11 September 2023

FIA position on the ESAs first batch of DORA policy products

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

FIA appreciates the opportunity to comment on the European Supervisory Authorities' (ESAs) first batch of DORA policy products. We support the ESAs aim to further harmonise ICT risk management tools, methods, processes and policies, as tasked by Article 15 of DORA. However, we would like to highlight remaining industry concerns in our responses below.

General Drafting Principles

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.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- At the overarching level, the same risk will have varying impact on different firms. Therefore, potential impact should be assessed by the firm. A proportionate Risk Management Framework would reflect this and provide sufficient flexibility and discretion for firms.

- Moreover, 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 be able to prioritise resources to mitigate 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.

- 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. 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 suggest several amendments to the text to that end in the responses below.

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.

FIA does not fully agree with the approach followed. Rather than adopt the 5 chapters as prescribed, it would be more logical to scrutinize the specific DORA Level 1 Articles, instead of creating new chapter titles, which may cause confusion. For example, Article 9 of DORA talks about "Protection and Prevention", which

aligns with NIST CSF "Protect". It would be logical that RTS focuses on specific NIST "Protect" subcategories, such as Access Control, Awareness & Training, Data Security, etc.

Further harmonisation of ICT risk management tools, methods, processes and policies (Article 15)

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.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- Firms will have different approaches to segregating responsibilities across their lines of defense (LoD), depending on the corporate model in play. Therefore, uniformity across the industry should not be an objective.

- Regarding Recital 31, we believe the statements regarding the internal organisation of the three LoD model are confusing both in the RTS and the level 1 text. Specifically, Art. 6.4 of Regulation (EU) 2022/2554 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 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. Further, prescriptive requirements in other jurisdictions could create a conflict of regulatory requirements that would be unmanageable for a financial entity or make good risk management more difficult to achieve.

- 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 clarifications in its 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 in the recitals to the RTS which would provide legal clarity for financial entities who might otherwise feel compelled to interpret those statements literally.

- Development of security awareness programmes and digital operational resilience training should be assigned to respective skilled personal instead of the control function.

- In this vein, 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, and different financial entities will have different structures, we believe it is more important that these trainings are designed well and their effectiveness monitored than this being done by one function or another. Article 19 covers this sufficiently. We therefore suggest the following amendment:

- Recital 31. Article 2 of the proposed draft RTS details the minimum list of ~~tasks and~~ responsibilities to be assigned to the control function referred to in Article 6(4) of DORA. **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.**

- 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 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.

- Regarding Article 2.1(f), we believe financial entities should retain the freedom to determine which function develops training and awareness programmes. It is rightly the role of a control function to monitor effective implementation, and it is possible that they could also develop the 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. 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.

Q4: Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- We believe clarification is required on whether the ICT Risk Management Policy referenced within Article 4 must be developed as a stand-alone DORA policy/document, or whether the requirements can be mapped across various existing policies and frameworks.

- Risk Tolerance Levels are defined and documented, but typically not within policy documents. The term "Risk treatment measures" does not reflect common industry terminology. This should be classified as "Risk mitigation measures".

- Regarding Article 3.3, it may not be necessary to update policies and procedures in responses to 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:
    - Article 3.3. 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.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- We believe that in this section in particular, it is important for financial entities to take a proportionate 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. For instance, an employee may choose to bring their computer mouse with them on a business trip resulting in a change of location that has no discernible impact on the financial entity's risk profile.

- Further, 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 in line with Article 4.2.b.ii of this RTS.

- Another example of where a financial entity needs to be able to apply proportionality and a risk-based approach is in the assessment of risk from legacy ICT systems. A financial entity may have old and disconnected hardware in its possession which is going through a decommission process. While this is considered legacy ICT systems, performing a specific ICT risk assessment on such an asset, according to Article 4.2.b.v of this RTS, would be a waste of resources and add no value from a risk management perspective. A financial entity needs to maintain the freedom to make this decision in order to ensure that resources are maximised in the service of mitigating ICT risk.

- Finally, it may not always be possible for a financial entity to document the links of all ICT assets to business functions as per Article 4.2.b.ix. 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.

- Therefore we recommend the following amendment:
    - Recital 42. One of the basic and initial steps in ensuring that the availability, authenticity, integrity and confidentiality of data is preserved, is the correct identification and classification of ICT assets and information assets. Without a correct identification and classification, it is very difficult to have a correct knowledge of these assets and a correct adaptation of the rest of the elements of the ICT risk management framework to them. In this line, Article 8(1) of DORA establishes that as part of the ICT risk management framework, financial entities shall identify, classify and adequately document, among others, their information assets and ICT assets**, taking into account the proportionality principle in Article 4 of DORA.**

- From our point of view, the Level 1 text does not refer to a policy requirement but focuses on the use of inventories. We believe clarification is required, whether a stand-alone policy is expected and/ or existing databases are required to be collated centrally.

