Insurance Europe response to the first batch of draft DORA Level 2 measures

Our reference:	EXCO-CS-23-087	Date:	08/09/2023
Related documents:	EIOPA Joint Consultation on the first batch of DORA policy products		
Contact person:	Personal & general insurance department	E-mail:	Zwagemakers@insuranceeurope.eu
Pages:	37	Transparency Register ID	33213703459-54

This document contains Insurance Europe's draft response to the four consultations on the European Supervisory Authorities (ESAs)' draft regulatory technical standards (RTS) and draft implementing technical standards (ITS) to complement the Digital Operational Resilience Act (DORA Level 2 measures):

- ANNEX I - Consultation paper on RTS on ICT risk management framework (Art.15) and RTS on simplified ICT risk management framework (Art.16)
- ANNEX II - Consultation paper on RTS on criteria for the classification of ICT-related incidents (Art.18.3)
- ANNEX III - Consultation paper on RTS to specify the policy on ICT services performed by ICT third-party providers (Art.28.10)
- ANNEX IV - Consultation paper on ITS to establish the templates for the register of information (Art.28.9)

Insurance Europe aisbl • rue Champ de Mars,23 B-1050 Brussels
Tel: +32 2 894 30 00 • E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

ANNEX I

1. Draft RTS on ICT risk management framework

Article 1. General elements of ICT security

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.*

While Insurance Europe appreciates the efforts of the ESAs in ensuring the draft RTS are proportionate and risk-based, the proposed approach falls short of achieving the objective. In particular:

- Article 29 on its own does not suffice to ensure proportionality; the principle should be enshrined throughout. The approach currently taken by the ESAs is too narrow, as Article 29 stipulates that only, "*elements of increased complexity or risk shall be taken into account*" when applying the proportionality principle.
    - As this implies that decreased complexity/lower risk should not be considered, Insurance Europe's strong recommendation would be to take a more comprehensive approach, for instance by including a reference to decreased complexity/lower risk in the final RTS or add wording along the lines of "*when relevant*".
    - "*Size*" and "*risk profile*" are not among the elements used to determine proportionality in Article 29, even though the two variables are key elements in Article 4 of Regulation (EU) 2022/2554.
- To ensure consistency between the L1 text and the RTS, Insurance Europe proposes making a reference in Article 29 to Article 4 of Regulation (EU) 2022/2254. Furthermore, Insurance Europe suggests that "*Chapter VI Proportionality principle*" should become the first chapter in the RTS, as this would more explicitly reflect that the RTS is built on the principle of proportionality and that the subsequent provisions should be interpreted with this principle in mind.
- Performing a risk assessment should, however, be compulsory for all entities, irrespective of their size. An entity should then be able to implement a control framework that is proportionate to the outcome of the assessment.
- Leaving the interpretation of risk and complexity of the different types of financial entities to the National Competent Authorities will result in increased uncertainty and, moreover, in a fragmented approach to DORA's implementation across Member States. In this regard, it is also important to point out that, to avoid conflicting policies within a group, the supervisor of the group, rather than the supervisor of individual entities, should be the designated competent authority.

Finally, some requirements may imply a significant cost impact on smaller entities, notably:

- The geographical segmentation requirements in Article 25 (2) c for small undertakings with just one company location.
- The requirement to map all network connections for all services (including, for example, meal plan).
- The requirements pertaining to all system changes (see responses in Q13 and Q15).

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.*

To ensure the proportionality principle is consistently applied, Insurance Europe proposes a more principle-based approach, for instance by integrating a discretionary leeway in all specifications. This would be especially helpful for requirements in relation to documentation, process, and system requirements, as well as with respect to strict deadlines and intervals.

In this regard, it should be emphasised that, unlike some other financial entities, insurers already have risk-based measures in place, in line with DORA L1, the Solvency II Directive, and the guidance issued by national supervisors. Therefore, while a more rule-based approach would be beneficial for some financial entities, a principles-based approach is more appropriate for the insurance industry.

2.4.1.1 Section I: Provisions on governance / Article 2. Provisions on governance

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

Article 15 of DORA does not mandate the ESAs to further specify requirements with reference to Article 6(4), which covers the assignment of responsibility for managing and overseeing risk to a control function. It is therefore yet to be confirmed whether the ESAs have a mandate to draft provisions on governance as proposed in Article 2 of the RTS on the responsibilities of the control function (as per Article 6(4) of DORA).

Should Article 2 of the RTS be maintained, the current wording conflicts with the "*three lines of defence model*", as well as with the Solvency II Directive (art 47). In order for the internal control functions to be regarded as independent, their staff do not perform any operational tasks that fall within the scope of the activities that the internal control functions are intended to monitor and control.

Therefore, Insurance Europe expresses caution against using wording that suggests a first line task. While it is acceptable to have a control function responsible for monitoring and reporting activities, verbs such as "*manage*" or "*develop*" should be avoided:

- "(b) ~~managing and~~ monitoring the financial entity's ICT risk"
- "(f) ~~developing and~~ monitoring the effective implementation of ICT security awareness"

In a similar vein, and in relation to Article 2 (1) c, Insurance Europe recommends for the specified task defining the ICT and information security objectives and setting the qualitative and quantitative measures of their attainment, key performance indicators and key risk metrics referred to in Article 6(8), point c of Regulation (EU) 2022/2554) to not be mandated to be performed by the control functions.

More broadly, Insurance Europe would welcome clarity as regards the responsibilities implied by the "*three lines of defence model*", notably:

- Could the ESAs clarify the duties associated with the first line responsible for "*managing, developing and monitoring*"?
- Could the ESAs clarify the duties associated with the second line responsible for "*managing, developing and monitoring*"?

2.4.1.2 Section II: ICT risk management / Article 3. ICT risk management

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

Yes.

However, in addition to the need for a clear definition of "*residual risk*" and "*residual IT risk*", the RTS should be more explicit about who is responsible for the residual risks.

