EIOPA - IRSG

ESMA
European Securities and Markets Authority
Securities and Markets Stakeholder Group

EBA EUROPEAN BANKING AUTHORITY
BANKING STAKEHOLDER GROUP

JC 2023 39

Deadline: 11 September, 2023

JC Consultation Paper: draft RTS to further harmonise ICT risk management tools, methods, processes and policies under DORA Arts 15 and 16(3)

Introduction

The Joint Committee (JC) is seeking feedback on draft Regulatory Technical Standards (RTS) which the ESAs are mandated to develop under Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, commonly referred to as 'DORA'. These draft RTS relate to the further harmonization of ICT risk management tools, methods, policies and processes under empowerments in DORA Article 15 and a simplified ICT risk management framework for certain entities under DORA Article 16. This part of the legislation relates to the management of ICT risks by financial institutions, rather than the regulation of certain critical third party ICT service providers.

While the empowerments are set out in Articles 15 and 16, they relate to other substantive Articles of DORA on specific aspects of the ICT Risk Management Framework and so the proposals must be read in conjunction with the relevant parts of the underlying DORA Regulation, referred to here as the 'Level 1' text.

Given that the DORA legislation and the RTS is cross-sectoral, and that digital/cyber-resilience also extends beyond the financial sector, the ESAs have consulted ENISA and referred to a range of existing standards in preparing the drafts, including: EBA Guidelines on ICT and security risk management (2019), EIOPA Guidelines on ICT security and governance (2020), NIS2 Directive and the NIST cybersecurity framework components, as well as ISO-IEC 27000 family standards, 2020 FSB CIRR toolkit, the G7 Fundamental Elements of Cyber security in the financial sector, CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, the BCBS principles for operational resilience and sound management of operational risk, effective risk data aggregation and risk reporting.

Mirroring the cross-sectoral collaboration undertaken by the ESAs to prepare the consultation, the stakeholder groups of the three ESAs have accordingly sought to collaborate to prepare a joint

response. Where necessary, we have identified any comments which we consider to be specifically relevant for one or more sector or type of financial entity.

Given the significant number of questions and the parallel consultations on other aspects of DORA we have not answered all EBA's questions.

General comments

We welcome the overall approach the JC has taken of setting overall principles, with further specification for specific sectors or types of entity only where necessary in the light of their activities and the associated risk profile. We consider this is likely to be both simpler to implement and more effective than trying to anticipate and prescribe in advance every detail.

We are also pleased to see that the three ESAs are working together as a single, integrated team which is necessary to deliver the regime efficiently and in a timely way, to make the best use of the available resources, and to ensure appropriate coherence in the resultant regime.

Many of our specific comments are designed to ensure that in implementing the risk management framework, financial entities pay due consideration to the impact of an incident on its customers and users. This will help financial entities themselves by providing clarity about priorities and helping to reduce the reputational harm and other fallout from incidents that arise. It should also reduce the harm to customers, which is not only financial, that can arise from such incidents.

Finally, we think it would be useful in due course to consider how physical impacts of climate change could interact with the ICT aspects of business continuity planning and incident recovery and to make a more explicit connection within the RTS to considering climate scenarios and climate stress tests in digital operational resilience. Some climate-related issues (e.g. a change in the propensity to flood of an area where datacentres are located) have a direct impact on digital operational resilience, while recognising that there are broader aspects of climate change that may be less directly relevant.

Answers to specific questions

Proportionality

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.

We agree that it is appropriate to include proportionality in this way as not all distinctions of risk and scale can be identified in advance and included explicitly in the rules. Incorporating this principle is

therefore useful. However, we think it is important that the proportionality criteria include consideration of the impact on customers and users, not just on the financial entity, and therefore suggest adding words as follows:

"For the purposes of defining and implementing ICT risk management tools, methods, processes and policies referred to in Articles 1 to 28 elements of increased complexity or risk shall be taken into account, including elements relating to encryption and cryptography, ICT operations security, network security, ICT project and change management, and the potential impact of the ICT risk on confidentiality, integrity and availability of data, and of the disruptions on the continuity and availability of the financial entity's activities **and on its customers and users**."

