, effort and headcount (analysing the results of the scans). Therefore vulnerability scans should be processed regularly for those IT assets supporting critical or important functions. We consider even the weekly vulnerability scans for ICT systems supporting critical or important functions to be inappropriate. There must be time to evaluate the scans and to derive and implement the need for action. • Art. 10.2 (b): Art. 10.1 describes a risk-oriented procedure. The focus should therefore be exposed on areas with a high visibility / attack surface. From this, the implementation interval should be defined. Therefore, we propose to delete Art. 10.2 (b) sentence 2 "For those supporting critical or important functions it shall be performed at least on a weekly basis". Should the supervisory authority see it differently, at least the period should be changed from ''at least once a week'' to ''at least once a month". Furthermore the scan should be done on relevant reference systems, if several completely identical systems exist. Proposal: Add "Scans can be based on reference systems". • Art. 10.2 (c): We suggest changing the phrase ''all vulnerabilities'' to ''relevant vulnerabilities'' because not all vulnerabilities that a service provider addresses are relevant to the financial institution.
Q12	Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.	The points mentioned in Article 11 2.k for Cloud Resources appear redundant to the topics "ICT and information security awareness and training" from Article 19 and the topic "Access Control" from Article 22. We propose to delete. Employees, including system administrators, should always have the necessary competence to correctly carry out the work entrusted to them, especially with regard to the secure use of IT systems (regardless of whether the IT system is in the cloud or not). In addition, all privileged admin access should be protected separately, not just privileged access to a cloud client interface for managing the cloud environment. The requirement should therefore be formulated in a generally technology-neutral way. Also: Not all trainings / competences / experiences are based on specific training certificates, other ways like training on the job should be accepted. There may not be trainings or specific certificates available on the market for some aspects of the use of cloud that a financial entity may want to undertake. This could be because the area is new, or because they are proprietary to the financial entity. A strict requirement for specific training, rather than having the necessary competence in general, could therefore limit the ability of FEs to use cloud or to innovate in the EU.
Q13	Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.	• Art. 13.1 (b) "mapping and visual representation of all the financial entity's networks and data flows": A delimitation according to the sphere of influence carried out (bank versa service provider). The visual representation of all networks should be possible in aggregated form to ensure manageable network security management. The term 'data flows' is reaches too far. A complete visual representation of all data flows appears neither feasible nor useful as a practical matter. A graphical network map showing connections is normally used by network management and monitoring; however, 'data flows' are not represented by such a map, as they include not only the technical links but also higher

		protocol layers, which may be redirected automatically by routing protocols and switch over facilities. 'Data flows' are only visible on OSI layer 5 to 7, which is far beyond the reach of network management tools, which address the lower layers 1 and 2, and on some occasions, layer 3 (traffic shaping). In our view, a detailed network mapping list should be sufficient for the required information needs. Our amendment: "adequate mapping and visual representation in an aggregated way of the financial entity' networks". • Art. 13.1 (c): We request the deletion of this article. A separate network for the management of ICT facilities with the prohibition of direct internet access does not provide any gain in security. The general requirement for network segmentation from Art. 13 (1a) is sufficient. In our view, it is appropriate to position the ICT asset management tools and databases in a secured common backend segment with other critical functions. In addition, the prohibition of direct Internet access would make remote administration impossible, but this is of great importance in practice. • Art.13.1 (h): should require 12 months instead of 6 months in order for a criticality-oriented way of use of resources. • Art.14.1: For any controls related to protecting data, it is important to take into account the financial entity’s information classification system. For example, public information that is readily available does not need to be encrypted or subject to strenuous controls. In contrast, the transmission of PII or market sensitive data requires financial entities to consider strenuous controls to ensure confidentiality and integrity of the data. This is recognised in other Articles of this RTS. We therefore recommend the following amendment: “1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement the policies, procedures, protocols and tools to protect information in transit, taking into account the results of the approved data classification and the ICT risk assessment processes.”
Q14	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.	No.
Q15	Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.	Generally: With regard to project management the current RTS draft seems to be very waterfall approach oriented. We suggest to explicitly include agile methods of developing and implementing new ICT topics. • Art. 15.3: Project and Change Mangement should be seperated. This allows a dedicated focus on the ICT Change Management procedures and aligned to the level 2 RTS as mentioned • Art. 15.2 (f), Art. 17: The aspects of the maintenance processes shouldn't be covered in the change discipline and the project management police. We would expect these aspects to be covered in the run processees.