Article 3 (a) should, moreover, clarify that the risk tolerance levels encompass both a quantitative and a qualitative aspect. Insurance Europe's recommendation would be to replace "*indication of the approved risk tolerance level*" with "*the approved risk tolerance levels*", making the provision more distinct.

2.4.1.3 Section III: ICT asset management / Article 4. ICT asset management policy & Article 5. ICT asset management procedure

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

Article 5 requires clarification. In particular, Article 5 (2) should reflect that the risk assessment should not influence or inform the criticality assessment. Rather, these are distinctive steps that should be taken in sequence. The article should therefore be reworded as follows:

Article 5
ICT asset management procedure
2. Such procedure shall detail the criteria to perform the criticality assessment of information assets and ICT assets supporting business functions. Following the criticality assessment, the ICT asset management procedure 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?*

Insurance Europe does not consider this important as such. While the end date of the provider's support is a useful piece of information, the extent to which it may be classified as important or critical would depend on the type of asset (e.g. network, server OS, database app, etc.). It should also be noted that the end date of the provider's support may not be known at the time of reporting and may also be subject to change (it could move forward or back). This information is therefore relative in terms of value.

2.4.1.4 Section IV: Encryption and cryptography /Article 6. Encryption and cryptographic controls

Q7. *Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.*

Article 6 (2) a (Encryption and cryptographic controls) states that if data in use cannot be encrypted it should be processed in a separated environment. Insurance Europe has several concerns about this proposed approach:

- On a network/platform level this is very costly to implement, as well as highly complicated based on currently available technologies. The benefits in terms of risk reduction are also questionable.
- Data in use always implies an unencrypted display for the end user. Insurance Europe therefore proposes requiring encryption of data on an individual basis and based on a risk assessment, classification, and cost/benefit analysis.
- It is unclear what "*separated and protected environment*" entails when encryption in use is not possible, notably because "*separated*" and "*protected environments*" are already described elsewhere.
- With regards to Article 6, encryption has no effect on "*availability*" and the terms "*availability*" should therefore be removed from Article 6 (1).
- Article 7 (Cryptographic key management) describes a register for all certificates and certificate storing devices. On the one hand, as every endpoint (e.g. PC/laptop) has several certificates stored, an ICT asset register would be redundant. On the other hand, creating and keeping an updated register for all certificates and certificate storing devices might result in extensive administrative work due to the wide use of certificates on servers, services, and endpoints, especially where the process cannot be fully automated. Insurance Europe therefore proposes to register a certificate with a data-field on which devices these certificates are stored.

Q8. *Is there any new measures 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

Section V: ICT operations security /Article 8. ICT operating policies and procedures.

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

Several elements of the suggested approach require additional clarification.

With regards to Article 8 (ICT operating policies and procedures):

- Article 8 2 (a) i: as it is unclear what is meant by "*secure*", the word "*secure*" should be either removed or clarified.
- Article 8 (2) ii: this requirement could result in extensive documentation for financial entities of all sizes, while the relevance to ICT operating procedures is not clear. Additional clarification would be helpful.
- Article 8 2 (a) iii: "*control of legacy ICT systems*" should be clarified, notably in terms of what should be achieved by financial entities through controlling legacy IT systems.
- Article 8 2 (b): "*Control…of ICT systems*'' should be clarified, notably in terms of what should be achieved by "*controlling*" ICT systems.
- Article 8 2 (b) ii: "*scheduling*" should be clarified, as it is not clear if this refers to batch jobs, scripts, or backups.
- Article 8 2 (b) iii: as the word "*protocols*" may be misleading, it could be replaced by "*requirements*". "*Requirements*" could subsequently be removed under iv and v.

As regards Article 10 (Vulnerability and patch management):

- Insurance Europe suggests integrating an "*emergency change process*", notably because in some cases related to high priority (security) patches, it may be relevant to prioritise the speed of installing over comprehensive testing in a separated environment.
- With regards to the requirement in Article 10 (2) c to handle *any* vulnerability, Insurance Europe proposes a more risk-based and proportionate approach. The requirement for ICT service providers to report any vulnerability to the financial entity is particularly unnecessary in cases where the vulnerability is handled by the ICT service provider on the basis vulnerability management procedures. Informing the financial entity would be relevant where a vulnerability is not handled by the ICT service provider and so would pose a high risk to the financial entity.
    - Insurance Europe suggests replacing "appropriate solutions;" with "possible updates or appropriate risk mitigating solutions;".
- The requirement in Article 10 (2) d to "*track the usage of third-party libraries, including open source, monitoring the version and possible updates*" is onerous and challenging, if at all possible, to fulfil. Insurance Europe would therefore suggest inserting wording to make the requirement more workable, for instance, "*if possible with reasonable effort*", or "t*o the extent possible*". Insurance Europe suggests removing the requirement in Article 10 (4) c to "*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*". This proposal is not in line with today's market reality, and financial entities cannot afford to implement the requirement for cloud applications.

Therefore, and because not all elements can be fully replicated, the recommendation would be to reword this paragraph as follows:

- "test and deploy software and hardware patch and updates in an environment *as similar or representative as possible, in terms of systems and patch levels, to the technologies deployed in production*, to avoid adverse consequences and disruption before their deployment to production environments".

- In relation to Article 10 2 (e), insurers fear that the disclosure of vulnerabilities may unnecessarily lead to a loss of confidence from the public towards the financial sector, especially as vulnerabilities are not always exploited. Moreover, disclosing vulnerabilities to the public would bring the weaknesses of the entity to the attention of hackers and increase the risk of malicious exploitation. This obligation should always be left to the discretion of the financial entity and should be limited to vulnerabilities that require action or a particular level of prudence from the client or the public.
- Article 10 2 (i) could be removed, as it pertains to elements already covered under items a through h.
- In order to clarify Article 10 4 (d), risk-driving aspects could be added, based on the following wording: "set deadlines for the installation of software and hardware patches and updates, based on the severity of the vulnerability, the current level of exploitation of the vulnerability, and the exposure of the ICT system". A new item e could subsequently add: "set escalation procedures in case the deadline cannot be met".

