DORA - Draft RTS

To further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

September 2023

Executive Summary

AFME welcomes the opportunity to respond to the draft Regulatory Technical Standard (RTS) to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554 [DORA][1]. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

Our response to this consultation is from the perspective of our bank members, focusing on those issues which are most relevant to wholesale capital markets. We are responding to each of the specific questions set out in the consultation paper, but wanted to raise as well two overarching points:

1. **Firms should be permitted to evidence compliance with DORA through existing risk management policies**

   In many instances the proposed requirements under the Risk Management Framework (RMF) are already captured but split across various corporate policies and procedures. In other instances the requirements will be met by other incoming DORA obligations. There would be no added-value in compelling firms to evidence/demonstrate their compliance with new, standalone DORA policies. Clarification that this is not being sought would be welcomed at the earliest opportunity. Financial entities should be entitled to evidence compliance with DORA requirements through a range of internal frameworks, policies, standards and governance, with no attempt to enforce a one-size fits all approach. AFME also looks forward to working with officials on future mapping exercises to address the overlap between regulatory frameworks, for example with the EBA guidelines on ICT and security risk management.

2. **Proportionality principle would be more successfully embedded through greater flexibility for firms**

   In several instances, the ESAs have proposed going beyond current practice through a more prescriptive approach, for example curtailing discretion during ICT project and change management or setting the frequency of IT security awareness training. One of the most effective ways of embedding the mutually-supported proportionality principle would be recognising that firms are often best placed to put into practice the supervisors' purported aims and intentions. Greater flexibility and discretion for firms will allow them to focus on these outcomes, including through the leveraging of various public-private initiatives on risk

[1] https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTSs_ICT_risk_management_tools_methods_processes_and_policies.pdf

management, whereas prescription risks a compliance, tick-box mentality to risk management which could ultimately backfire.

Please see below our responses on questions 1 – 26. Given AFME's membership we have not responded to the questions on a simplified risk management framework. We remain available to discuss further any points raised.

Consultation Questions

Question 1 **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.**

- Firstly, we endorse the aim of embedding proportionality into the RTS. We suggest in the questions below how to tailor and more fully embed this concept within the various specifications, but at the overarching level we stress that the same risk will have varying impact on different financial entities. The financial entity is best placed to assess the potential impact and a proportionate RMF would recognise this and provide sufficient flexibility and discretion for financial entities. While the ESAs are in many instances mandated by the Level 1 text to establish for example additional components or criteria, there remains considerable room for manoeuvre within the Level 2 instruments, and we encourage the ESAs to be more ambitious in incorporating proportionality and a risk-based approach. This is expanded upon in the questions below, but for example includes not mandating the encryption of *all* data, especially data in use; not applying change management procedures to *all* changes, thereby capturing many BaU (Business as Usual) updates; and not mandating specific scenarios for business continuity testing, but instead allowing the financial entity to choose a scenario based on its own risk-based assessments.

- In relation to the complexity and risk considerations set out within Article 29 of the Delegated Regulation, an outcomes and risk-based approach is encouraged. Such an approach would give greater weighting to the final two considerations referenced, namely the impact on data and the disruption to continuity of services. As currently drafted, Article 29 seems to provide only the freedom to go beyond the requirements in the RTS, not the freedom to determine where the risk presented to the financial entity allows for the implementation of a different control or reduced monitoring. This is important, as financial entities must prioritise resources. 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. The current phrasing also does not account for instances where the control being required is not technically feasible, for instance the scanning of ICT assets that do not have an IP address, such as keyboards. 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.

- We also flag how inconsistency in language across Title 1 of the proposed RTS has unnecessarily created uncertainty. In particular the term "*ICT security policies*" is at times used interchangeably with "*Risk Management Framework*" and at other times, as a component of

the framework, alongside "*procedures, protocols and tools".* We recommend the term Risk Management Framework is applied to prevent overlap, particularly within Articles 2, 4, 8 and 9.

Question 2 **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.**

- N/A

Question 3 **Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.**

- We believe the statements regarding the internal organisation of the three lines of defence (LoD) model are confusing both in the RTS and the Level 1 text. Specifically, Art 6(4) of the Level 1 text says that responsibility for managing ICT risk should be assigned to a control function, but also that the ICT risk management function and control function should be segregated and independent. Taken literally, these statements are in conflict.

- Further, some of the statements in Article 2 of the RTS could be interpreted as forcing financial entities to locate their cybersecurity functions within the 2nd LoD. 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. Further, prescriptive requirements in other jurisdictions could either create a conflict of regulatory requirements that would be unmanageable for a financial entity or result in requirements which are ill-fitting or inappropriate, for example in the case of 3rd country branches where there will not be a local board.

- Similar comments were made by the industry in response to the EBA's draft Guidelines on ICT and Security Risk Management 2019. The EBA made helpful clarification in their final text and in the analysis of those comments (see page 73). 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, acknowledging that firms should assign responsibilities as appropriate to their models in the recitals to the RTS.

