Contribution ID: b1024963-5d1c-4e97-9143-9c9160035bac
Date: 08/09/2023 21:53:38

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

Fields marked with * are mandatory.

Introduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the first batch of Consultation Papers on the mandates stemming from the Digital Operational Resilience Act (DORA) with the aim to collect market participants' feedback on the proposed draft regulatory technical standards (RTS) to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554.

Market participants are invited to provide their feedback to the draft technical standards by responding to the questions presented in this consultation paper. The feedback received will be taken into account in the finalisation of the draft technical standards, which are due to be submitted to the European Commission by 17 January 2024.

Comments are most helpful if they:

- respond to the questions stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence (including relevant data, where applicable) to support the views expressed;
- reflect a cross-sectoral (banking, insurance, markets and securities) approach, to the extent possible; and
- describe any alternative approaches the ESAs could consider.

To submit your comments, please click on the blue "Submit" button in the last part of the present survey. Please note that **comments submitted after 11 September 2023 or submitted via other means may not be processed.**

Please clearly express in the consultation form if you wish your comments to be disclosed or to be treated

as confidential. A confidential response may be requested from the ESAs in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request.

Any decision we make not to disclose the response is reviewable by the ESAs' Boards of Appeal and the European Ombudsman.

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the ESA websites.

General Information

* Name of the Reporting Stakeholder

Deutsche Börse Group

Legal Entity Identifier (if available)

529900G3SW56SHYNPR95

* Type of Reporting Organisation

- [ ] ICT Third-Party Service Provider
- [x] Financial entity
- [ ] Industry Association/Federation
- [ ] Consumer Protection Association
- [ ] Competent Authority
- [ ] Other

* Financial Sector

- [ ] Banking and payments
- [ ] Insurance
- [x] Markets and securities
- [ ] Other

* Jurisdiction of Establishment

Germany and Luxembourg

* Geographical Scope of Business

- (•) EU domestic
- ( ) EU cross-border
- ( ) Third-country
- ( ) Worldwide (EU + third-country)

Name of Point of Contact

Sujata Wirsching

* Email Address of Point of Contact

sujata.wirsching@deutsche-boerse.com

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.

Yes, within the framework of defining and implementing processes, methods, and stipulated requirements in the specific Articles, it is essential to integrate the principal of proportionality, despite uncertainties surrounding the delineation of thresholds.

Notably, the uniform application of the proportionality principle encounters challenges due to mandated obligations — such as the comprehensive testing of critical function ICT systems, broad implementation of data encryption measures, and the registration of details pertaining to all ICT services.

As a proposition, it is advisable to ensure a consistent application of the proportionality principle within DORA with clearly defined thresholds. In our view it is in general not clear what Article 29 defines in terms of proportionality.

Further, when considering which financial entities could become subject to more advanced testing, both the principles of proportionality and subsidiarity should be considered, as well as the need to ensure a level playing field. It would not be proportional to make all financial entities subject to the same levels of requirements without distinguishing between their levels of size, type, and criticality to EU markets. However, the size of a financial entity should not be the most relevant metric when determining what cybersecurity requirements ought to apply. Rather, entities should be subject to similar requirements, if they have similar risk profiles, including their systemic impact, and whether they conduct similar activities.

In general, we would caution against overly prescriptive technological measures which would rapidly be outdated due to technological evolution. While there is a need for a coordinated approach to cyber-resilience, when considering further regulatory requirements in this space it is important that flexible innovation is safeguarded since “one size does not fit all”. Hence a risk-based and proportionate approach is needed.

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 support the consideration of the proportionality principle and that a risk-oriented approach is essential to apply.

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.

We consider that qualitative and quantitative indicators are not always possible to establish and therefore propose to include “if possible, to measure the impact and likelihood of occurrence of these vulnerabilities and threats.”

In relation to the tasks of the control function under Article 2(f), the development of security awareness programs and digital operational resilience training should not necessarily sit with the Control Function but instead with “appropriately skilled personnel.” The control function should instead be tasked with the oversight and monitoring of security awareness programs.