- Regarding Recital 43, we believe that it is helpful to clarify that the RTS does not prescribe the creation of a single inventory or system of record. Such a clarification was given for the EBA ICT Risk Management Guidelines (page 94). We therefore recommend the following amendment:
    - Recital 43. Section III elaborates on the requirements of Article 8 of DORA through two articles. The first article requires financial entities to establish a policy for the management of ICT assets, complementing the elements already included in Article 8(6) of DORA with respect to the inventory of the ICT assets and information assets. **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. These RTS specify only what should be maintained.**

- Regarding Article 4.2, as per our comments on Recital 42, we believe it is particularly important for the proportionality principle to be acknowledged for these requirements. We therefore recommend the following amendment:
    - Article 4.2. **In line with the proportionality principles 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 or RTO, 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, as per the comments above, the proportionality principle is particularly important in ensuring that financial entities are able to focus resources and develop a manageable process for determining the criticality of ICT assets. We therefore recommend the following amendment:
    - Article 5.2. **In line with the proportionality principle in Article 4 of Regulation (EU) 2022/2554, s**uch procedure shall detail the criteria to perform the criticality assessment of information assets and ICT assets supporting 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.

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?

- 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 unnecessary and could conflict with continuous daily checks on hardware and software obsolescence.
- It goes without saying that this is an important information, but it should not be a prescriptive requirement in an asset management policy. It is more important to see that each asset should have required support either from a service provider or inhouse resources.

Q7: Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- We believe the encryption requirement should be limited to sensitive data, as classified by the financial entity.
- Moreover, the requirements for data, which cannot be encrypted should be changed from "held in a separate and protected environment" to "subject to network segmentation and/ or other compensatory measures" to make this feasible.
- Specifically, regarding Article 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.
- We therefore recommend the following amendment:
    - Article 6.2.(a) rules for the encryption of data at rest, in transit and, where relevant, in use, taking into account the results of the approved data classification and ICT risk assessment processes to protect the availability, authenticity, integrity and confidentiality of data. 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.

- Regarding Article 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:
    - 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.

- Regarding Article 7.4, the text should allow firms to take a proportional and risk-based approach to this requirement. 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 is digital operational resilience**. The register shall be kept up-to date.

Article 11(2)(g) and 11(2)(h) describe the controls needed to delete, dispose, or decommission data. FIA recognizes the importance of securely destroying information stored off-site, hosted at a third-party location, or maintained internally once the data is no longer required. However, FIA requests that the ESAs provide clarity that cryptographic deletion (i.e., the destruction of cryptographic keys) is a valid form of secure deletion. While the data is still available in encrypted form, the deletion of the keys needed to render the data would be destroyed, leaving the data unreadable.

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.

Q9: Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- We deem a general weekly frequency for vulnerability scanning/ assessments to be disproportionate. Frequency should follow a risk-based approach as defined by financial entities as per internal guidelines.

- As a common practice, backup and recovery requirements are part of and documented in scope of business recovery plans. Requirement for duplication within multiple policies should be avoided.

- Logging-requirements (Article 12) should distinguish between self-developed software and third party software.

- Regarding Recital 53, 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 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 Art. 8.2.c.iii. However, these should not 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 way financial entities choose to complete and maintain their ICT operations documentation may vary between organisations 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 in. We therefore suggest the following amendment:
    - Recital 53. ICT operating procedures shall cover key elements such as installation, maintenance, configuration, and deinstallation of ICT assets, as well as controls and monitoring of ICT systems, error handling, and recovery procedures. ICT operating procedures help maintain the availability, authenticity, integrity, and confidentiality of data, while also addressing legacy systems and interdependencies among ICT systems. By adhering to these procedures, financial entities can minimize disruptions to business operations, detect and respond to security incidents promptly, and ensure the continuity and security of their services. **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.**

- Regarding Recital 55, 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. We therefore suggest the following amendment:
    - Recital 55. In terms of capacity and performance management, financial entities, **with regard to the proportionality principle in DORA Article 4,** need to identify the capacity requirements of their ICT systems and implement resource optimization and monitoring procedures. The aim is to maintain and enhance the availability and efficiency of ICT systems while preventing capacity shortages. Specific attention should be given to systems with long or complex procurement processes or those that are resource intensive.