We also think there would be benefit in carrying out supervisory convergence work after implementation to ensure appropriate coherence and consistency in the assessment of risk and complexity undertaken by different authorities.

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.

We welcome the explicit consideration of proportionality considerations.

Q3. Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.

We consider it important that assigning responsibilities to the 'control function' does not relieve the business itself, as first line of defence, of responsibilities to 'design-in' and facilitate the delivery of robust information security and service delivery. Doing so could mean that in practice security considerations are considered too late in the day or remotely from other decisions to be effectively incorporated. We therefore suggest that the JC consider changes to the wording of Article 2, paragraph 1, point (b) and point (f) as follows:

(b) ~~**managing and**~~ monitoring and **ensuring the management of** the financial entity's ICT risk in accordance with requirements laid down in Section II of this regulation and Chapter II of Regulation (EU) 2022/2554;

(f) ~~**developing and**~~ monitoring the effective **development and** implementation of ICT security awareness programmes and digital operational resilience training referred to in Article 13(6) of Regulation (EU) 2022/2554.

We also think that consideration should be given to including a provision on the role of assurance in both preventing and remediating problems and in verifying the first line's assessment of ICT robustness and resilience, and that at least for systems supporting critical and important functions and for complex change projects that is likely to require some external assurance.

In Article 1 (2c) it is unclear whether having a specific policy for exception management, governing the lifecycle of exceptions, should be enough. Also, the requirement to record all potential exceptions could be unfeasible and should incorporate some criteria to discriminate exceptions according to risk, breadth of scope and/or pervasiveness in specific domains.

We do not think adequately that a policy for security policies should define the consequences of non-compliance with those policies for staff members as indicated in Article 1 (2e). Banks articulate policies for employees that are not compliant with internal policies generically but not at specific policy level. This requirement has not been seen in other policies, nor required by any other EBA guidance.

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

In Article 3(1)(b) to Article 3(1)(e) it is unclear whether the aim is to describe the content of the risk assessment methodology and procedure or the result: i.e. is this describing the procedure and methodology to identify vulnerabilities and threats, or what those threats and vulnerabilities actually are. We think that both the content and result are needed and suggest that the easiest way to achieve this could be to include an explicit provision on the documenting of key assessments and decisions made in accordance with the policy and process as follows:

(f) requirements for the documentation of key assessments and decisions made in the implementation of the policy.

We also think that consideration should be given to including a provision on the role of assurance in both preventing and remediating problems and in verifying the first line's assessment of ICT robustness and resilience, and that at least for systems supporting critical and important functions and for complex change projects that is likely to require some external assurance.

Finally, we suggest referring to 'risk mitigation measures' rather than 'risk treatment measures' in, for example, Article 3(1)(c) to better align with standard terminology.

Q5. Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.

We consider that the objectives specified in DORA Article 15(a) which underpin these provisions are broader than those incorporated in the current text. The missing element should be incorporated because the penetration of systems may result in harm to the institution and its customers even where the data remains available, for example where it enables a denial of service attack. We therefore propose the following addition:

1. As part of the ICT security policies, financial entities shall develop, document and implement a policy on management of ICT assets, with a view to **ensuring the security of networks against intrusion and** preserving the availability, authenticity, integrity and confidentiality of data.

In relation to the protection of data, we consider that it would be helpful to make specific reference to the documentation of 'end-of-life' procedures for the ICT assets to ensure that data cannot be compromised after the ICT asset is taken out of use. We therefore propose to add a new point x) as follows:

x) the measures to be taken at the end of the ICT asset's use to protect the integrity of data.

In Article 5(2) it is important that the assessment of the impact of data loss takes explicit account of the impact on customers, users or counterparties not only the financial institution's business processes and activities. Without this requirement there is a potential for financial entities to make prioritisation decisions that do not take account of the wider market impact of data being compromised or unavailable. We therefore propose an addition as follows:

2. Such 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 the **financial entity's** business processes and activities **and its customers, users or counterparties**.