- In addition, we believe that the RTS should avoid listing specific tasks which are to be carried out by specific functions. For example, Article 2(1)(f) says that the control function should develop ICT security awareness programmes and trainings. In many firms, these are developed by the cybersecurity function located within the 1LoD. This has benefits as it allows the financial entity to more easily incorporate relevant threat intelligence, for instance in the design of the financial entities phishing tests. While it is entirely possible that the control function could do this, different financial entities will have different structures, and we believe it is more important that this training is well designed and effectiveness monitored than stipulating which function is responsible. Article 19 also covers this sufficiently.

- Regarding Article 1(1), we do not believe that it is possible to guarantee these requirements in all situations. Financial entities should put in place measures to reduce the risk that the events listed in this article do not occur, but in any ICT environment, it is possible that issues will arise and 100% availability cannot be guaranteed. We recognise this phrase appears in the Level 1 text, but suggest that the ESAs avoid reusing it if possible. We have suggested an alternative amendment. We therefore recommend the following amendment:
    - *Article 1(1): Financial entities shall ensure that their ICT policies including information security and related procedures, protocols and tools are embedded in the ICT risk management framework. Financial entities shall establish the ICT security policies, procedures, protocols and tools in Chapter I with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and ~~guarantee an~~ **facilitate** accurate and prompt data transmission without major disruptions and undue delays.*

- We have also assumed that the "consequences" referred to within Art 1(2)(e) do not relate to employee sanctions for misconduct, which would be inappropriate within a security policy.

- Additionally, further to the broader point above on the tasks of the control function, we flag that the development of security awareness programmes and digital operational resilience training, under Article 2(1)(f), should not necessarily sit with the control function but instead with "appropriately skilled personnel." It is possible that the control function could develop such training, but in some financial entities the expertise to do this may be located in another function and we do not believe there is a risk management benefit to limiting this role to the control function. The control function should instead be tasked with the oversight and monitoring of security awareness programmes. We therefore suggest the following amendment:
    - *Article 2(1)(f) ~~developing and monitoring~~ **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.*

Question 4 **Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.**

- As stated within our executive summary, AFME members strongly argue that the ICT risk management policy referenced within Article 4 must not be developed as a stand-alone DORA policy/document, and that financial entities are able to evidence compliance with these requirements by reference to various existing policies and practices, as subject to internal risk driven models and thresholds.

- We highlight that the inclusion of several components within the risk management policy does not reflect existing commercial practice:

    - Risk tolerance levels are to be defined and documented, but typically these are not set out within policy documents.

- ‘Risk treatment measures’ should be classified as ‘risk mitigation measures’ to reflect standard terminology and avoid confusion.

- The Article now includes the terminology “authenticity”, whereas long standing practice has been ‘CIA’ (confidentiality, integrity and availability).

- On Article 3(1)(e) it is noted that changes in the ICT risk profile may likewise impact the digital operational resilience strategy: the relationship is two directional.

- Regarding Article 3(3), it may not be necessary to update policies and procedures in response to all changes in the threat landscape, ICT services or ICT assets. 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 the following amendment:
  - *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.*

Question 5 **Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion..**

- We note that the Level 1 text stipulates how firms must evidence their obligations on ICT asset management through the use of ‘inventories’, whereas the Level 2 Delegated Regulation has expanded this into a ‘policy’. AFME strongly cautions against any expectation that financial entities must create and maintain a single inventory or system of record. A corresponding clarification was given within the EBA ICT Security and Risk Management Guidelines (page 94) is sought.

- Regarding Article 4(2), we believe it is particularly important for the proportionality principle to be acknowledged for these requirements, particularly with regards to scope expectations. We therefore recommend the following amendment:
  - Article 4(2) ***In line with the proportionality principle in Article 4 of Regulation (EU) 2022/2554,*** *the policy on management of ICT assets shall*:

- Regarding Article 4(2)(b)(vii), this is another example where, if the financial entity is not able to take a risk-based approach, the requirement would become meaningless. Some ICT assets such as computer key boards have no RPO (recovery point objective) or RTO (recovery time objective), whereas the recovery objectives for critical applications are of top concern for a financial entity’s resilience. Equating these assets in the financial entity’s asset management programme would obscure the entity’s view and understanding of its risks and should be avoided.

- Regarding Article 5(2), again the proportionality principle is particularly important in ensuring that financial entities are able to focus resources and develop a manageable process for determining criticality, by for example relying upon their Business Impact Analysis (BIA). We therefore recommend the following amendment:
  - Article 5(2) ***In line with the proportionality principle in Article 4 of Regulation (EU) 2022/2554,*** *such procedure shall detail the criteria to perform the criticality*

*assessment of information assets and ICT assets supporting **critical** business functions. The assessment shall take into account the ICT risk related to those business functions and their dependencies on the information assets or ICT assets and how the loss of confidentiality, integrity, availability of such information assets and ICT assets would impact their business processes and activities.*

Question 6 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?

- Both dates serve different purposes, but their application or relevance varies depending on the nature of the product and the relationship with the provider. Further prescriptive instructions relating to either are though unnecessary and could conflict with continuous daily checks on hardware and software obsolescence.