- Art. 16.1: We note that the EBA Guidelines on ICT and Security Risk Management include clarifying text that reiterated the importance of taking a risk-based approach in this area. We believe that including this clarification in the RTS remains important and suggest it be maintained.
  We note that Art. 16 requires a policy specific to acquisitions and that Section 3.6.1 of the EBA Guidelines on ICT and Security Risk Management did not include acquisitions in this section.
  Amendment: "As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a policy governing the acquisition, development and maintenance of ICT systems. This process should be designed using a risk-based approach. While the policies required by this Article cover acquisitions, it is not intended to prescribe precisely where this policy is documented within the financial entity.″
- Art. 16.4, 16.8. and 16.9:
  The draft RTS goes beyond the requirement of Art. 25(1) DORA, which requires source code review only to the extent that it is feasible. This is also confirmed by the relevant international standard ISO/IEC 27001/2 according to recital (56) DORA, which only requires source code inspection for developers and not for users.
  Conducting static and dynamic testing on every open souce and proprietary code by every entity within the scope of this RTS would be a tremendous workload and thus problably not even possible with regard to the labour market. Source code verification is practically impossible for purchased/licensed applications, as the source code is usually not available or not released. In addition, a financial company generally does not have the competence for a source code review, since very specific development know-how is required for this. For Commercial of the shelf software from recognised producers, trust in their internal testing is necessary. E.g. Windows should be tested by Microsoft and through bug bounty programs, not by each and every user. The same is true for standard open cource code, tested by their respective community.
  We propose that the requirement for a source code inspection be limited to the areas of in-house development.
  Proposal: ″In-house developed code should be tested for vulnerabilities with respect to the criticality of the application (can be tested by automated tools).
- Art. 16.5: The two terms "software packages" and "security testing" should be defined.
- Art. 16.6: The part should be deleted or risk-orientated based on the integrity and confidentiality of data used in non-production environments. The protection of all data in non-productive environments is not always appropriate and nessesary ("playing data", publicly available data or other data with low confidentiality should not need to be anonymized, pseudonymized or randomized). No productive data outside the productive environment can also be a constraint in the development for instance of AI models, since real data is needed here to train the AI. In this case, the development environment containing real data has to been protected in the same way as the corresponding

		production environment. The regulation should also take into account the requirement to use production data for debugging purposes in case of production issues and should allow such use if additional safeguards against misuse (e.g. monitoring, session recording) are in place. • Art.17.2: It is important that financial entities retain the ability to apply the requirements using a risk-based approach. Not all changes require the same levels of governance and oversight, and applying a single standard could have significant impacts on financial entities' ability to maintain their operations. It would also overwhelm any governance processes put in place and lead to a significant backlog of work. For instance, many minor changes to low-risk applications should not require approval from a second-line function as this would create unnecessary bureaucracy disproportionate to the risk. Amendment: "Financial entities shall include in the ICT change management procedures in respect to all changes using a risk-based approach…"
Q16	Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.	No.
Q17	Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.	Yes.
Q18	Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.	Yes.
Q19	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.	No.
Q20	Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.	• Art. 19.1: It should be clarified, that the specific ICT security programmes relate to ICT security staff and not all staff. The given specification of training elements are primarily technical efforts to reduce the operational information security risk. Furthermore they focus on specific technical knowledge needed in close relation to specific IT assets in use. The industry continues to believe that it will never be appropriate or practical to include third-party providers in the financial entities training schemes, as required under Article 13.6 of DORA. Financial entities should continue to rely on 3rd party providers to ensure that they maintain their own security training programmes that are of commensurate sophistication. • The inclusion of providers in security awareness and training measures should be limited to those providers that provide services for critical systems. In addition, it must be