Article 4.2. v prescribes that the financial entity will keep records of all the information needed to perform specific ICT risk assessment on all legacy ICT systems. We think that it is an excessive burden for institutions to include all this information, we think only information needed to assess the criticality of the application should be stored for all systems, and only when an application is critical all other information should be stored.

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?

Yes. This should help financial entities themselves to identify and manage sources of potential risk and is a key safeguard for customers, users and counterparties who may be affected if such risks are not managed. The risk profile of an asset increases significantly once it is out of support, so clarity on when this will happen is an important first step towards risk management.

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

In general we agree with the approach taken.

In particular, we support the reference to 'leading practices' given the rapid evolution likely to occur in this area. We also support the requirement to document the reasons where a financial entity concludes it cannot adopt such 'leading practices', and the mitigation and monitoring undertaken as a result. However, it would be useful to identify – not necessarily in the legal text but perhaps in supporting material – the kinds of situations in which it might be necessary and acceptable not to use leading practice. Given the quick evolution on encryption technology and practices and the time required to adopt them, policies should reflect adoption times, having in mind that "leading practices" could change due technology evolution (even when the former leading practices stay secure) or due to not being secure or due to vulnerabilities published in protocols (e.g. TLS 1.0)

In relation to Article 6(2)(a), we note that it is increasingly feasible to encrypt data 'in use' and that such encryption is likely to be the best way to protect 'in use' data. If there are situations where this is not possible with the available technology, we agree that there should be a requirement for a segregated environment, although some stakeholders envisage this would be costly to implement and would welcome clarification of the benefits in terms of risk reduction. Developing a new segregated environment for data that cannot be encrypted at use can be excessively prescriptive on the mitigation solution, it could be better stated that banks should define compensatory measures to minimize the associated risks.

On the other hand, we think that this provision should make it clear that data must be encrypted in the case of sensitive data, and depending on the classification of the information established by the entities. The current wording is not too clear, and it seems that it is necessary to encrypt all data, regardless of its classification.We think it is important to include the specific measures on cryptographic key management in Article 7 given the impact of any loss or failure to protect such keys on entities and their customers.

Q8. Is there any new measure or control that should be taken into consideration in the RTS [on encryption and cryptography] 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.

Yes, subject to the points below.

Article 10(2)(b) requires a weekly automated scan for vulnerabilities in relation to critical systems. There may be situations where:

- in times of heightened threat a weekly scan is clearly insufficient;
- regardless of the scanning an entity is specifically alerted to a particular vulnerability.

We consider that provision should be made for these two situations, such as the following:

(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 **or more frequently where a heightened threat level or vulnerability is identified by or notified to the financial entity**.

Article 10 does not appear to require patches to be deployed promptly once identified, even though it is not until the patch is deployed that the risk is reduced and it is entirely possible that an extended delay between identifying the patch and implementing it could be the root cause of vulnerabilities being successfully exploited. We do not think this gap is addressed by the wording on prioritisation in point (g) because 'prioritise' is used there more in the sense of determining relative priorities. We therefore suggest adding to point (f) as follows:

"(f) deploy patches **promptly** to address identified vulnerabilities. If no patches are available for a vulnerability, financial entities shall **promptly** identify and implement other mitigation measures;"

The criteria for prioritisation of patches in Article 10(g) should also cover the impact of a successful exploitation of a vulnerability on customers, users or counterparties, not just the criticality to the entity itself"

(g) prioritise the deployment of patches and of the other mitigation measures, where applicable pursuant to point (f). For the purposes of the prioritisation, financial entities shall consider the criticality of the vulnerability, the classification and risk profile of the ICT assets affected by the identified vulnerabilities **and the impact of a successful exploitation of a vulnerability on customers, users or counterparties**;"

Article 10(2)(c) requires the ICT TPSP to handle "any" vulnerability. It would be useful to consider whether there is scope for incorporating a risk-based approach more explicitly in this requirement.