Question 7 Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

- AFME has three main points on the approach to encryption and cryptography:

  i. The encryption of data should be explicitly limited to only *sensitive* data, as classified by the financial entity using a risk-based and proportionate approach. Cryptography increases processing times, requires additional capacity and entails allocation of technical skills.

  ii. We object to the requirement under Article 6(2)(a) for data, which cannot be encrypted, to be held in a *separate and protected environment*. In many cases this will not be feasible so instead we propose that firms should be obligated to "***consider, using a risk based approach,*** holding data which cannot be encrypted in a separate and protected environment". Further, given that encryption of 'data in use' (as opposed to data in transit, data at rest and data in storage) remains an emerging field, this requirement would be extremely premature and almost certainly unfeasible, capturing the vast majority of data processing, with no current solution capable of scaling to this level. The reference to 'data in use' should be removed for now.

  iii. On the application and incorporation of "leading practices", firms will naturally take account of new market techniques and practices when setting their own approach, though not all will be appropriate, for various reasons including corporate model and risk appetite. The expectation on firms to monitor market developments is though more appropriate at the overarching level, in terms of broader market innovations. Cryptanalysis is a cutting-edge field and it is not currently possible to have in-house experts to judge the scope of certain attacks. Rather than creating a specific requirement in the field of cryptanalysis, it is preferable for financial entities to be obligated to "***be mindful of leading practices using a risk based and commercial lens".*** Such an overarching requirement could also call out the need to consider sunsetting legacy techniques as new practices emerge.

- We additionally recommend that the wording in:

i. Article 7(3) is amended to focus on the recovery of data**,** instead of the recovery of cryptographic keys. To our knowledge the latter is not currently technically possible. 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 suggest an amendment to this effect:
   - Article 7(3): *Financial entities shall develop and implement methods to recover the ~~cryptographic keys~~* ***data*** *in the case of lost, compromised or damaged keys.*

ii. Article 7(4) is amended to clarify that it is only certificates and certificate storing devices "*deemed to be material to digital operational resilience*". As currently written, this requirement is overly broad and likely not achievable for the vast majority of firms. 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 funded firms, not something that could be currently expected across the industry. We therefore recommend the following amendment:
   - Article 7(4): *Financial entities shall create and maintain a register for all certificates and certificate storing devices* ***deemed to be material to digital operational resilience****. The register shall be kept up-to date.*

iii. Article 6(1) is amended, with the word "availability" removed, given it is not an attribute for encryption of data.

Question 8 **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 additions proposed, but in future the ESAs could explore building an equivalent of the ANSSI's RGS (General Security Benchmark) at the EU level.

Question 9 **Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.**

- The approach given in Article 8 covers areas that are typically the responsibility of teams wider than the security function. For instance, Article 8(1) says that ICT operating policies and procedures should be part of the ICT security policies and procedures. However, ICT operating policies and procedures would typically be owned by the technology function, rather than the cybersecurity or ICT controls functions. Equally, capacity management is typically not governed, and should not be recorded, under a financial entity's ICT security procedures as stated in Article 9(1).

- It is also the case that some of the requirements given in Article 8, while appropriate capabilities for a financial entity to have, are classified in a way which implies too limited a

purpose. For example, financial entities' policies and procedures should cover ICT systems restart, rollback and recovery, as per Article 8(2)(c)(iii). However, 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. Error handling should ideally be dealt with under incident management.

- The way financial entities choose to complete and maintain their ICT operations documentation may vary between organisation and we do not believe the exact location should be prescribed. For these reasons, we suggest adding a clarification to the recitals 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 within. The wording within Article 9 is particularly prescriptive, with references to three specific scenarios relating to planning ahead which do not feel additive to the text. We also suggest monitoring obligations should relate to the financial entity's own performance targets, with the financial entity to determine remedial action if performance targets are not met. This promotes an SLO-based monitoring approach that can be measured.

- Further, financial entities recognise the importance of capacity and performance management. However, we believe it is necessary to apply a risk-based approach that prioritises some assets over others. Capacity management for low risk applications is not a standard practice as it is not considered an effective use of time for reducing risk to the financial entity. If a low risk application has a capacity issue, the financial entity should be able to resolve the problem according to its policies and procedures without impact materialising.

- Similarly it would not be scalable or beneficial for ICT third-party service providers to inform financial entities of all vulnerabilities they identify and patch. The vulnerability management (VM) programmes of financial entities are 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. Instead, we believe ICT third-party providers must manage their own vulnerabilities, patch them as appropriate, and adequately assure financial entities that this has been done. Financial entities should prioritise assessing the VM and patching programmes of their third-parties to ensure they are adequate, rather than verifying the activity against any one vulnerability. We have suggested an amendment to the text accordingly.
    - Article 10(2)(c): *ensure that ICT third-party service providers handle any vulnerabilities related to the ICT services* ***supporting critical or important functions*** *provided to the financial entity and* ***provide adequate assurance on the state of their vulnerability management and patching programmes*** ~~*report them*~~ *to the financial entity. In particular, financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root cause and implement appropriate solutions*;

- Regarding the importance of logging and monitoring, this again needs to be done taking into account a risk-based approach in order for it to be scalable within a financial entity. For instance, it is not necessary to keep capacity logs for low-risk or non-capacity oriented ICT assets. The EBA previously recognised the importance of proportionality in their commentary

on the 2019 ICT and Security Risk Management Guidelines page 94. We believe it would be helpful to restate that clarification within the recitals to the RTS.