With regards to Article 11:

- Article 11 2 (a): "*the access restrictions*" should be clarified. In addition, the ESAs may consider merging Article 11 2 (e) and Article 11 2 (i), as the two articles cover data loss prevention requirements.
- Article 11 (2) k could be added to Article 19, as the provision relates to "*ICT and information security awareness and training*" and the provision should pertain to all computing resources, as opposed to only "cloud". It should read:

  - (k) for computing resources:
  - i. the requirement that the individual in charge of using the administrative interface to manage the computing resource shall have adequate competences and training in the management and security of the computing resource that are specific to the resource used;
  - ii. implement technical and organisational security measures on the credentials used to access the administrative interface to manage the computing resource.

Article 12:

- Article 12 2 (c) i, logging for physical access control, should be limited to the buildings of the entity that hold critical and important processing facilities.
- Article 12 2 (a) and Article 12 2 (d) may be merged, as both provisions cover requirements on the retention period of logs.
- Article 12 2 (c) i: the requirement to log events related to ''l*ogical and physical access control and identity management*'' is vague and should be clarified.
- Insurance Europe proposes removing Article 12 (2) (c) ii - iii, as capacity management and change management are not relevant in this context.

- The requirement in Article 12 (2) (c) v can become overly extensive because, as currently drafted, all connections (per user) would have to be logged. Therefore, Insurance Europe suggests a more risk-based approach, for instance by inserting wording to limit the scope, such as "*at least for ICT assets and information assets supporting critical or important functions*".
- The retention period, as per Article 12 (2) a, should be defined considering that the requirements relate to personal data and criminal investigations.
- Insurance Europe proposes a more risk-based and proportionate approach to the requirement in Article 12 (2) g. It is not feasible for financial entities to synchronise clocks between, for example, different cloud providers, SaaS services and multiple and geographically distributed data centres. It would therefore be important to establish that clocks need to be synchronised for ICT systems related to the same process.

Q10. *Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples*

No

Q11. *What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.*

Vulnerability scanning should be done based on the risk profile and risk appetite. Rather than imposing weekly scans which may be either insufficient or result in an unnecessarily large volume of activity (1000-100.000 devices for bigger undertakings), a risk-based approach would be more appropriate and workable. In line with this approach the organisation may, where deemed necessary, foresee additional ad-hoc scanning.

It should be noted that for a company with thousands of assets it is not feasible to scan all ICT systems within a week within reasonable costs and without impacting business processes.

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.*

Yes, Insurance Europe agrees with the requirements and does not foresee additional measures.

2.4.1.6 Section VI: Network security / Article 13. Network security management.

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

Generally, Insurance Europe proposes that Section VI on Network Security is revised in view of bringing the proposed requirements in line with existing (good) practices. For example, an increasing number of authorities and organisations (including ENISA) are abandoning network segregation-based architectures for security reasons, and instead resort to architectures rooted in zero-trust principles, which consider all networks to be non-secure. Such principles ensure access for trusted devices in a more dynamic and consistent manner. The requirements around separate administrative networks, encryption of traffic at network level, and limitations on internet access in particular are not entirely aligned with contemporary approaches to network security.

More specifically, clarification is required with regards to the combined application of article 11 (2) (k) (ii) and article 37 (2) (h). These two requirements are almost identical, apart from the addition of the word "*strong*" in article 37 (2) (h):

-Article 11.2 (k) (ii): "implement technical and organisational security measures on the credentials used to access the cloud client interface to manage the cloud computing resource."

- Article 37.2 (h) "*where relevant, the implementation of **strong** technical and organisational security measures on the credentials used to access the cloud client interface to manage the cloud computing resource."*

For the sake of clarity, the two requirements should (i) either be identical, (ii) or it should be specified when to apply each requirement and how to implement "*strong*" measures.

Moreover, with regards to article 11 (2) k, some controls will be very difficult for public cloud providers. In particular, cloud providers strongly limit the scope and frequency of pen tests in the contractual clauses. This should be reflected in the RTS.

The requirement in Article 13 (1) will be difficult and rather costly to implement for old apps and infrastructure.

With regards to Article 13 (1) b specifically ("*mapping and visual representation of all the financial entity' networks and data flows*"), it will be important to integrate wording to allow for a risk-based approach or to specify that the requirement pertains only to data flows supporting critical functions. As currently drafted, the requirement applies to all data flows, whereas it is not possible to visualise *all* data flows. Furthermore, Insurance Europe would welcome clarification of the objective expected to be achieved by "visualisation", as this would make it easier for financial entities to construct a visual representation that is fit for purpose.

It is not possible to implement the requirement in Article 13, (1) c for cloud applications ("*use of a separate and dedicated network for the administration of ICT assets and prohibition of direct internet access from and to devices or servers used for information system administration*").

Insurance Europe would welcome further clarity with regards to Article 13 (1) c, notably because it is not clear at what level networks should be dedicated. In this regard, it is key to consider the different set-ups needed for secure administration (e.g. a network device vs a server farm, vs an application on a server, vs a cloud application). Additionally, clarity would be helpful in terms of what is meant by "*direct internet access*", as limited

direct internet access to a specific service implies much less risk than, for example, internet wide indirect access via a proxy. Therefore, the focus of this article should rather be on the expected outcome for financial entities, which is currently not clearly established.

As Article 13 (1) c will be challenging to implement, it would be important to clarify the scope of ICT assets to be included. Insurance Europe recommends only critical and important ICT assets be in scope.

Article 13 (1) d would require implementing mandatory network access control for all entities, which would represent very large costs and efforts, especially for smaller companies. A more proportionate approach, for instance limiting the requirements to high-risk locations, would be appropriate.

Insurance Europe proposes excluding already encrypted traffic from the requirement in Article 13, (1) e. Communication can be encrypted both on the network and application level. Requiring a network level encryption for all communication is likely to result in double encryption on both layers, implying both a financial and latency burden.

Article 13 (1) g, as well as Article (1) m should be clarified as the requirement is not clear.