The intention of Article 4 lacks clarity. It implies that the policy should distinguish between various types of ICT third-party service providers. Yet, it doesn't elaborate on the purpose of such differentiation. The proposed wording suggests a preference for certain ICT third-party service providers over others, a determination that falls outside the RTS scope. We hence recommend its removal.

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

The suggested approach on ICT risk management policy and procedures reflects ESA’s comprehensive effort to ensure the security and resilience of financial entities’ networks.

We agree with the suggested approach, however we suggest clarifying that the proposed requirements relate only to ICT systems which are critical and not all ICT systems.

Further, we believe that a slight adjustment could further enhance its precision and overall effectiveness. Specifically, we would like to emphasize the importance of closely monitoring “relevant” or “significant” aspects that may have a material impact on the overall ICT risk profile to ensure an effective and focused approach on the critical aspects for the financial industry as well as for the regulators. Including provisions on the monitoring of “any” changes as described in Article 3 (1)(e) would dilute the scope and focus.

Moreover, we suggest adding “monitoring that the aggregation of accepted risks is within the risk appetite of the financial entity, in Article 3(1)(d). Lastly, we consider Article 3(3) too broadly defined for implementation on the financial entity’s side in order to allow for a better understanding, we suggest defining specific guidelines on how to tailor and update the ICT risk management policies and procedures as well as risk assessment in case of material changes as stated in the proposal.

Art. 3 (also Art. 33) mentions risk tolerance levels, but it is not clear or defined if the expected risk tolerance is determined specifically for each of ICT risk or for all of them together. This requires clarification and reformulation of the phrase, as calculating the likelihood and impact of vulnerabilities and threats does not add value if it is done at the risk level. We suggest several changes to the policy and process laid out in Art.

3.
- Art. 3 (1)(d)(ii): The audit frequency should be risk-oriented and target aggregated risks.
- Art. 3 (1)(d)(iv): The wording should be adjusted, and "any" should be replaced by "relevant"

Further, any proposed security risk management framework should be based on already existing internationally developed standards.

Moreover, any requirement to disclose details on cyber resilience should be conducted in a careful manner to ensure sharing of such information does not unintentionally better equip potential attackers, thereby increasing cyber resilience-related risk.

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

The suggested approach on ICT asset management provided in Article 4 is overall in line with our view.

However, we consider that Article 4 of the proposed Draft RTS on ICT asset management policy requires further clarification. While welcoming the definition of 'ICT asset' in DORA Art. 3, we would appreciate receiving more detailed definitions of 'ICT' and 'information asset'. The provided definition of 'information asset' in DORA Article 3 is as follows: "'information asset' means a collection of information, either tangible or intangible, that is worth protecting".

In regard to the suggested approach on ICT asset management provided in Section III (i.e., Articles 4 and 5) is majorly in line with our view. However, we would like to point out that the scope of the proposed requirements seems to be majorly limited to "ICT assets". Information assets are only mentioned in Article 5 (2), which appears inconsistent with the requirements stipulated in DORA, covering both "information assets" and "ICT assets" (i.e., Article 8 of DORA). Consequently, we suggest explicitly including "information assets" in Section III provisions in order to ensure consistency and better reflect the initial requirement from DORA.

In addition, another consideration would be about the stipulation made in Article 4 paragraph 2 (b)(ix) which appears to be already covered in paragraph 2(b)(vi).

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 are equally important as they serve different purposes.

Monitoring both seems important: e.g. "end of support dates" is being considered important, as it would enable financial entities to plan the renewal/decommissioning of underlying assets accordingly. It additionally would lead financial entities to consider that there are assets with long procurement lead times or high costs.

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

While the suggested approach on encryption and cryptography considered in the draft RTS is mostly in line with our view, it could be further improved by recommending that lost, compromised, or damaged keys shall be replaced instead of relying on recovery, as proposed in Article 7 (3), as those keys are overly risky to be recovered.

Furthermore, there is a need for clarity in Article 7 (4), to further specify whether the register pertains to only certificates or encompasses keys as well. We believe that these refinements would strengthen the overall framework, ensuring a more robust and secure approach to encryption and cryptographic key management. Too detailed descriptions should be avoided, but rather left to the entities decision based on their risk analysis in such cases.