- The backup and recovery requirements as part of the ICT operations security policy (Article 8(2)(b)(i)) will be addressed by the firm's broader business recovery plans. This raises the question on how to approach duplicative/overlapping policies and procedures, and how broader incoming frameworks can be relied upon. AFME strongly encourages the ESAs to proactively assure firms that there is no requirement for duplication through the creation of separate RMF policies.

- In relation to vulnerability and patch management specifically:

    - We strongly object to the proposal to conduct automated vulnerability scanning and assessments on ICT assets supporting critical and important functions on at least a weekly basis (Art 10(2)(b)). The frequency of such testing should be decided on a risk-based approach as defined by financial entities in their own respective guidelines. Additionally, the terms "vulnerability scanning" and "assessments" are not clearly defined.

    - There is additional overlap between Art 10(2)(e) on disclosure of vulnerabilities to clients and counterparts and the broader communication obligations under Article 14 of DORA. We highlight here that such disclosures may in any case be prohibited by contractual agreements or could increase a financial entity's vulnerability through misuse by malicious actors. We seek clarification that firms have the discretion to decide if and when disclosure is not "responsible", and that this should take account of remediation or mitigation measures which are available and have been implemented. There should be no requirement to disclose to the public in general.

    - Under Article 10(2)(f), the requirement to implement other mitigation measures where patches are unavailable for a given vulnerability does not take a proportionate approach, or consider risks associated with vulnerabilities. In some circumstances, mitigations may be not be feasible – in these instances, in line with risk management principles, financial entities would assess the risk associated with the vulnerability and determine the appropriate course of action, which could include risk accepting the vulnerability where appropriate. Mandating the outcome of this assessment undermines the financial entity's ability to manage their risks. Further, requiring blanket mitigation measures could impede firms' ability to allocate their resources appropriately to deliver the greatest mitigation of risk available. We would propose that the wording is amended to "***If no patches are available for a vulnerability, financial entities shall identify and implement other mitigation measures where feasible and commensurate with risk".***

    - It will not always be possible to test and deploy software and hardware patch and updates in an environment which replicates the production one. Article 10(4)(c) should include the caveat "***as far as is feasible economically and technically, using a risk-based approach****."*

- Regarding Article 10(2)(i), as 2(b) and 2(h) would both include an element of recording, it is unclear what this provision 2(i) would require above and beyond those.

- There are six further points on the ICT operations security policy:

  - Remove from Article 8(2)(b)(v) the sentence "*The segregation shall consider all the components of an environment, such as accounts, data or connections in accordance with Article 13(1) point (a)*". Firms are best placed to identify which factors should be taken into account.

  - Article 8(2)(c)(ii): Support and escalation contacts should not be included within the ICT operations security policy itself. The details of these contacts should be stored separately.

  - In relation to Article 11(2)(a), it may not be feasible to set out access restrictions for all data classifications – for instance, certain non-sensitive data classifications stored in unstructured data locations. We propose that the wording be amended to: "*the access restrictions, in line with Chapter II Section II of this Regulation, supporting the protection requirements for each level of classification,* ***where feasible****;*"

  - Regarding Article 11(2)(b), we note that in the EBA ICT and Security Risk Guidelines, 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. We therefore recommend the following amendment:
    - *Art 11(2)(b): identification of secure configuration baseline for ICT assets taking into account* ***a risk-based approach,*** *leading practices, appropriate techniques referred to in international standards that will minimise their exposure to cyber threats, and measures to verify regularly (as determined by the financial entity) that these baselines are those that are effectively deployed*;

  - Regarding Article 11(2)(i), we do not recognise the term data leakage and believe it is better replaced with the term data loss. We therefore recommend its removal.

  - Article 11(2)(c) references "end point devices". The ESAs should clarify the definition in light of varying member interpretations. Subsection f has created further confusion by referring to "non-portable end point devices".

Question 10 **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 further measures proposed.

Question 11 **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**

- As noted at Q9, the frequency of such testing should not be set by the supervisors within the Level 2 instruments, but determined by each financial entity within their policies using a risk based approach, taking into account the vulnerability assessment and remediation timeframes. In any event, we strongly object to weekly testing on the grounds it is often not feasible, given the number of items to be inspected, the network load generated (DoS risk) and the number of security alerts reported. Monthly testing should be retained as a general rule, with any more regular testing focused on a financial entity's most critical assets rather than all assets.