In relation to Article 13 (1) h, the proposed requirement to perform a review every six months would be very complex for bigger undertakings and would moreover require significant (financial) resources. The review should rather be done on an annual basis, similarly to the requirement in Article 13 (1) i.

Insurance Europe would welcome a clearer definition of "I*CT asset administration*".

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

2.4.1.7 Section VII: ICT project and change management /Article 15. ICT project management. Article 16. ICT systems acquisition, development, and maintenance & Article 17. ICT change management.

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

Insurance Europe proposes that Article 15 be removed given the absence of corresponding DORA Level 1 requirements. Technology is an increasingly inherent part of business projects, which means that this article could limit the options available to financial institutions because ICT project management is not only related to risk management, but also to business development.

Should Article 15 be maintained, the requirements in Article 15 should be revised because they refer largely to project management in the waterfall model. An explicit inclusion of agile software development would be

welcome. More broadly, it would be important to cater to non-project-based ICT-development methodologies and to avoid imposing a linear sequential design approach for ICT project management.

With regards to Article 16 (4), the reference to dynamic testing as part of source code review should be clarified. Dynamic testing is performed on a running system, rather than on the source code. It would therefore constitute a separate complementary activity to source code review and static testing of code.

Additionally, it would be important to clarify what is meant by "*non-production environment*" in Article 16 (6) and to specify the extent to which this requirement also applies to the backup of productive data.

Article 16 (9) would be impossible to comply with in cases when the third-party service provider is the owner of the source code, for instance if the software is licenced, or in case of Software as a Service (Saas). In such cases, the financial entity would not have access to the source code and should be allowed to rely on a report established by the third party, ensuring that the relevant tests and analysis have been conducted on the software. It would also be important to clarify if this provision is applicable to all source code/third-party software limited to software/code connected to critical or important functions.

As currently drafted, the requirement in Article 17 (2) "i*n respect of all changes to software, hardware, firmware components, systems or security parameters*" means that every change to a system parameter would have to be made via Change Management. As this is not in line with current practice, it would be important to take a more risk-based approach. Furthermore, while "*systems*" are specifically mentioned to be in scope of the ICT change management procedure, alongside software, hardware, and firmware, "*systems*" are in fact composed of software, hardware, and firmware. The reference to "*systems*'' may therefore be removed.

Article 17 (3) can be considered redundant in light of Article 16 (2) a and b, and could therefore be deleted.

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

No

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

N/A

2.4.1.7 Section VIII: Physical and environmental security / Article 18. Physical and environmental security.

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

While Insurance Europe recognises the importance of physical security, the provisions are rather broadly defined. Furthermore, the term "*environmental threats*" in Article 18 (2) a is very general and should be made more

concrete so that it is clear which protective measures are envisaged and required. For example, does this term include threats resulting from the specific geographic location of the facility (high-risk flood/earthquake area) or more general weather-related threats (heavy rain, storms)?

More generally, the requirements are not proportionate for smaller undertakings.

Finally, "*information processing facilities*" in Article 19 (2) d should be clarified given the absence of corresponding DORA Level 1 requirements.

Q19. *Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.*

No.

2.4.1.9 Section IX: ICT and information security awareness and training /Article 19. ICT and information security awareness and training.

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

It is highly desirable to continue to adhere to market standards in relation to information security. In this regard, the draft measures refer merely to ISO27000. Adhering to (a) market standard(s) would stimulate better recognition of standards across the industry and beyond. As regards outsourcing, it is important to note that financial institutions outsource some of their ICT activities.

With regards to Article 19 (2), the concept of "*training*" should be clarified. Security training generally involves an organised course programme and lessons, designed to teach employees or individuals specific security practices. It is typically a more structured and formal approach, educating individuals about cyber security risks, including prevention and mitigation. As such, these trainings are designed to be conducted only once. Security awareness, on the other hand, pertains to efforts to improve the general understanding of security risks. Such initiatives are about promoting a culture of security, where individuals are encouraged to be vigilant and aware of the potential threats at a given time. As such, awareness refers to a consciousnesses and posture, as well as personal responsibility. In summary, while security training is typically used to teach specific skills or to reinforce security protocols, security awareness is about creating a security culture that is supported by everyone in the entity. Conducting yearly training would create unnecessary burden and costs, without having clear benefits.

2.4.2 Chapter II: Human resources policy and access control/Article 20. Human resources policy & Article 21. Identity management & Article 22. 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.*

Article 20 (1) b i goes beyond the scope of DORA Level 1:

- Article 15 (b) DORA mandates the ESAs to further develop the components of the controls of access management rights (Article 9 (4) c, and associated Human Resources policy specifying access rights, procedures for granting/removing rights, and monitoring anomalous behaviour).
- However, Article 20 (1) b i in the RTS implies requirements to "*be informed of and adhere to the financial entity's ICT security policies, procedures and protocols*", exceeding the scope of Level 1.
- Additionally, the section on Human Resources in the Level 1 text does not imply a relation to this Level 2 RTS.

Additionally, as service providers typically cater to a wide range of customers with inevitably conflicting policies, procedures and protocols, it is unfeasible for service providers to not only inform all their staff of every financial entity's ICT security policies, procedures and protocols, but also to ensure they are allowed adhered to (e.g. in light of likely conflicting policies).

Insurance Europe therefore proposes rewording this article to:
20 (1) a identification and assignment of any specific **access management** responsibilities;
20 (1) b requirements for staff to:
i. be informed about, and adhere to, the financial entity's **access management** policies, procedures and protocols;
(…)

20 (1) c requirements for ICT third-party service providers, and their staff, to:
i. align the ICT third-party's ICT security policies, procedures and protocols with the financial entity's ICT security policies, procedures and protocols;
ii. be informed about, and adhere to, the ICT third-party entity's access management policies, procedures and protocols;
iii. be aware of the reporting channels put in place by the service provider for the purpose of detection of anomalous access activities, including those established according to Directive (EU) 2019/1937:
iv. upon termination of employment, requirements for the staff to return to the service provider all ICT assets and information assets that belong to the service provider or financial entity.