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.

We are of the opinion that Art. 10(2c) is excessively broad, in particular when it comes to the reference to “vulnerabilities”. We suggest providing a clearer definition of vulnerability, e.g. as any which would result in a critical third-party ICT service no longer being available to the customer and this impacting the customer.

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

With regard to the patch management procedures described in Article 10, we propose that the testing and deployment of software and hardware patches and updates should be conducted in an environment that does not entirely “replicate” but is instead “very close” to the production one, as some minor differences (e. g., fewer memory capacity) would not cause any disruptions on the testing process. The requirement as proposed would lead to increased complexity and limit flexibility.

Moreover, the synchronisation of clocks requirement, encompassed in the logging procedures proposed in Article 12, should be limited and tailored exclusively to ICT systems serving important and/or critical services. By adopting this focused approach, it could be ensured that critical operations receive precise focus and timestamping while optimizing resource allocation across the organization and thus ensuring financial stability.

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.

In addition, systems should be tested to confirm that sufficient capacity is available to meet performance requirements.

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.

The frequency of such testing should not be set by the supervisors within the Level 2 instruments, but rather be determined by each financial entity within their policies using a risk-based approach. There might be measures which detect on weekly basis, but this depends on the ICT assets. It should be determined by taking their classification, risk profile and the purpose of ICT assets, especially for larger organizations.

Given that the number of assets is high, running scans on “all assets” without proper consideration of the asset classification might impact financial entities by causing network slowdowns. Moreover, it would also lead to a significant number of false positives that would need to be analyzed by the operating teams.

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.

No additional measures specifically for cloud computing are proposed.

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

The suggested approach on network security, particularly the emphasis on network security management and the encryption of network connections to safeguard against intrusions and data misuse in Article 13, is deemed comprehensive. However, from a trading venue perspective, co-location services play a critical role in reducing latency and ensuring competitive operations. Technological development has allowed the establishment of low latency environments in global trading landscapes. Market participants are involved in those low latency environments, allowing markets to grow. The rule as proposed would lead to massive impact on latency and, thus, on trading characteristics which would put Europe at disadvantage compared to other trading landscapes globally (e.g., UK, USA). We suggest inserting another sentence which would emphasize on certain exemptions being possible with regards to communication within the same data center.

Q14: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No answer

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

An alignment with the EBA Guidelines on ICT Risk Security Risk Management (Section 3.6.1) would be welcomed.
Article 15 (g) as currently worded is too broad. We recommend amending the wording so it is clear that testing under an ICT project management policy relates only to any incoming/newly developed or acquired ICT assets.
On article 16:
o Security testing of software packages under article 16 (5) should extend only to an application unit, as opposed to each of the libraries, including OSS and third party proprietary software.
o There should be an exemption for user acceptance testing environments under article 16 (6): in relation to the requirement that “non-production environments shall only store anonymized, pseudonymized or randomized production data.”
o Article 16 (9) refers to source code and proprietary software provided by ICT third party services providers. This would not happen in practice as it often prohibited by the license agreement or could cut across proprietary interests. Also this is not possible to achieve, we strongly suggest the removal of testing and depend on the certification/reports provided by ICT third party service provider.

Further, we suggest removing Section VII on ICT risk and change management. We are indeed of the opinion that such provisions do not add any benefits to the current ICT risk and management practices.

Q16: Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.

No answer

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

We do not support the specific approach proposed for CCPs of the consultation paper and subsequent proposals. In our view, this approach presents complexities and creates undue uncertainty.

- ICT systems security is subject to intensive and extensive multilevel regulation, which includes EU and national regulations and international standards and guidelines;
- financial market infrastructures are already subject to extensive entity-specific risk- management provisions, including ICT requirements. This is mainly due to the fact that vertical entity-specific regulation takes a functional approach that looks at the overall operational risk to which a specific service is exposed.

Instead, it is worth to underline that DORA overcomes the functional approach with the aim to consolidate and upgrade ICT risk requirements to a single horizontal framework applicable across the entire financial sector alongside the operational risk requirements that have, up to this point, been addressed separately in various Union legal acts.