- Equally important is that financial entities retain the ability to risk accept the non-scanning of some ICT assets based on their risk profile. For example, a financial entity may have a server rack in their ICT asset inventory. However, a server rack would not have an IP address and therefore could not be scanned using automated tools. Because it is not internet facing and does not have an active threat profile, it would likely be well within the financial entities risk appetite not to subject that asset to automated scanning. One large financial entity estimates that there are approximately 500 ICT assets which it does not scan frequently out of a population of approximately 1 million ICT assets in total. We believe this approach and the scale of exceptions is defensible and consistent with best practices for security and vulnerability scanning. We therefore recommend against expanding the requirement to all ICT assets independent of their overall risk profile.

Question 12 **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.**

- No additional measures specifically for cloud computing are proposed, in line with AFME's overarching position that operational risk controls should be technology neutral. It has been noted though the terminology appears out-of-date and would benefit from breaking down cloud computing into IaaS, BaaS and SaaS.

Question 13 **Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.*?***

- As stated, we do not recognise the term 'data leakage' and believe the variations in terminology creates confusion, with divergence likely to develop over time. We note that the EBA chose to remove the term from its 2019 Guidelines on ICT and Security Risk management (page 81) and replace it with data loss, which we believe is more appropriate. This proposed amendment should apply to all parts of the RTS where the term is used.

- 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 (personally identifiable information) or market sensitive data requires

financial entities to consider strenuous controls to ensure confidentiality and integrity of the data. The need to account for data classification is recognised in other Articles of this RTS and so we suggest adding the following amendment which restates that formula:

- Article 14(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 consideration the results of the approved data classification and ICT risk assessment processes.***

- Even with the assumption that the *segregation and segmentation* of network systems (Article 13(1)a)) is interchangeable with *separation*, and does not entail an entirely isolated network, this obligation remains a significant operational task. This requirement should be restricted to ICT Systems supporting critical or important functions only. It also fails to reference how the use of Zero Trust Security or Zero Trust Architecture are acceptable options for network systems.

- The introduction of the requirement to review ICT systems supporting critical or important functions at least every 6 months has caused particular concern (Article 13(1)(h)). For larger firms, given the multitude of systems in operation, this could in practice result in firms conducting continuous, rolling reviews. We would recommend at a minimum that this be extended with firms only required to conduct a review once every 12 months, including the review for firewall rules and connection filters. Such a timeframe also provides greater consistency across the Delegated Regulation. Ideally however, there should be no set frequencies within the Level 2 text, and instead the review process be determined by financial entities using their own ICT risk assessments.

- With regards to the "mapping and visual representation of all the financial entity' networks and data flows" under Article 13(1)(b), the RTS should clarify that this is limited to critical data and is based upon standard design documents, as opposed to real time mapping. Any centralised visual output would itself represent a potential operational risk for financial entities as a target for malicious actors. For large financial entities, mapping literally all data flows and networks would result in a product that was too complex to use for risk management purposes. Further clarity on what is meant by "network services" (under Article 13(1)(m)) would additionally be beneficial.

- Finally, we flag that under Article 13(1)(e) any expectation that this encompasses data from external data centres would not be appropriate or in practice feasible.

Question 14 **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 additional measures or controls are proposed.

Question 15 **Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.**

- While we recognise the importance of a policy designed to govern the acquisition of ICT systems, such a policy may not always be included within the ICT project management policy of a financial entity. Similarly, it may be common for project management and change management to be handled and managed by separate teams. We note that Article 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. We therefore suggest a clarification be included in this Recital to the effect that "***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."*** Similarly we stress the need for financial entities to have the discretion in how to implement the project risk assessment under Article 15(3)(d) and the change management requirements under Article 15(3)(f).

- Otherwise the alignment with the EBA Guidelines on ICT Risk Security Risk Management (Section 3.6.1) is welcomed.

- Article 15(3)(g) as currently worded is too broad. We recommend amending the wording so it is clear that testing under a ICT project management policy relates only to any incoming/newly developed or acquired ICT assets.

- On Article 16:

    - Regarding Article 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.

    - Security testing of software packages under Article 16(5) should extend only to an application unit, as opposed to each of the libraries, including OSS and third-party proprietary software.

    - There should be an exemption for user acceptance testing environments under Article 16(6): in relation to the requirement that "non-production environments shall only store anonymized, pseudonymized or randomized production data."

    - Article 16(9) refers to source code and proprietary software provided by ICT third-party services providers. This would not happen in practice as it is often prohibited by the licence agreement or could cut across proprietary interests.

    - We assume that "ICT systems developed or managed by users outside the ICT function" under Article 16(10) refers to end user computing solutions, as opposed to shadow IT.

- The text of Article 17(2) says that this requirement applies to "all changes". This could encompass many minor or BaU updates that do not qualify as a major change. As such it does not take into consideration modern software development practices that encourage smaller, incremental changes that promote safer introduction of changes thereby minimising the need for fall-back procedures for every change. In addition, as drafted it covers software, hardware and at all levels of criticality. And, as the RTS recognises, it also covers urgent changes that

may be made for security or resilience reasons. It is important that financial entities retain the ability to apply the requirements in Article 17(2) using a risk-based approach. Not all changes require the same levels of governance and oversight, and applying a single standard could have significant impact on financial entities' ability to maintain their BaU (business as usual) 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. Regarding Article 17(2)(c) specifically we propose that the change management procedures be performed by appropriately skilled/knowledgeable staff, as opposed to the current wording on ensuring effective quality assurance.