In relation to Article 21 (3) a, it must be noted that a unique identity can be linked to more than one user account. For instance, an administrator would have an account for office uses (e.g. internet, e-mail, O365, etc.), in addition to another specific account for systems administration purposes. The following wording is therefore recommended: "*each user account shall be linked to a unique identity assigned to each staff member*".

Furthermore, Article 21 (3) a raises questions about the extent to which third-party providers should be considered as using corporate equipment/network and/or as being physically present in the corporate environment.

The RTS would also benefit from a clear definition of the term "*generic accounts*".

The requirement in Article 22 (1) e) iv ("*review of access rights...at least every six months for ICT systems supporting critical or important functions*") is challenging to implement and places a disproportionate burden on organisations. A review on a twelve-month basis would be more workable. Additionally, it would also be important to be clear about the extent to which "*critical ICT systems*" should be interpreted as ICT systems that are supporting critical or important functions.

Furthermore, it will be important to clarify what exactly is meant by "*review of access rights shall be performed also whenever a change is necessary at user level*". Insurance Europe understands that this provision is limited to central counterparties, as per Regulation (EU) No 648/2012.

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.

2.4.3 Chapter III: ICT-related incident detection and response /Article 23. ICT-related incident management policy & Article 24. Anomalous activities detection and criteria for ICT-related incidents 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.*

As the requirements around ICT response and recovery plans are specified in Article 27, Article 23 (1) f could be removed.

Insurance Europe would welcome clarification with regards to:

- ICT incident reporting requirements (level of data, and when to report);
- The seven criteria required to classify incidents accurately, especially secondary criteria, which are very subjective and which means there is a risk that each firm will establish their own thresholds, leading to deviations among firms;
- The elements outlined in Article 24 (2) a) ("*collect and analyse all the following information on: i. internal and external factors, including business and ICT administrative functions; ii. potential internal and external threats, including usual scenarios of detection used by threat actors and scenarios based on threat intelligence activity*")
    - It would be important to clarify if the meaning of "*usual scenarios of detection used by threat actors and scenarios based on threat intelligence activity*" relates to well-known attack scenarios and newly discovered attack scenarios.

2.4.4 Chapter IV: ICT business continuity management /Article 25. Components of the ICT business continuity policy/Article 26. Testing of the ICT business continuity plans / Article 27. ICT response and recovery plans

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

Overall, Insurance Europe would appreciate clarification about how the proposed "*ICT business continuity management*" framework is meant to exist alongside or embedded within existing resiliency frameworks that already plan for business continuity, disaster recovery and incident management.

As currently written, it is unclear whether new ICT-focused Business Continuity Plans and Response & Recovery Plans are to be created and developed, in addition to and distinct from current industry best practices of developing process-focused BCPs and application-focused DRPs. If so, Insurance Europe would disagree with the suggested approach because all critical processes are already captured through existing processes; the associated resources (applications, facilities, staff, dependent processes, etc.) are documented within BIAs and recovery plans, and tested as per the company's policies and standards.

While we understand that there may be more granular specifics of the ICT business continuity framework that firms will need to mitigate and solve, creating another layer and type of plan (if that is the intended goal) would imply a duplication of current efforts, and may not provide additional value to the business. It would not significantly increase the recoverability of the company's processes and IT assets.

More specifically:

- With regards to Article 25 (2) a, the proposed two-hour timeframe is not risk adequate. The timeframe should be longer.
- The geographic requirements in Article. 25 (2) c) ii-iv are expected to have a significant impact on smaller undertakings, having sites only in one location. Insurance Europe proposes a more proportionate approach. It would also be necessary to clarify "*geographical risk profile which is distinct from that of the primary site*", as the requirement implies expensive investments.
- In Article 25 (2) c) iii, the word "*immediate*" should be deleted from "*immediate access to a secondary business site*". Indeed, is impossible for a secondary business site to be accessed immediately: even if all the technical means can be used (building, offices, network, workstations...), activating the site and sending staff requires (minimal) time.
- With regards to testing ICT business continuity plans as per Article 26 (2) a, it would be important to clarify that the scenarios considered for the development of the plans are tested over time and based on a risk-based approach, rather than for these plans to become an integral part of any testing effort. This will ensure a risk-based approach, keep costs in check and ensure the feasibility of the effort.
- With regards to Article 26 2 c and considering the proportionality approach, it will be important to clarify when it is required to run the production applications from a secondary location (e.g. "*(c) include the successful switchover … to the disaster recovery environment and … run in this way for a sufficiently representative period of time …"*). For example, would this be the case only for essential services when a service has a Recovery Time Objective (RTO) of less than 24 hours? For the sake of consistency and legal certainty, it will be helpful to establish whether the reference to "*critical business functions*" in this article should be understood as "*critical or important functions*".

- Furthermore, this provision goes beyond what has been required so far. Insurance Europe would therefore propose simplifying the requirements (i.e. which requirements should only apply to critical and important functions). The same can be said for Article 27 (2) and (4).
- With regards to Article 27 (2), considering the focus of DORA is on ICT, the disaster recovery scenarios should be clarified to ensure they relate to ICT only, notably to avoid any overlapping with Business Continuity. Currently, there is reference to non-ICT scenarios, which would normally be covered outside "*ICT response and recovery plans*".
- The recommendation would be to determine the necessary number and selection of scenarios on an enterprise-specific basis. Additionally, the scenarios should be identified/developed within the context of the Business Impact Assessment, rather than as part of the business continuity plans.
- With regards to testing IT continuity plans, more attention should be paid to the advancement of cloud and technologies used for continuity. Testing IT continuity within the cloud requires a different approach than the approach taken in conventional data centres.
- The detailed specifications imply that the report can only be prepared with significant effort. The requirements should be simplified. It would also be important to clarify whether the report should be produced by the first line of defence, or by the control functions.