		prevented that for central financial service providers who provide services for a large number of institutions, is now in turn included as a provider in the measures of these institutions. While we agree that provider awareness programmes are essential to our own security and resilience business, we propose that the providers' own efforts can be taken into due account when it comes to provider awareness trainings requirements. • Art 19.2: The minimum annual cycle should be deleted as the added value of a static procedure seems questionable. Instead, measures should be taken on an as-needed basis to ensure effectiveness.
	Human resources policy and access control	
Q21	Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion.	• Art. 20.1 (b): As currently drafted, the requirements are to be extended to ICT third-party service providers. We agree, that the service providers must comply with the requirements of the FE. However, the current wording could be misleading. Therefore, we suggest to change the wording in the article 20.1 (b) i to "be informed about, and adhere to, the financial entity's ICT security requirements, procedures and protocols". • Art. 22.1 (a): the distinction between ''need-to-know'' and ''need-to-use'' and "least privileged" is not clear. There is no concrete and generally valid distinction between the terms. In the literature and the relevant international standard, only the term ''need-to-know'' is used. We suggest either deleting the term "need-to-use" or clarifying the distinction between the terms. • Art. 22.1 (b) and Art. 22 1 e iv: Please clarify the term "critical data". • Art. 22.1 (e) iv.: the review-period of access rights should be extended to six months only for privileged access rights (e.g. administration accounts), one year für systems supporting critical or important functions and regularly for all other accounts. Continuous rights allocation processes already ensure a risk-based use of rights. • Art. 22 1. (f) i.: When selecting authentication methods, it should also be possible to take existing controls into account ("taking into account existing control mechanisms") • Art. 22.1 (f) ii.: Here, 2-factor authentication is required not only for remote access, but generally for privileged rights and access to ICT assets that support critical or important functions. This would require 2-factor authentication virtually across the board in a financial institution. We propose that the need for 2-factor authentication be assessed on a case-by-case basis as part of an individual risk classification by the financial service provider. This also satisfies the principle of proportionality pursuant to Art. 4 DORA. • Art. 22.1 (g): i.: Documentation or recording of all natural persons of access to sites or premises is not manageable and always appropriate and should be limited to critical premises or sites only. Proposal: identification of natural persons who are authorised to enter the critical locations of operation of the financial entity and the recording of every entry to these critical locations; • Art. 22.1 (g): iii.: As described above, the monitoring of physical access to premises should be limited to critical areas and supplemented by these.

		Proposal: Monitoring of physical access to critical locations, data centres and sensitive designated areas identified by the financial entity where ICT and information assets reside. • Art. 22.1 (g) iv.: An addition of "critical locations" should be documented here for the immediate withdrawal of physical access rights". Proposal: "review of physical access rights to critical locations to ensure that unnecessary access rights are revoked in.
Q22	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.	No.
	ICT-related incident detection and response	
Q23	Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.	• Art. 23.1 (f): It is unclear why ICT response and recovery plans have been included in this section, which is otherwise about incident management. These are of course related topics, but they are not typically governed within the same policy within a financial entity. As the testing of ICT response and recovery plans is already adequately covered under Articles 25, 26 and 27, we suggest to delete the sentence “The ICT response and recovery plans shall be reviewed against a range of different plausible scenarios” in this section to avoid confusion. • Art. 24.2 (a) ii and Art. 24.2 (d): It is unclear what the term “usual scenarios of detection used by threat actors” means in this context. We believe it is significantly more clear to simply require the identification of threats based on threat intelligence. We note that the EBA Guidelines on ICT and Security Risk 3.4.5 only required the identification of internal and external threats. This was well understood by the financial sector and covers the full range of activities that a financial entity might use to determine a threat. We therefore recommend to delete the part “including usual scenarios of detection used by threat actors and scenarios” from the sentence. • Art. 24.2 (d): One might use threat intelligence scenarios to consider risk, but they would not be recorded in the same logs as anomalous activities, nor would you necessarily want to proactively reconsider them as this is a highly manual process and therefore could not be replicated at the scale envisaged by this requirement. Amendment: Reduce the sentence to “proactively monitor and analyse the logs collected in accordance with Article 12.” and *delete the part “ensuring that all scenarios identified under point 2(a)(ii), and the alerts specified in point (b) of this paragraph”.* • Art. 24.2 (b): The identification of malicious activity can be detected by anomalies. However, the existence of the totality of all anomalies is not a given. The identification of all anomalies in this context is therefore not possible to apply and ensure. Thatswhy "any" should be removed from the sentence.