Question 16 **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 specific elements are proposed, with supply-chain risk sufficiently addressed in other DORA provisions, including via the Register of Information and creation of the regime for Critical Third Party Providers (CTTPs). Further additions to the proliferation of regulatory initiatives on supply chain resilience in recent years would only create overlapping duplication which may obscure policymakers' underlying intentions.

Question 17 **Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.**

- N/A

Question 18 **Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.**

- AFME has no objections to the suggested approach, subject to the assumption that it does not cover within scope non-digital information assets.

Question 19 **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 new measures or controls proposed.

Question 20 **Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions..**

- It is not clear to the industry what the practical difference is between ICT security and digital operational resilience training. We agree that all staff should undergo ICT security training. However, the vast majority of a financial entity's employees have no role in digital operational resilience and nor would technical training be appropriate.

- 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.

- We note that the EBA Guidelines on ICT and Security Risk Management reference inclusion of contractors, rather than third-party providers, which we believe is more realistic and aligns to existing best practice. The term contractors was adopted by the EBA after concerns were raised in the feedback to the EBA Guidelines around the use of the term third-party provider in this context (page 72).

- Regarding Article 19(1), It is unclear how a financial entity could include information on cryptographic techniques in its ICT security or digital operational resilience training. Such information is highly technical and would be irrelevant to all but highly specialist employees. The financial entity would also need to treat information regarding how it encrypts data with the appropriate caution and details of those processes should not be widely shared within the entity. We therefore recommend that this specific requirement be removed.

Question 21 Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion.

- No. As currently drafted, the requirements in Article 20(1)(b) are to be extended to ICT third-party service providers. We do not believe this is practical or responsible from a risk management perspective. For instance, a third-party service provider cannot be expected to adhere to the financial entities ICT security policies and procedures, nor would it make sense for them to do so as they would be tailored to the ICT environment of the financial entity. In line with our comments on question 20, we believe ICT third-party providers should be replaced by the term "contractor" in this context. We have suggested an edit to the text accordingly:
    - Art 20(1)(b): "*requirements for staff and ~~ICT third-party service providers~~ **contractors** to…*"

- Similarly, regarding Article 21(3)(a), we do not believe the current phrasing is appropriate. We therefore recommend the following amendment:
    - Art 21(3)(a): *A unique identity corresponding to a unique user account shall be assigned to each staff member of the financial entity or ~~staff of the third-party service providers~~ **contractor** accessing the information assets and ICT assets of the financial entity. These identities shall be linked to a specific natural person also in the case of reorganisation or after the contractual relationship has ended without prejudice to the retention requirements set out in EU and national law. Financial entities shall maintain records containing every identity assignment*.

- In relation to Article 22(1)(e)(iv), we believe it is important that financial entities be able to take a risk-based approach to reviewing access rights. While the regular timelines are unlikely to be a problem, it is unclear what level of review would be required whenever a change is necessary at user level. For instance, does adding a new user necessitate a review of all access rights across all ICT assets? For a large organisation where access rights change on a regular

basis as a result of staff change, this would not be manageable. It may be possible to review access rights for that specific ICT asset after a change at user level, but this too may not be feasible for some ICT assets within a large firm. Instead, we believe that annual or semi-annual reviews, as required in the rest of this Article, should be sufficient to successfully manage risk within an acceptable level. We therefore recommend:

- Article 22(1)(e)(iv): *review of access rights, at least once a year for all ICT systems, other than critical ICT systems and at least every six months for ICT systems supporting critical or important functions.* ~~*Review of access rights shall be performed also whenever a change is necessary at user level.*~~

- The omission of any reference to monitoring of anomalous behaviour additionally creates confusion as to how to interpret the Level 1 text with regards to user monitoring. Article 15 of DORA specifically states the ESAs shall "develop further components of the controls of access management rights referred to in Article 9(4), point c, and *associated human resource policy* specifying access rights, procedures for granting and revoking rights, *monitoring anomalous behaviour in relation to ICT risk through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices*."

- Finally, we note that access controls would not necessarily sit under a financial entity's HR policy. The industry will assume that provided these controls exist within various frameworks, they do not need to be specifically within the HR policy. We recommend the removal of the HR reference.

Question 22 **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 new measures or controls proposed.