In this regard, we support the centralisation and primacy of DORA, with the consequent repeal of redundant /equivalent ICT risk management requirements set forth in Level 2 vertical specific regulations.

With this said, a proposal as that supported by ESAs in the consultation paper and which introduces a further specific provisions at L2 for CCPs results in contrast with the above mentioned objective of DORA Regulation, in particular for the horizontal approach across the financial sector for the ICT risk requirements. Indeed, the proposed approach for CCPs introduces a differentiation between the different financial entities with the consequence that the goal of consolidation remains only at the formal level and not at the substantial level. In this regard we notice that DORA L1 measure includes some specific requirements for CCPs, but this approach should not be replicated in L2.

In addition, the proposed approach increases uncertainty. Indeed, the consultation paper does not clarify how for example the coordination between DORA L2 and EMIR L2 will be carried out.
We are further concerned about the risk of redundancies and inconsistencies. We believe this uncertainty undermines one of the key objectives of the DORA L1 as stated under recital 102 and 103 i.e. the consolidation of the ICT risk management provisions across multiple regulations and directives applicable across the financial sector.

With regard to CSDs: we support the introduction of the specific obligations to CSDs under Articles 16 (2) & 17 DORA to the extent that they consolidate not only the sector-specific regulation of CSDs (CSDR), but also those laws and regulations applying to its interdependent financial entities. Doing so, will consolidate all CSD inter-dependent ICT-related requirements.

As for true for CCPs - also for CSDs - ICT systems' security is subject to extensive multilevel regulation, including EU and national regulations as well as international standards and guidelines. In addition, FMIs are already subject to successive and extensive entity-specific risk management provisions, including ICT requirements. Therefore, similar concerns as addressed above should be taken into consideration, i.e. the development of the draft RTSs should take into account a horizontal approach that reflects the degree of

interdependency of the financial ecosystem. The requirements should consolidate CSD inter-dependent entities subject to DORA.

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

We are of the opinion that, regarding, Art. 18(2)(d) further clarification is needed on what is meant by a “clear screen policy”.

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.

Failover tests for the mitigation of risk arising from physical damage to data centers could be taken into consideration and referenced from Article 11.

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

The requirement for training is considered too prescriptive with respect to content and frequency to be conducted “at least yearly”. We instead recommend the content and regularity of training is set by the organization based upon the position held, access to data and resources, with greater flexibility for financial entities in tailoring the training content. It seems too restrictive to sum up the necessary ingredients. This could not be the most important topics after a year or depending on the organization. There are other regulations that prescribes for instance malware and there are other topics depending on the audience for instance secure coding. It now seems very data (protection) oriented.

We recommend amending article 19 (1) to “Financial entities shall include in specific ICT security awareness programs and digital operational resilience training elements regarding the high-risk topics in your branch and organisation".

The suggested approach regarding ICT and information security awareness and training as outlined in Article 19, specifically paragraph 2, does not highlight the initial training requirements which must be established and are necessary for the implementation of DORA. The entities need also to consider appropriate training plans for technical teams responsible for the development, configuration, and maintenance of ICT assets, based on an assessment of required skills for their roles and responsibilities.

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.

With regards to the proposed approach on access control, we suggest including the terms “user reconciliation” and “user recertification” as part of Article 22(e)(iv).

Q22: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No answer

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.

In order to enhance clarity and ensure practical feasibility, we suggest removing third-party ICT infrastructure and network management from the scope of Article 24 and rather consider it exclusively under the ICT third-party services framework. Additionally, we encourage a clear definition and guidelines for the treatment of "ICT network performance issues" at the third-party infrastructure.

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.

The proposal put forward with regards to ICT business continuity management, including the specific considerations for CCPs, CSDs and trading venues, does not reflect nor align with the exchange perspective. Firstly, various concerns emerge regarding the feasibility of maintaining identical secondary processing sites with distinct geographical risk profiles. It should be taken in consideration that the Recovery Point Objective (RPO) in regard to data loss is required to be close to zero, which can hardly be achieved in the setup indicated in the proposal. Coping with the 'different geographical risk profile' requirement is therefore limited by the RPO.