- Regarding Recital 56, the text of this recital is slightly ambiguous and could be further clarified. 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. As per the rest of the

recital, tracking disclosures and prioritising patching based on the criticality of the vulnerability are vital tasks to security operations. Instead, we believe the recital should reference the need for ICT third-party providers to 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. We therefore suggest the following amendment:

- Recital 56. Regarding vulnerability and patch management, financial entities must establish procedures to detect vulnerabilities and update relevant information resources accordingly. Regular automated vulnerability scanning and assessments, typically using specialized software tools, of ICT assets are required, especially for critical or important functions. Also, ICT third-party service providers should **appropriately address** ~~handle~~ any vulnerabilities and **provide adequate assurance on the state of their vulnerability management and patching programmes** ~~report them~~ to the financial entities. The tracking of ICT third-party libraries (including tracking patches and updates), disclosure of vulnerability-related information, and deployment of patches are also vital. Financial entities need to prioritize patch deployment based on vulnerability criticality and risk profiles, while monitoring and verifying remediation.

- On the same vein, regarding Article 10.2.c, we suggest the following amendment:
  - Article 10.2.(c) ensure that ICT third-party service providers handle 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** ~~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 Recital 60, while the industry recognises the importance of logging and monitoring, this 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 and have suggested text in line with the EBA's comments in 2019. We therefore recommend the following amendment:
  - Recital 60. Finally, developing and implementing logging procedures, protocols, and tools allow financial entities to secure networks, preserve data integrity, and detect anomalies. By identifying events to be logged, setting retention periods, and securing log data, entities can effectively monitor and investigate ICT security incidents. The level of detail in logs should align with their purpose and the usage of the ICT asset producing the log, facilitating accurate analysis. **The authorities consider that logging and monitoring requirements are important and need to be in place. However, the manner and extent to which they are implemented is decided upon by institutions proportionately.**

- Regarding Article 9.1, we note that capacity and performance management are not typically part of security procedures and therefore would not be recorded as suggested by Article 9.1.

- Regarding Article 10.4.c, while it is best practice to test patches in a non-production environment, financial entities need to maintain the flexibility to choose when this is appropriate. For instance, a critical vulnerability in an internet facing application, with proven exploit in the wild, should be patched as soon as possible. It may be the case that the application is not critical to the functioning of key business services and therefore the risk of disruption is preferable to an extended exposure of the non-patched application. Alternatively, similar patches may have already been tested for another similar application thereby giving the financial entity assurance about the utility and safety of the patch. In this case, the financial entity may again prefer to implement the patch directly into production. We therefore suggest the following amendment:
    - Article 10.4.(c) **where feasible and using a risk-based approach,** test and deploy software and hardware patch and updates in an environment, which replicates the production one, to avoid adverse consequences and disruption before their deployment to production environments;

- 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:
    - Article 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 that these baselines are those that are effectively deployed;

- Regarding Article 11.2.i, as per our comments on Recital 66, we do not recognise the term data leakage and believe it is better replaced with the term data loss. We therefore recommend the following amendment:
    - Article 11.2.(i) the identification and implementation of security measures to prevent data loss ~~and leakage~~ for systems and endpoint devices;

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.

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.

- We would support more proportionality for the frequency of vulnerability scanning/ assessments. The frequency should follow a risk-based approach as defined by financial entities as per internal guidelines.

- Automated vulnerability scanning on ICT assets should be commensurate to the classification and the overall risk profile of the ICT asset. It is important for financial entities to not just discover vulnerabilities, but to help understand vulnerability risks with threat context and insight into potential business impact. Some sophisticated financial entities may already conduct such scanning on a weekly basis regardless of

the ICT assets classification, so the frequency might not be a significant concern for them. However, weekly vulnerability scans may not be a feasible or even a beneficial approach for all financial entities. FIA encourages the ESAs to consider focusing on the need for more actionable vulnerability reports with a risk-based emphasis, rather than weekly automated scans for all ICT assets that may contain virtually no useful data.

- What is important is that financial entities retain the ability to risk accepting the non-scanning of some ICT assets based on their risk profile. Non internet facing assets, which do not have an active threat profile, would likely be well within the financial entities risk appetite not to subject these 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. We therefore recommend the following amendment:
    - (b) ensure the performance of automated vulnerability scanning and assessments on ICT assets, commensurate to their classification and overall risk profile of the ICT asset. ~~For those supporting critical or important functions it shall be performed at least on a weekly basis.~~

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.

Q13: Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- For larger firms, a requirement to review ICT systems supporting critical or important functions at least every 6 months could lead to continuous, rolling reviews. We recommend an annual review requirement.