Question 23 **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.**

- No. The definition of ICT-related incident could be interpreted broadly to include a large number of incidents, or even potential threats which did not lead to an incident and which should be treated differently within the financial entity. For example, an employee losing access to home wifi while on a client call could be considered an adverse impact on the availability of the service provided by the financial entity. If all such incidents of negligeable impact were to be in scope, then the documentation, classification and recording requirements in Article 23 would be overwhelming for a financial entity and would distract from good risk management. We therefore believe that it is necessary for a financial entity to apply proportionality and a risk-based approach to its interpretation of what constitutes an ICT-related incident, and specifically "anomalous activities and behaviours". Additionally we recommend the following:
  - Article 23(1)(b): *establish a list of* ***relevant*** *contacts with internal functions and external stakeholders that are directly involved in ICT operations security,*

including on detection and monitoring cyber threats, detection of anomalous activities and vulnerability management;

- For Article 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 the following amendment to remove response and recovery plans in this section and avoid confusion:
    - Art 23(1)(f): *review and update at least once a year the ICT-related incident management policy, its procedures, protocols, and tools. ~~The ICT response and recovery plans shall be reviewed against a range of different plausible scenarios.~~*

- Regarding Article 24(2)(a)(i), we flag that the language is very broad and the ask is unclear, in particular, what is meant by anomalous events related to "*internal and external factors".* The requirement to analyse, record and evaluate *"all anomalous events"* should be subject to the caveat "***taking a risk based and proportionate approach***".

- Regarding Article 24(2)(a)(ii), it is similarly 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 the following amendment:
    - Art 24(2)(a)(ii): *potential internal and external threats, ~~including usual scenarios of detection used by threat actors and scenarios~~ based on threat intelligence activity*

- Regarding Article 24(2)(c), we believe the primary purpose of this requirement is to ensure that alerts function and are monitored at all times. Given that, we find the reference to managing incidents within RTO to be confusing and unnecessary. As the text is currently drafted, it implies that the detection is management within an RTO, not the incident itself. Further, managing an incident within an RTO depends on a great number of factors in addition to detection time. Therefore equating the two concepts is not appropriate here. We suggest removing the reference to managing an incident within RTO, and adding the word "prompt" in front of detection in order to convey the expectation that alerts are considered and acted upon in an appropriate time. We therefore recommend the following amendment:
    - Art 24(2)(c): *define the alerts referred to in point (b), to allow the **prompt** detection of ICT-related incidents ~~to be managed within the expected recovery time,~~ both during and outside working hours.*

- Regarding Article 24(2)(d), the text of this requirement is incomplete and therefore it is unclear what the expectation on financial entities is. Do the ESAs intend that all scenarios under subclause 24(2)(a)(ii) are monitored? We also note our comment above that the reference to scenarios is confusing in this context and suggested that it be removed. That is equally the case here where the connection between logs and scenarios is not clear. 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. If that is accepted then this requirement should also be changed and we suggest the following amendment:

- Art 24(2)(d*): proactively monitor and analyse the logs collected in accordance with Article 12,* ***and taking into account alternative observability mechanisms*** ~~*ensuring that all scenarios identified under point 2(a)(ii), and the alerts specified in point (b) of this paragraph*~~;

- Regarding Article 24(2)(e), financial entities would need to take a risk-based approach to point (e). 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 prioritise based on risk, which is made up of a number of factors beyond only whether there is a connection to critical or important functions. We therefore recommend the following amendment:
  - Art 24(2)(e): *record, analyse and evaluate* ~~*all*~~ *relevant information on* ~~*all*~~ *important anomalous activities and behaviours automatically where possible, or manually by staff;*

- Regarding Article 24(4), we believe the word data is a typo and that the ESAs intended to require the identification of the date of the incident.

- We recommend amending the wording of Art 24(5)(a) to "indications that malicious activity may have penetrated an ICT system or network, and may cause actual harm." The current wording is too broad and likely to result in too many false alarms being captured.

Question 24 Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

- We stress that in practice the ICT business continuity plan under Article 25 will be integrated into the financial entity's broader business continuity plan, as a sub-set of ICT related considerations. Any expectation that the Level 1 mandate requires a separate, standalone ICT business continuity plan would represent an operational risk. A holistic approach which encompasses ICT-related issues is the safest and most effective way of avoiding disruption. Yet the wording taken in DORA and the RTS is likely to create confusion within the industry, most notably on whether there is a need to create and maintain a distinct policy for *ICT* business continuity. This is likewise the case regarding the ICT response and recovery plans under Article 27. We acknowledge that paragraph 92 of the consultation paper attempts to clarify that the financial entity has some flexibility in how these are organised, but would urge the ESAs to consider an additional statement in the recitals that clarifies how neither DORA nor the RTS mandate exactly where the information required is recorded, so long as it is readily accessible and part of a coherent and holistic plan.

- Similarly, client and counterpart communications (under Article 25(1)(j)) should not be framed within a siloed ICT context, but recognised to be part of the financial entity's wider communication plans, or as evidenced in other standards and policies (for example the Incident Management Standard).