Q25. *Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.*

It will be important to clarify that small entities that are part of a group can benefit from the simplified regime, even if the group itself does not meet the conditions.

Further elements of systems, protocols, and tools to minimise the impact of ICT risk

Q26. *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.*

In relation to Article 28 2 (a) ii, it would be welcome to have clarification on the purpose of the required report on the ICT risk management framework review.

With regards to Article 28 2 (h) v, "*major and immediate deficiency*" should be clarified to understand how reporting requirements around major and immediate deficiencies differ from those in relation to major ICT incidents.

As there can be other than log-based measures to detect anomalies, Article 36 (g) ("i*dentify and implement measures to monitor and analyse logs to detect anomalies for critical or important ICT operations*") should be phrased setting the objectives rather than in terms of methodology. The article should therefore be reworded as follows: "i*dentify and implement measures to detect anomalies for critical or important ICT operations*".

Q27. *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.*

Expanding the ICT operation security for all ICT assets would constitute significant additional building and running costs, which would be disproportionate for entities of all sizes. This has limited impact in terms of an entity's risk profile. A longer implementation planning period of no less than two years will be required.

ICT business continuity management

Q28. *Are there any additional measures or control that should be considered specifically for cloud resources in the draft RTS, beyond those already identified in Article 37(2)(h) of the proposed draft RTS? If yes, please explain and provide examples.*

N/A

Q29. *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

Q30. *Do you agree with the suggested approach regarding the article on Format and content of the report on the simplified ICT risk management review? If not, please explain and provide alternative suggestion as necessary.*

N/A

Other comments not clearly referable to any of the questions on Draft RTS ICT Risk Management:

In the RTS "*CP - Draft RTSs ICT risk management tools methods processes and policies*" there is an insufficient focus on specific and commonly used methods, such as Agile and Dev(sec)Ops.

Financial entities are required to establish procedures to assess compliance with the specific requirement in Article 14 (1) a (on securing information in transit). As assessing compliance can be considered important for all relevant RTS, clarification would be welcome as to why the ESAs have proposed specific compliance requirements for Article 14 (1) a, and not for any other requirements.

Article 15 (ICT Project management) and Article 16 (ICT systems acquisition, development, and maintenance) describe a waterfall model approach, but the methods typically adopted in such an approach are not so regularly used (as opposed to Agile and Dev(sec)Ops).

ANNEX II

2. DRAFT RTS on classification of ICT incidents

Q1.	*Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest.*

First and foremost, to ensure compliance with the RTS, financial entities need to be able to determine what parts of their business operations are relevant in terms of "I*CT related incident classification*". The draft RTS refer to "*the service*", "*critical services affected*", "*critical functions*", "*non-critical services*", and "*critical or important functions*" and the inconsistent and interchangeable use of these terms is expected to result in legal uncertainty for financial entities. To ensure clarity and certainty, Insurance Europe proposes sticking to "*critical or important functions*", as clearly defined in the Level 1 text throughout the RTS.

Generally, there is a risk that by classifying cyber incidents as ICT incidents, cyber elements are not sufficiently considered. Not all cyber threats can be classified as ICT incidents. Some ICT incidents are caused by cyber, but not all of them. Furthermore, the approach taken appears rather rigid and lacks proportionality in the sense that it does not reflect that some incidents may commonly be perceived as minor incidents, while the model would classify such incidents as "major" (or the other way around). This means that the model may not be usable. For the model to be efficient, it should be possible to reflect that what constitutes a "*major incident*" may differ across member states and sectors.

The overall approach (criteria and suggested thresholds) itself is demanding in the sense that it requires the gathering of a wealth of information collected from different sources within the entity, the media, and even from several member states. It is therefore important to stress that when a major incident occurs, the resources of the entity should be mainly focused on resolving the incident, rather than looking for the necessary information.

Consequently, an entity would need at least 72 hours to conduct the required assessment of the significance of the incident, which would take place in parallel to managing the incident itself. These efforts would benefit from a very simple template for the initial incident report, as well as the necessarily level of flexibility, so as not to overburden the IT teams in the wake of an incident.

Finally, while we agree with the general principle of having well-defined criteria to classify an incident as "*major*", as well as with having higher standards for communication and reporting for major incidents, the 2-level decision tree with 3 primary criteria and 4 secondary criteria is very complex. An example of a simpler model (e.g., a 1-level decision tree), could be as follows:

- 4 criteria (affected clients, financial counterparts and transactions; duration and service downtime; geographical spread; data losses);
- an incident is "major" if at least 2 of those 4 are met.

Such a model would capture most of the incidents covered by the proposed model, but with a considerably lower burden on financial entities and competent authorities.

Q2. *Do you agree with the specification and materiality thresholds of the criterion 'Clients, financial counterparts and transactions affected', as proposed in Articles 1 and 9 of the draft RTS? If not, please provide your reasoning and suggested changes.*

Insurance Europe believes the value should be more proportionate to the size of the undertaking. The proposed thresholds are too low for larger undertakings (the 10% materiality threshold of clients affected should be raised to 20% or 25%) and may result in overreporting without any benefits in terms of resilience. At the same time, the thresholds are significant for smaller undertakings.

Thresholds should be set based on percentages, rather than in absolute terms.

It would be important to specify at which level the thresholds should be applied: group or entity level (entity-level is recommended).

It should be noted that the definition of "*relevant*" client or financial counterpart is subjective. Insurance Europe will consider that the ESAs have done this on purpose, leaving each company to decide how to define "*relevant*".

Q3. *Do you agree with the specification and thresholds of the criteria 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact', as proposed in Articles 2, 3, 4, 7, 10, 11, 12 and 15 of the draft RTS? If not, please provide your reasoning and suggested changes.*

Overall, Insurance Europe proposes a more proportionate approach with regards to the thresholds to establish economic impact and remove any absolute thresholds (Article 15). If a threshold is established at EUR 100.000, most incidents will meet this threshold, especially larger entities which are more inclined to avail of (external) forensic support services than smaller entities. An EUR 100.000 threshold may reduce their incentive to allocate resources to incident root cause analysis.