- We do not recognise the term data leakage and believe it creates confusion. We note that the EBA chose to remove the term from its 2019 Guidelines on ICT and Security Risk management (see commentary page 81) and replace it with data loss, which we believe is more appropriate. We have suggested an amendment here and in other 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 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:
    - Recital 66. Regarding securing information in transit, financial entities must develop policies, procedures, protocols, and tools to protect data transfer. This includes ensuring the availability,

authenticity, integrity, and confidentiality of data during network transmission. Measures to prevent data ~~leakage~~ **loss** and secure information transfer with external parties are also essential. Confidentiality and non-disclosure arrangements, along with compliance assessments, protect sensitive information. Financial entities should also comply with data protection laws is required for the transfer of personal data. **All of this should be done taking into consideration the results of the approved data classification and ICT risk assessment processes.**

- Regarding Article 14.1, as per our comments above, we therefore recommend the following additional 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**. In particular, financial entities shall ensure all of the following:

- Regarding Article 14.1.b, as per our comment on Recital 66, we do not recognise the term data leakage and believe it should be replaced with data loss. We therefore recommend the following amendment: (b) the prevention and detection of data ~~leakage~~ **loss** and the secure transfer of information between the financial entity and external parties;

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.

Q15: Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- We recommend to separate project management and change management. In some organisations, this is managed by different functions and combining this into one document could cause unclear ownership responsibilities for some financial entities. Financial entities should have the flexibility to demonstrate that they cover off on DORA elements throughout their policies, standards and procedures structure rather than having prescriptive rules that would entail restructuring its policies.

- Regarding Recital 69, 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. 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. We therefore recommend the following amendment:
    - Recital 69. Section VII elaborates on these aspects through three articles. The first one focuses on the relevance of having a project management policy as a basic mechanism for ensuring the security of networks, against intrusions and data misuse and, in order to preserve the availability, authenticity, integrity and confidentiality of data. This article is based on the EBA Guidelines on ICT and security risk management, in particular Section 3.6.1, notably with regard to the elements

to be included in the policy. **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.**

- 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. We therefore recommend the following amendment:
    - Article 16.1. 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.** This policy shall:

- Article 16(6) requires financial entities to only store anonymized, pseudonymized or randomized production data in non-production environments. FIA requests that the ESAs consider limiting this requirement to data that is highly confidential or sensitive as there may be some situations where financial entities need to use actual production data in non-production environments to simulate a change. While the data is real, it is no longer useable to a threat actor and therefore would not warrant strong information security controls. FIA does agree that certain information should be protected, therefore requests for Article 16(6) to read: Financial entities shall protect the integrity and confidentiality of data in non-production environments. Highly sensitive and confidential data (e.g., Personally Identifiable Information (PII)) shall be anonymized, pseudonymized or randomized in non-production environments; controls should be in place that are commensurate with the data classification of information being stored in non-production environments."

- Regarding Article 17.2, the text says that this requirement applies to "all changes". This could encompass many minor or Business as Usual (BaU) updates that do not qualify as a major change. In addition, as drafted it covers software, hardware, etc. of 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 impacts on financial entities' ability to maintain their BaU 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.

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.

Q17: Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.

Q18: Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.

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.

Q20: Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- 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 training them improve the entity's resilience capabilities.

- 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. We therefore recommend the following amendment:
    - Article 19.1. Financial entities shall include in specific ICT security awareness programmes and digital operational resilience training elements regarding the security of networks, the safeguards against intrusions and data misuse and the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, ~~including the cryptographic techniques used~~. The ICT security awareness programmes and digital operational resilience training shall be aligned to the overall ICT security awareness programmes and digital operational resilience training referred to in Article 13(6) of Regulation (EU) 2022/2554.

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.

FIA does not agree with the approach followed. Below, we share remaining industry concerns:

- 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.

- Regarding Article 20.1.b, We do not believe the requirements in Article 20.1.b are appropriate for ICT third-party service providers as this would present security risks for the financial entity and would likely not be possible to agree in contracts. These requirements are more appropriately suited to contractors employed by the financial entity. We therefore recommend the following amendment:
    - Article 20.1.(b) requirements for staff and ~~ICT third-party service providers~~ **contractors** to:

- Regarding Article 21.3.a, for the same reasoning as given for Article 20.1.b, we do not believe this is appropriate. We therefore recommend the following amendment:
    - Article 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.

- Regarding Article 22,1.e.iv, we believe it is important that financial entities be able to take a risk-based approach to the review of 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 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 review required in the rest of this Article should be sufficient to successfully manage risk within an acceptable level. We therefore recommend this requirement be removed. We therefore recommend the following amendment:
    - 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.~~

- In Article 22.1.e.iv, period review of access rights should be conducted on a risk-based approach, such as accounts with privileged rights. Prescribing this review requirement for “once a year for all ICT systems” is excessive.