		• Art. 24.2 (e): Financial entities would need to take a risk-based approach. For a financial entity of any scale, it may not be advisable to attempt to analyse all information related to all anomalies. It is possible that the RTS overestimates the extent to which automated tooling can be relied on. Financial entities should prioritize based on risk, which is made up of a number of factors beyond only whether there is a connection to critical or important functions. Amendment: delete “all” from the sentence: „record, analyse and evaluate relevant information on important anomalous activities and behaviours automatically where possible, or manually by staff” • Art. 24.3: Please provide a definition of "data in use" • Art. 24.5 (b): In this case we don't see any context to "availability".
	ICT business continuity management	
Q24	Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.	• Art. 25.1 (f): In compliance with the ISO 22301 standard, business continuity plans are not created specifically for certain scenarios as listed in Article 27.2, but for the worst case of resource failure. BCPs are designed by taking into account threats identified through risk analyses (RA), in alignment with associated emergency measures / workarounds. A distinction should be made between BCM process steps (BIA, RA, BCP) to implement appropriate BCPs and other contingency plans (e.g. restart and recovery plans, crisis plans for severe threat scenarios). • Art. 26.2. (a) together with Art. 27.2: ICT response and recovery planning, the effects on relevant resources are usually examined as emergency scenarios, e.g., personnel failure, IT failure, building failure and service provider failure. Based on these scenarios, ICT response and recovery plans are prepared and emergency exercises are designed. To determine the likelihood of an emergency scenario occurring, root causes must be considered, e.g., insider attack, pandemics, intrusions, power outages. Root causes and effects are different levels of consideration and cannot be managed equally as scenarios (as is done in listing Art. 27.2. (a) through (i)). We suggest that instead of the listed scenarios the effects should be named in the listing Art. 27.2 and that their root causes be stated in parentheses in each case: - Failure or partial failure of a site (e.g., due to flood, major fire, area closure, access control failure). - Significant failure of IT systems or communications infrastructure (e.g., due to errors or attacks) - Loss of a critical number of employees (e.g., in the event of a pandemic, food poisoning, strike) - Failure of service providers (e.g., suppliers, power providers) Any financial entity needs to take a risk-based approach to testing and the choice of scenarios given that the number of scenarios that could be tested will always greatly exceed the time and resources available to the financial entity. This is especially the case of this Article references the scenarios given in Article 27.2. While testing programmes should account for the full range of threats facing the financial

		entity, which threat to test, the frequency that it is tested and the systems or infrastructure to be tested, must be a decision for the financial entity to take, balancing a number of risk factors. Above all, impact and likelihood must remain the primary lens through which the financial entity determines which tests to conduct and when. Mandated scenarios could also result in firms navigating towards the same prescribed scenarios rather than taking a risk based approach. We therefore alternatively suggest to change the last sentence in Article 27.2: “The scenarios could include the following:” • Art. 26.4: In the sense of the proportionality principle, it should be added here that the performance of reference tests for the business continuity plans is sufficient (especially in groups, where one intragroup provider supports many financial entities) • Art. 26.5: A distinction should be made between "any" and material deficiencies that need to be reported to management body. BCM always identifies improvements but not all are critical findings or material deficiencies. Proposal: "Test results shall be documented and any identified deficiencies resulting from the tests should be analysed and addressed. A reporting to the management body shall be done for all tests that include at least all identified critical or major deficiencies. • Art. 27.1 (b), the RTS uses the term critical ICT systems and services. This phrase is not defined in DORA and will create confusion in the industry regarding how to understand criticality in this context. We recommend that the text be changed to the following: “describe what actions shall be taken to ensure the availability, integrity, continuity and recovery of at least the ICT systems supporting the critical or important functions of the financial entities; “ • Art. 27.1 (e): The meaning of long-term in this context is not clear. Please provide an explanation. • Art. 27.4: creates a new category of ICT third-party provider of “key importance” to a financial “institutions” ICT service continuity. We believe this will create further definitional confusion by adding another layer or term of criticality and request that this requirement be aligned to terminology and requirements in the rest of the DORA text.
Q25	Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.	• Art. 25.2 (a): Not a maximum recovery time of two hours for all critical functions: In the event of a disruption caused by malicious cybersecurity incident, we believe that a mandate to recover within 2hrs could drive CCPs and CSDs to attempt to recover outside of their risk appetite and before the necessary mitigation processes have been completed. The first paragraph of the requirement should be adapted. Proposal: "The maximum recovery time for its critical functions should be set in such a way that end of day procedures and payments shall be completed on the required time and day in all circumstances." • Art. 25.2 (c) ii please specify whether "secondary processing site" refers to secondary data centers • Art. 25.2 (c) iii Since COVID-19, "secondary business sites" seem not automatically needed, if institutions risk profile and the business can be run by staff working from home.