Analysing the number of customers lost following an incident will not reveal anything substantial. Historic cyber incidents have not resulted in any loss of revenue or impact in terms of customer retention. Rather, the sector has observed a reduction in available cash or earnings before interest and taxes. There are a very wide range of factors that may, on a day-to-day basis, impact revenue, meaning that it is difficult to assess the extent to which revenue loss is related to an incident. Establishing a direct link would require significant involvement from the finance team.

Insurance Europe would therefore propose that each entity defines the relevant applicable threshold in relation to economic impact, based on its size and overall risk profile, as well as on the nature, scale and complexity of its services, activities, and operations. Taking this approach, the entity could explain the rationale behind the determination of the threshold in a dedicated policy.

Insurance Europe would also propose establishing a definition of "*resolved incident*". While some financial entities may not consider an incident resolved until the root cause has been determined and permanent mitigating

measures have been put in place (in line with existing practices and processes around incident and problem management), which could take weeks or even months, other financial entities may consider an incident resolved once normal operations have resumed.

The two-hour threshold for duration and service downtime (Article 11) is too low and not relevant for insurance operations, which are not time sensitive on a two-hour basis. For example, if a claims management system were down for two days, there would be very little impact on customers as payments of claims can occur days or weeks after the claims. This threshold would lead to unnecessary operational costs for financial entities and for the regulator. The appropriate duration should be set by the individual financial entity and in accordance with its business impact analysis or its service level agreement. It should be in line with its size and overall risk profile, including the nature, scale and complexity of its services, activities and operations.

Furthermore, in relation to reputational impact, the wording of rationale behind Article 2 (b) is unclear and implies overregulation. Moreover, the number of complaints would potentially meet this criterion very easily. We would suggest that the term reputational impact is more clearly defined as it is ambiguous. Reputational impact may not be immediate, and it may not be possible to judge the impact immediately after the incidents. In addition, when reputational impact is high, it may trigger other criteria such as ''*Data losses*'' or ''C*lient, financial counterparts and transactions affected*''.

The reporting times should be aligned with the GDPR to streamline processes and reduce administrative overhead.

Finally, Insurance Europe would welcome additional clarification on the approach financial entities should take in assessing whether a third-party service provider in another member state "*may be common with other financial entities*". In its current form, the draft RTS may end up resulting in arbitrary practices, relying on the assumptions a financial entity makes about third-party providers in other member states and the potential impact of an incident.

Q4. *Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? If not, please provide your reasoning and suggested changes.*

It is important to define "*data loss*". There are different interpretations when looking at Intellectual Property, privacy, and business. For example, Windows System files can be understood as "*data*". However, loss of Windows System files in the wake of an attack could result in no loss of business. Guidance in relation to the interplay between the GDPR (Article 33 and 34) and "*data losses*" in the DORA would also be important.

In addition, Insurance Europe would welcome a clearer definition of "*significant*" in the context of article 13, which introduces "*significant impact*" as a criterion.

Q5. *Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? If not, please provide your reasoning and suggested changes.*

In principle yes. However, in line with the Level 1 text, the criticality of the services affected should be a prerequisite for an incident to be considered major. This means that, if "*critical services*" is a different notion than "*network and information systems that support critical or important functions*", it should be defined for the sake of clarity and consistency.

For this criterion to be workable, the threshold should be linked to the mobilisation of a crisis unit within the entity which is, in practice, the response to a major incident.

Furthermore, "*Authorisation*" should not constitute a criterion to define criticality. Rather, Business Impact Analysis would be considered more appropriate.

Q6. *Do you agree with capturing recurring incidents with same apparent root cause, similar nature, and impact, that in aggregate meet the classification criteria and thresholds as major incidents under DORA, as proposed in Article 16? If not, please provide your reasoning and suggested changes. Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on data from the previous two years (you may also indicate the number of these recurring incidents)*

Yes.

However, companies will need a standardised way in ITIL (Information Technology Infrastructure Library) to do so. Today, companies do not have local systems that can track recurring incidents, and this means that the assessment/reporting will put undue (financial) burden on entities.

Furthermore, it will be important to clarify what is understood by "*recurring*", firstly because the notion of "*recurring incident*" does not feature in the DORA Level 1 text (Article 18 (1)), and secondly because the current definition is likely to capture relatively minor incidents, which means that the assessment and reporting would add disproportionate cost for entities. Clarification is key considering, for example, the following scenario: over a period of three months a company is confronted with two cases of employees receiving "fake" WhatsApp messages by attackers, impersonating as the employee's line manager or senior management. Will these incidents be considered recurring incidents? If so, will authorities and entities alike be able to manage the flood of information/reporting resulting from these incidents?

While several repeated small incidents can be considered equal to a major incident in terms of severity (it will be important to be clear about the threshold and to establish a mechanism to identify and track the incidents to assess the threshold), a threshold of twice in three months can be considered too low. Major incidents with complex root causes may require several weeks to fully remediate and a threshold of three times in three months would be more appropriate.

Q7. *Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes.*

The rationale behind Article 17 is unclear and the wording leaves too much room for interpretation. Overall, Insurance Europe fears that Article 17 (paragraph a and b in particular) will force financial entities to make guesses about another firm's risk exposure and cyber threat measures.

For instance, it is not clear how "*high probability*" should be defined. Companies today are faced with cyber threats that could impact critical systems on a constant basis. They track "*cyber incidents*", but they do not track "*cyber threats*", as such, as this is not mandated by any regulation/guideline/standard.

While large companies could rely on third party services to provide information on threats (Mandiant, for example), this would be a more costly exercise for smaller companies.

Q8. *Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19? If not, please provide your reasoning and suggested changes.*

This proposed approach raises several key questions, notably regarding the rationale behind it:

- Is it the intention of the ESAs to harmonise existing rules? As per existing national rules, incidents affecting clients in various EU Member States need to be reported to all National Competent Authorities.
- What if a major incident impacts a non-Member State?
- Could this approach end up serving as a "honey jar" for hackers and state-sponsored attacks?