- Lastly, access controls are not necessarily embedded in HR policies. Hence, we believe that control documentation within various frameworks is sufficient and, therefore, additional documentation in HR policies will not be required.

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.

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.

FIA does not agree with the approach followed. Below, we share remaining industry concerns:

- The definition of ICT-related incident could be interpreted broadly to include a large number of incidents. 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.

- For Article 23.1.b, we recommend the following amendment:
    - 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:
    - Article 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.ii, 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 the following amendment:
    - Article 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 managed 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:

- Article 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, for example whether the ESAs intend that all scenarios under point 2(a.ii) are monitored. We also note our comment above that the reference to scenarios is confusing in this context and suggest 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:
  - Article 24.2.(d) proactively monitor and analyse the logs collected in accordance with Article 12 ~~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:
  - Article 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.

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.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- A holistic business continuity plan which addresses ICT-related issues is the safest and most effective way of avoiding disruption and reflects common standards. Specific scenarios should not be mandated but defined by the firms taking a risk-based approach, which would lead to increased proportionality.

- We note that the approach and wording taken in DORA and the RTS is likely to create confusion within the industry, most notably on the difference between the ICT risk management framework, ICT resilience and recovery plans, and business continuity plans. Typically these are related by distinct disciplines within a financial entity and we do not believe it is practical or desirable from a risk management perspective, to combine them. Some of the considerations and requirements in the RTS and DORA rightfully belong to these different areas and could not adequately be covered under the others. For instance, an individual application will have a recovery plan that needs to be recorded and understood by the application owner as part of technology recovery planning. However, a business continuity policy needs to be focused on the level of the business service, which may have any number of individual applications supporting it. As a further example, the criteria for activating the technology recovery plans of an individual application are likely to be very different from activating the business continuity and recovery plans, as well as crisis management. These should be aligned and complimentary in how the financial entity builds resilience, for instance the RTO/RPO targets for an individual application need to support the RTO/RPO for the business they support. But recording them in the same document, or setting ownership within the same team, is often not scalable or helpful within a financial entity. We acknowledge that recital 92 attempts to clarify that the financial entity has some flexibility in how these are organised. However, we ask that the ESAs consider an additional statement in Recital 92 that clarifies that neither DORA nor the RTS mandate exactly where the information required in both the level 1 and level 2 texts is recorded within the financial entity so long as it is readily accessible and part of a coherent and holistic plan to deliver good resilience and risk management.

- FIA notes that Article 26.2 asks financial entities to test viability of their business until "critical operations" are restored. FIA requests for the ESAs to replace "critical operations" with critical or important functions, to remain consistent with DORA EU 2022/2554.

- The industry requests clarity on the meaning of Article 26.2.a. 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 if this Article references the scenarios given in Article 27.2. We do not believe any financial entity could test all of these scenarios for all its ICT business continuity plans 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. 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 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:

- Moreover on Article 26.2.a., 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 risk driving attention toward areas where investment in resilience measures may be inefficient on ineffective in reducing risk compared to investment in preventative controls.

- Regarding Article 26.2.b, the opportunity for ICT business continuity testing with third parties to gain qualitative and quantitative data for evidence to meet their recovery plans 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 recognize 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 appropriate evidenced and meet the standards expected by the financial entity.

- Regarding Article 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:
    - Article 27.1.b, describe what actions shall be taken to ensure the availability, integrity, continuity and recovery of at least the ~~critical~~ ICT systems **supporting the critical and important functions** ~~and service~~ of the financial entities;

- Finally, we note that Article 27.4 creates a new category of ICT third-party provider of "key importance" to 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.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- 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 PFMIs, its applicability to the modern threat environment is questionable. We accept a 2hr RTO as a target for non-malicious technology of business disruptions, but 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. 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.

- Regarding Article 25.4, 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 house for some data, but of 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 the following amendment:
    - 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.

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.

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

The format and content of the report on the ICT risk management framework is overly detailed and, given the numerous causes that would result in a report being required, excessively frequent. Due to the complexity of the reports, it is unlikely that financial entities will be able to fully complete all reports within the year required and this would soon overwhelm entities. An entity's risk management framework is held across numerous functions (e.g. technology risk, cybersecurity, compliance) and various teams and any reporting will require coordination across all relevant governance forums with appropriate senior sign-off. In order for the report on the ICT risk management review to focus on improving an entity's resilience, we recommend that the report is only required once annually and reports on the effectiveness of the entity in complying with the RTS in the preceding year.

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.

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.

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.

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.

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.

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.