In addition, to ensure orderly markets, order data is being purposely deleted. A fresh order book would allow the market to take new information into consideration and therefore add new trading interest into an order book rather than confronting market participants with the order book outdated information.

Lastly, with regards to the testing of the ICT business continuity plans outlined in Article 26, it is imperative to introduce a mitigating opening clause in order to prevent from any adverse repercussions on the trading venues' business and operational landscape. For orderly trading to take place on trading venues, it needs to be considered that technological developments allow low latency trading in which many market participants globally engage. The proposal put forward would severely impair the way trading is performed globally, as it would add massive latency.

Also for Q25
Similarly to the response to Q23, ambiguity arises with regards to the consideration of third-party services in the ICT response and recovery plans requirements of Article 27. We recommend the explicit de-scoping of such services in this article and consider it exclusively under the ICT third-party services framework.
In addition, we suggest not to extend the two-hour recovery time objective to "critical functions" as opposed to "critical IT systems" as currently recommended in Principle 17 of the PFMI as well as set out in Art. 17(6) of EMIR RTS 153/2013.

In addition, concerning Art. 26(6), we suggest specifying that the review of business continuity plans mandated on a yearly basis only apply to those business continuity plans related to critical functions.

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

We consider that a one-size-fits-all model for duration and recovery would not be suitable. Moreover, any regulatory measures in this space would need to be sufficiently broad to allow flexibility to new types of situations and issues, recommending specific and quantitative parameters should thus be avoided. It is very important that different approaches, in line with the different needs of exchanges, are allowed.

Exchanges avail of a number of mechanisms to safeguard trading and price discovery and their discretion should not be limited by overly prescriptive regulatory measures when it comes to the functional design, application and interplay of cyber-resilience measures. We consider that the RPO should be the point in time when the market operator is comfortable that it can ensure again a fair and orderly market. On a general basis, financial market infrastructure operates under a 2-hours RTO guidance, as per CPMI-IOSCO Principles of Financial Market Infrastructure. 2-hours RTO guidance works well under operational disaster recovery plans, but we consider that mandating RTO under specific legislation would be counterproductive. Furthermore, exchanges have in place outages standard protocols tailored to different markets. DORA should take this into consideration.

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.

In regard to the suggested approach on the format and content of the report on the ICT risk management framework review highlighted in Article 28, there is a need for clarity, particularly in paragraph 2 point a (iii). Article 6(5) of DORA entails that the "ICT risk management framework shall be documented and reviewed at least once a year," and reviewed by independent auditors. The proposed RTS stipulates a detailed report that appears to mirror the content of the framework, resulting in duplicated requirements. If a company has a stable framework (yearly reviewed and audited), a report on possible deltas should be considered sufficient.

This article is disproportionate, with the information sought creating overlap with the Register of Information.

We suggest reducing the content of the report on the ICT risk management framework review, especially for reviews that are triggered ad-hoc by major ICT-related incidents. In this case, we would rather favour following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes.

We also consider that there is no need for the ad-hoc reviews defined in Art. 28(2) if the trigger is a major ICT-related incident because:

- The impact of the incident and the root-cause analysis should determine the scope and details.
- There is no need to analyze all services provided, if only one service is impacted where there are no dependencies with other services provided.

Simplified ICT risk management framework

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.

No answer

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.

From a trading venue perspective, co-location setups play a critical role in reducing latency and ensuring competitive operations. As highlighted in Q13, technological developments have allowed the establishment of low latency environments in global trading landscapes. Market participants are involved in those low latency environments, allowing markets to grow. The rule as proposed would lead to massive impact on latency and, thus, on trading characteristics which would put Europe at disadvantage compared to other trading landscapes globally (e.g., UK, USA). Therefore, we would like to emphasize on the need for an introductory clause in Article 37 (1) and (2) explicitly considering these imperatives. By doing so, the implementation of security measures can be harmonized with the low latency imperative and future trading developments but also overall ICT risk impact while pursuing efficient financial activities.

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.

No answer

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.

No answer

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.

The suggested approach regarding ICT business continuity management under the simplified ICT risk management framework appears sufficiently substantiated and is therefore in line with our view.

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.

No answer

Submission of the responses

Contact

Contact Form