In Article 12(2)(c)(i) and in relation to logging for physical access control it would be preferable to limit the scope to the financial entity's premises that hold critical and important ICT [processing] facilities.

Article 12(2)(g) requires the synchronization of all the financial entity's clocks to a single, reliable reference source. Given that for trading venues and their members both the acceptable sources and tolerances for the required accuracy are already specified in Level 2 measures, we consider it would be helpful to include a cross-reference here, as follows:

(g) the synchronisation of the clocks of all the financial entity's ICT systems upon a single reliable reference time source, **taking account where applicable of the time source and accuracy requirements in Commission Delegated Regulation 2017/574**.

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 believe that requiring vulnerability scans to be performed on a weekly basis for assets supporting critical and important functions is too demanding. A monthly periodicity would be more in line with the risk criteria referred to in this same article.

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.

In relation to Art 13, (b) mapping and visual representation of all the financial entity' networks and data flows, maintaining up-to-date diagrams of this type is extraordinarily costly and technically challenging. A clarification of the expected level of detail and scope would be helpful, as it is obviously impossible to maintain this for "all networks & data flows". Perhaps it should be considered to maintain only the most critical.

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.

We welcome the inclusion of provisions on ICT project and change management to address situations in which exposure to risks and vulnerabilities can change and may be particularly acute.

We welcome the fact that the requirements are applied to both the 'acquisition' and 'development' of systems as both require effective security management. We think it is important to clarify that the requirements apply not only in relation to the initial acquisition or development, but also to any subsequent development, upgrade or material reconfiguration, for example as follows:

2. The ICT project management policy shall define the elements to ensure effective management of the ICT projects related to the acquisition, maintenance and, where applicable, **the initial and any subsequent further** development **or material reconfiguration** of the financial entity's ICT systems.

In relation to art. 15 g) testing of all requirements, including security requirements, and respective approval process when deploying an ICT system in the production environment, we would ask for clarification about what is meant by "all requirements" since it could be unapproachable as part of all the changes. Perhaps it is necessary to clarify that they are only the requirements associated with the change itself.

We propose that two extra matters should be addressed in Article 15(3):

- Criteria for 'Go/no go' decisions should include consideration of the risk of harm to customers/users/counterparties from either decision, at least for critical systems; and
- It would be helpful to specifically reference the identification and management of interdependencies in planning and in 'go/no go' decisions.

3. The ICT project management policy shall include all of the following elements:

(a) project objectives

(b) project governance, including roles and responsibilities;

(c) project planning, timeframe and steps;

(d) project risk assessment**, including identification and management of dependencies**;

(e) key milestones;

(f) change management requirements;

(g) testing of all requirements, including security requirements, and respective approval process when deploying an ICT system in the production environment;
(h) criteria for 'go/no go' decisions on deployment which take account of the risk of harm to the financial entity's customers or users from either decision.

We agree that it is important to ensure appropriate reporting on ICT projects to the management body. A typical problem with such reporting is that information is conveyed in a way which might be meaningful for IT professionals but does not convey the impact on the business, its customers, clients or counterparties. We think it is important that this problem is recognised and addressed. This would help both the customers, clients and counterparties and also enable the financial entity to better manage reputational and other risks. We therefore propose an addition to paragraph 5 as follows:

5. The establishment and progress of ICT projects impacting critical or important functions and their associated risks shall be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, periodically and, where necessary, on an event-driven basis, in accordance with ICT project risk assessment included in paragraph 3, point (d). **Such reporting should be in a form that conveys to non-ICT specialists the business impacts and impacts on customers, users and counterparties of the status of the ICT projects and of any alternative options under consideration.**

It is important that Article 16(2) applies in relation to any upgrade or reconfiguring of functionality, not just to the initial deployment. This should be clarified. It is also important that assessment of criticality takes account of the impact on customers and users, not just the financial entity itself.