		- Art. 25.3 (a): Replace "any" by "relevant". Proposal: "takes into account relevant links and interdependencies to at least users,...". - Art. 25.3 (b): Ensuring recovery for critical and important functions is relevant, but no concrete recovery time should be specified here, but it should be ensured that this is done in an adequate time. Institutions should be able to define appropriate availability requirements based on their risk profile (also in line with their business area) and not on a generalised <2 hours RTO. There are different risk profiles and time criticalities across the industry that seem appropriate. Proposal: "requires its ICT business continuity arrangements to ensure that the recovery time objective for their critical or important functions shall be in an adequate time". - Art. 25.4: The wording should be more general and not specify specific times and only critical functions should be considered. Institutions should be able to define individual restart time frames / criticalities according to their risk profiles and needs of coordinated continuity requirements e.g. with customers. Zero data loss is not a realistic expectation. The ability to recover corrupted data depends among other things, on the frequency of the financial entity's backups. We recommend the following amendment: "In addition to the requirements referred to in paragraph 1, trading venues shall ensure that its ICT business continuity arrangements allow trading can be resumed within or close to two hours of a disruptive incident and that the maximum amount of data that may be lost from any IT service of the trading venue after a disruptive incident is minimised." - Art. 26.3-4: It may not always be appropriate to include members in the testing if ICT Business Continuity Plans. We recommend the inclusion of the phrase "where applicable", similar to the formula in Article 26.2.b.
	Report on the ICT risk management framework review	
Q26	Do you agree with the suggested approach on the format and content of the report on the ICT risk management framework review? If not, please explain and provide alternative suggestion.	No. We miss in Art. 28 the scope of interpretation for institutions of different sizes as envisaged in Art. 4 of the DORA. Furthermore there are a number of different causes for conducting the review given in Article 6(5) of DORA. If each of these causes is triggered only once in a year, which is a conservative estimate, then the frequency of the reviews would easily outpace the speed with which a financial entity could complete them. We therefore propose the following alternative wording for the entire Art. 28, which is in line with common practice in German supervision: "The management body of the financial institution shall be informed on an ad hoc basis and on a regular basis, but at least quarterly, in particular on the results of the risk analysis and changes to the risk situation as well as on the status of information security. The status report shall include, for example, the assessment of the information security situation compared to the previous report, information on information security projects, information security incidents, and penetration test results." The minimum content of the report on the review of the ICT risk management framework is very extensive (including

		introduction, detailed analyzes and assessments of vulnerabilities, measures taken and their timetable, influence on budget and resources...). Management reports during the year should focus on the concrete changes, not repeat all facts. Furthermore we propose to restrict the report on summarys with references of the details in other documents. • 28.2 (a) The items listed contain too much details for a summarize - the summarize should focus on the major changes and a short description of the context of the the report, the details should be part of the ICT-strategy-document, information register, threat landscape etc. • 28.2(d) Please explain the purpose of documenting the start and end dates of the review period. How exactly is the start and end date of the review to be determined.” • 28.2 (g) The report should focus on a summarize of the analysis/ assessment of the weaknesses, defencies and gaps and not include all the details on this. "summary of the findings of the review and summary of the analysis and assessment of the severity of the weaknesses, deficiencies and gaps in the ICT risk management framework during the review period"; • 28.2 (h) appropriate level of detail in the report as well e.g. iii.: limit to responsibility - not details like tools / staff iv.: summary of the impact, not all te details vi.: explanation instead of detailed explanation • 28.2 (k) List of past reviews not as part of the report
	Simplified ICT risk management framework	
Q27	Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.	N/A
	Further elements of systems, protocols, and tools to minimise the impact of ICT risk	
Q28	Do you agree with the suggested approach regarding the further elements of systems, protocols, and tools to minimise the impact of ICT risk under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.	N/A
Q29	What would be the impact for financial entities to expand the ICT operation security requirements for all ICT assets? Please provide details and if possible, quantitative data.	N/A

Comments Consultation on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

Q30	Are there any additional measures or control that should be considered specifically for cloud resources in the draft RTS, beyond those already identified in Article 37(2)(h) of the proposed draft RTS? If yes, please explain and provide examples.	N/A
	ICT business continuity management	
Q31	Do you agree with the suggested approach regarding ICT business continuity management under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.	N/A
	Report on the ICT risk management framework review	
Q32	Do you agree with the suggested approach regarding the article on Format and content of the report on the simplified ICT risk management review? If not, please explain and provide alternative suggestion as necessary.	N/A