- On Articles 26 and 27, we object to the mandating of specific scenarios as part of the business continuity and response and recovery testing: this could result in firms navigating towards the same prescribed scenarios rather than taking a risk based approach. Any financial entity needs to take a risk-based approach to testing and selection 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. We especially do not believe any financial entity could test all of the scenarios set out within Article 27(2) with any frequency. 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. Such flexibility is also the most effective way of enabling firms to react to "unforeseen circumstances" rather than seeking to provide for every eventuality, as could be suggested by Article 27(3). Above all, impact and likelihood must remain the primary lens through which the financial entity determines which tests to conduct and when. We therefore recommend an amendment:
    - Article 27(2) *The ICT response and recovery plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. The scenarios ~~shall~~* ***could*** *include,* ***but are not limited to,*** *~~all~~ ~~of~~ the following:*

- Further, we recognise the value of considering a severe, but plausible scenario for testing financial entities' resilience and making the assumption that controls have failed or been bypassed. However, scenarios that require the coordinated failure of a large number of preventative controls for which there is no precedent cannot be considered plausible. Equally, when designing a scenario the threat profile of the asset must be taken into account, for instance whether it is externally facing. Consideration of the threat profile, as well as ensuring plausibility, matters since by focusing on scenarios which are implausible and which require the assumption of the failure of a great many controls, authorities again risk driving attention toward areas where investment in resilience measures may be inefficient on ineffective in reducing risk compared to investment in preventative controls.

- On testing, we additionally flag that:

    - Regarding Article 26(2)(b), the benefits from ICT business continuity testing with third parties, in order to gain qualitative and quantitative data, can be quite limited. It can be challenging for third parties to dedicate time and resources to bilateral testing with each of their customers. This issue is often a point of contention during contractual negotiations and we recognise that some third parties must seek to balance their own resilience activity with the demands of their clients or members. We believe that it is important that financial entities are able to continue to rely on the assurances provided by third-party providers regarding their own ICT business continuity planning and testing regime, provided these are appropriately evidenced and meet the standards expected by the financial entity.

    - Article 26(2) uses the term "critical operations" while Article 27(1)(b) uses the term "critical ICT systems and services". To avoid confusion the RTS should consistently

adhere to the term "critical and important functions" with financial entities recognised as best placed to make the determination.

- Article 26(2)(c) should not lead to any expectation that switchover testing of tech, people and processes be conducted together at the same time.

- Finally, we note that Article 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. Additionally, we recommend the replacement of the word "*implement"* with *"prepare*", in terms of the continuity measures. Such measures are in many cases contingent on the failure occurring and should not be implemented in advance. We recommend therefore:
  - Article 27(4) *As part of the response and recovery plans, financial entities shall consider and ~~implement~~* ***prepare*** *continuity measures to mitigate failures of ICT third-party service providers~~ which are of key importance for a financial institution's ICT service continuity~~.*

Question 25 Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion

- No. We are concerned about the potential negative implications that the 2 hour RTO requirement in Article 25(2)(a). While this RTO is well established from the Principles for Financial Market Infrastructures, its applicability to the modern threat environment is questionable. We accept a 2 hour RTO as a target for non-malicious business disruptions, but in the event of a disruption caused by a malicious cybersecurity incident, we believe that a mandate to recover within 2 hours could drive CCPs and CSDs to attempt to recover outside of their risk appetite and before the necessary mitigation processes have been completed. We note that in their thematic findings to their 2022 Cyber Stress Test, the Bank of England noted that "*there might be instances where the disruption caused by an incident was such that, despite prior planning, attempting to recover by the end of the value date could have a more adverse impact on financial stability than failing to do so".* We support this finding and encourage EU authorities to consider the implications of a policy that may encourage financial entities to attempt to recover from a cybersecurity incident in such a way that the adverse impact to financial stability increases.

- It is also the case that 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. The financial entity may determine that it can tolerate an RPO of 12 hours for some data, but 2 hours for others. It is also the case that the more frequent the financial entity backs up its data, the greater the likelihood that any corruption is copied to the back-up rendering the data unusable. A financial entity will need to balance these risks versus investment in technologies such as data immutability. We recommend that the text of Article 25(4) be amended to:
  - Article 25(4): *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*** ~~*close to zero*~~*.*

- Regarding Article 26(3,4) it may not always be appropriate to include members in the testing of ICT business continuity plans. We recommend the inclusion of the phrase "***where applicable***", similar to the formula in Article 26(2)(b).

Question 26 **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.**

- This Article is very disproportionate, with the information sought creating overlap with the incoming Register of Information and other regulatory reporting obligations such as the SREP ICT Questionnaire, the JST (Joint Supervisory Team) regular engagements, specific onsite inspections and the new cyber resilience stress test. It reduces unnecessarily the flexibility for a financial entity to make continuous updates to ICT related frameworks, while failing to provide any value-add. We would recommend the ESAs instead focus on setting out minimum requirements, with the financial entity to review their RMFs annually taking into consideration any of the criteria set out in Article 28(2).

[AFME is not responding to Qs 27 – 32 on the simplified risk management framework]

Contacts

AFME	Andrew Harvey	+44(0)20 3828 2694	andrew.harvey@afme.eu
AFME	Stefano Mazzocchi	+32(0) 2883 5546	stefano.mazzocchi@afme.eu
AFME	Coen Ter Wal	+44(0)020 3828 2727	coen.terwal@afme.eu
AFME	Marcus Corry	+44 (0)20 3828 2679	marcus.corry@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. AFME represent the leading global and European banks and other significant capital market players. AFME advocates for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. AFME aims to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work. For more information, visit https://www.afme.eu/