We propose to address the first two points as follows:

Financial entities shall develop, document and implement an ICT systems acquisition, development, and maintenance procedure, for testing and approval of all ICT systems prior to their use and after maintenance. **The policy shall cover the initial acquisition or development and any subsequent development or significant reconfiguration.** The level of testing shall be commensurate to the criticality of the concerned business procedures and ICT assets **and the risk of harm to customers or users from any resulting incident or outage**. The testing shall be designed to verify that new ICT systems are adequate to perform as intended, including the quality of the software developed internally. Financial entities shall use test data and environments that adequately represent the production environment. In addition: (a) a CCP shall involve, as appropriate, in the design and conduct of these tests, clearing members and clients, interoperable CCPs and other interested parties;

And the third point by adding a new point (c) based on the drafting for CSDs.

(c) a **trading venue** shall, as appropriate, involve in the design and conduct of these tests: users, critical utilities and critical service providers, other **trading venues**, other market infrastructures, and any other institutions with which interdependencies have been identified in its business continuity policy.

Article 16.5 establishes that Financial entities shall perform security testing of software packages not later than the integration phase. A clarification is needed on what is meant by "packages", whether it is an application unit or if it refers to each of the libraries, including OSS and third-party proprietary software.

As per article 16.9."The source code and proprietary software provided by ICT third-party service providers or coming from open-source projects shall be analysed and tested for vulnerabilities." This requirement is difficult to guarantee for the owner; it could be prohibited in the license to perform these tests or be complex due to not having the source code. Clarification is needed on what is expected for third-party software for which financial institutions do not have source code or for which there is no compile in-house.

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.

We agree that it is appropriate to have provisions relating to CCPs and CSDs that involve appropriate users in testing, given the centrality of CCPs and CSDs to the functioning and stability of markets.

However, we are surprised not to see analogous provisions for at least the most significant trading venues. Trading venues also play a key role in enabling the market to function and in some cases are not substitutable for alternative venues. Furthermore, as ESMA has indicated in its consultation and subsequent Opinion on Market Outages there have been many challenges with outages at exchanges, and significant potential wider market impacts where, for example, closing auctions cannot take place. Some other jurisdictions have already recognized this through enhanced requirements for market infrastructures including significant trading venues, and associated supervisory oversight programs. An example is the US SEC's Regulation Systems Compliance and Integrity ('Reg SCI'). We think this gap in

the JC's proposed requirements should be addressed. We also note that the SEC is currently consulting on expanding the scope of Reg SCI to a wider range of entities and would encourage the JC to consider whether such an approach would have merit here.

(c) a **trading venue** shall, as appropriate, involve in the design and conduct of these tests: users, critical utilities and critical service providers, other **trading venues**, other market infrastructures, and any other institutions with which interdependencies have been identified in its business continuity policy.

We also think that consideration should be given to similar provisions for Approved Publication Arrangements (APAs) and Approved Reporting Mechanisms, at least in relation to users.

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

We think it should be made explicit that the financial entity needs to take into account the impact of any incident on its customers in determining priorities and proportionality for protection of physical and environmental security, as follows:

2. The physical and environmental security policy shall include all of the following:
(a) measures to protect the premises, data centres of the financial entity and sensitive designated areas identified by the financial entity where ICT assets and information assets reside from unauthorised access, attacks, accidents and from environmental threats and hazards. The measures to protect from environmental threats and hazards shall be commensurate with the importance of the premises, data centres, sensitive designated areas**,** the criticality of the operations or ICT systems located there **and the impact of penetration or outage on customers**;

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.

Yes, but about the requirement that programs and training shall be conducted at least yearly, it could be a too high a frequency. We would ask for reconsideration

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.

Yes.

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.

N/A.

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.

We support many aspects of the criteria set out in Article 24(5). In particular, we welcome the inclusion of the non-availability of systems as a trigger given the potential for this to have customer/user impacts even if at that point the financial entity has not determined the cause. We propose one clarification and one addition to the criteria.

We agree it is appropriate for financial entities to consider all the factors listed. However, we think it is important to clarify that not all the factors need to be present in a particular situation before it is appropriate to launch the incident response processes. Any one of the factors, or combination of them, may be sufficient to warrant triggering the incident response. We therefore propose redrafting as follows:

5. Financial entities shall consider all the following criteria to trigger ICT-related incident detection and response processes **and shall trigger a response where warranted by any one or more of the criteria**:

We also think it is important to add a criterion relating to the notification to the financial entity by a relevant public authority of an ongoing incident which could affect it, which may or may not be specific to the financial sector. An example could include a widespread distributed denial of service attack, or a concerted exploitation of a known vulnerability in widely-used software. We have not attempted to draft this because the wording will need to mesh with other legislation and means for referring to such relevant public authorities, but we consider it important that on receipt of such an alert a financial entity would at least consider triggering its incident response.

Q24. Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

We generally support the provisions, subject to three important additional comments below.

We particularly welcome the explicit reference to locating the ICT business continuity management clearly within the overall business continuity management in Art 25(1)(a) so that the focus on ICT continuity management is given due prominence but not to the exclusion of other elements.

We also welcome the emphasis on testing of recovery plans in Articles 25(h), 26 and 27 as this is essential to ensuring that they are realistic and achievable when the need arises.

We think that explicit provision should be made in Article 25 for the business continuity policy to require consideration of ways to limit the harm to customers, users, market integrity and financial stability. It is important that where options are available about the response these factors inform decision-making and not solely matters such as cost or convenience for the financial entity. We suggest doing this through a new provision as follows:

(ea) criteria to guide decision-making during incident response and recovery, including reducing the impact on the financial entity's customers and users.

We think that consideration should be given to further specifying how appropriate recovery time and recovery point objectives should be determined for systems needed to provide customer access to current accounts (credit institutions) and payment accounts (PSPs) to retail clients. Given the widespread decline in the use of cash and increased reliance on electronic payments, without access to such accounts, customers may be unable to meet basic needs where such facilities are unavailable, particularly where the system outage is not pre-planned and pre-announced. Ideally, the recovery timeline would be within the same day. However, if this is not considered feasible at this stage, we consider that next-day recovery is essential and should be feasible. We also suggest that this is an important area for future supervisory focus and benchmarking.

Finally, we think it is important that ICT business continuity management takes account of how climate change may impact both the physical threats to digital operational resilience and potential recovery scenarios. We therefore suggest that a reference is added to considering any relevant national climate risk assessment or strategy when identifying potential threats to digital operational resilience and planning responses.

Q25. Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.

We agree that specific provisions are appropriate for these entities given the role they play in the wider market.

However, we also think Articles 25 and 26 should specifically reference the need for trading venues to prioritize ensuring that opening and closing auctions or other mechanism for determining opening or closing prices can operate, and that explicit provision is made for back-up arrangements to enable this to happen and for regular testing of fail-over procedures needed to maintain trading, including with the venue's users.

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.

It is important that the report and review demonstrably take account of lessons learned from previous incidents. This learning should consider both root cause analysis and also lessons learned on how the impact of incidents on the entity, its customers and markets could be reduced. We therefore propose adding a new point to Article 28(2)(l) as follows:

"v. lessons learned from incidents since the last review, including root cause analysis and analysis of how the impact of the incident on customers and markets could be reduced."

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.

Yes, broadly speaking we agree. However we think the JC should incorporate suitably tailored versions of our comments in relation to the 'non-simplified' regime here.

In particular, we think it is important that there should be a ceiling placed on the permitted time for recovery of systems critical to the provision of current accounts or payment accounts. This would ideally be the same as that provided under Article 25. However, if this is not considered to be feasible at present, a transitional period could apply during which a longer, specified recovery time would be acceptable.

We also cannot envisage what circumstances the "where applicable" in Art 39(1) is intended to capture and propose that this should be deleted.

It would also be helpful to clarify the extent to which the simplified ICT risk management framework is applicable to small entities that are part of a larger group.

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.

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.

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.