Finally, with regards to the addition of "*without any anonymisation*" in Article 19, re/insurers are concerned about reports/information on an incident becoming publicly available. As this would potentially expose a financial entity to reputational damage, Insurance Europe recommends allowing anonymisation of the financial entity in the report.

ANNEX III

3. DRAFT RTS ICT services performed by ICT third-party

Q1. *Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?*

Overall, Insurance Europe would welcome a more proportionate approach. Furthermore, clarification would be welcome in a number of areas:

- The application of DORA: the draft RTS indicates that a company must be consistent in its approach. Consequently, it will be important to get certainty with regards to the extent to which the DORA is to be adopted globally, i.e., whether the RTS apply to all ICT TPPs globally.
- In Article 1 (1), it is unclear what "*location of the ICT third party provider*" means (legally or operationally).
- In Article 1(1), it is unclear what "*elements of increased complexity or risk*" means (operationally, legally, etc.).
- It is not clear which criteria "*increased complexity or risk*" will be assessed. Based on the current wording, it appears as though a "*decreased*" complexity/lower risk cannot be taken into account in applying the proportionality principle. Insurance Europe recommends including a reference to "*decreased complexity/lower risk*" in the final RTS to ensure a more comprehensive application of the proportionality principle. This could, for instance, be done by adding "*when relevant*" to any proposed requirement.
- In Article 1(1), it is unclear what "*the nature of data shared with the ICT third-party service providers, the location of data processing and storage*" means (personal data, non-personal data or both).
- Auditing of ICT TPP: the policy is required to include the details of the auditing of ICT TPP and this would need to be aligned with the first, second, and third line of defence. It is unclear whether DORA requires internal audit involvement in the auditing of ICT TPPs.
- Clarity is needed with regards to the policy review process.
- It is unclear whether the requirement is to separate policy per entity/location, or if a group-wide policy will suffice, provided it entails requirements prescribed by DORA.

Article 1 does not contain a clear reference to Article 4 of Regulation (EU) 2022/2554. For clarification purposes, Insurance Europe proposes inserting a specific reference to the proportionality principle to clarify that the policy should be designed with the proportionality principle in mind. Furthermore, additional details on how the principle of proportionality may affect the design of the policy would be helpful.

Moreover, Insurance Europe proposes including a reference to the general principles of managing ICT third-party risk, outlined in Article 28, (1) (b) of Regulation (EU) 2022/2554. More specifically, the proposal would add the following paragraph to Article 1 of the RTS:

"2. The policy shall be based on the general principles for managing ICT third-party risk outlined in Article 28, (1) (b) of Regulation (EU) 2022/2554".

In addition, it will be important to ensure consistency with the Level 1 text with regards to the following recitals:

- Recital 7: the review of the policy should be "*regularly*", instead of "*once per year*". This is important, as it paves the way for a risk-based and proportionate application.
- Recital 11: "*a written agreement*" should be replaced by "*one written agreement*".

With regards to article 2, while it makes sense that the policy applies on a sub-consolidated/consolidated basis, the parent undertaking should not be responsible for local implementation of the policy. Local CEO/Head of Group functions are responsible for local implementation and for reporting to the parent undertaking to ensure sufficient oversight. It will be important to elaborate how the objectives of Article are 2 are to be achieved (notably in terms of group application).

Q2. *Is article 3 regarding the governance arrangements appropriate and sufficiently clear?*

While Article 3 is generally appropriate, some elements require clarification or need to be slightly modified:

- Paragraph 1: seems to require that the parent undertaking be responsible for the local implementation of the policy (see the answer to Q1).
- Paragraph 2: a "*regular*" review rather than a yearly review should be sufficient and would also allow for a risk-based approach.
- Paragraph 3: it will be helpful to explain and clarify which methodology should be used for determining which ICT services support critical or important functions.
- Paragraph 6: "*monitoring the relevant contractual arrangements*" should be replaced with "*overseeing and strategically monitoring the contractual arrangements''.*
- Paragraph 7: Insurance Europe would welcome clarification about what should be understood by "*consistent with*".
- Paragraph 8: it will be helpful to clarify that an "*independent review*" can be performed by internal audits. Furthermore, as paragraph 8 requires that the in-scope ICT services provided by ICT third- party service providers be included in the financial entities' audit plan, it would be helpful to get clarity about whether a financial entity when executing an audit plan, should perform audits on the ICT third-party service provider on behalf of the financial entity's management or, rather, whether the audit should assess the financial entity's oversight and risk management over the ICT third-party service provider (or both).

Q3. *Is article 4 appropriate and sufficiently clear?*

The rationale behind Article 4 (a) is unclear. It is not clear why entities should "*differentiate*" between service providers registered in a member state and those registered in a third country. This should be clarified as well as what "*differentiate*" concretely means (does it mean that different requirements need to be specified for these service providers / services?).

Furthermore, the requirement implies a detailed mapping and analysis of all ICT (critical and non-critical) services through a company's service entities, via intra-group service agreements to ultimate group entities receiving services. As this also implies the need for tooling, as well as for tracking/documenting all approvals, management, controls and tracking for critical/important ICT external and intra-group services, this will be a costly requirement for companies.

Q4. *Is article 5 appropriate and sufficiently clear?*

Insurance Europe would welcome clarity on "*involvement of business units*" in Article 5 (1) f, and with regards to the responsibilities that the ESAs foresee placing on business units in financial entities.

Clarity would also be welcome on the term "*internal controls*" in the same paragraph because it is not clear whether reference is being made to a specific function in the second line or first line of defence.

With regards to Article 5 (1), clarification on what "*each main phase of the lifecycle of the use of such ICT services location of the ICT third party provider*" means (what phases are distinguished) would be welcome.

Q5. *Are articles 6 and 7 appropriate and sufficiently clear?*

Article 6 is not appropriate in the sense that risks need to be assessed locally. As currently drafted, Article 6 implies risk assessment at financial entity level or at consolidated/sub-consolidated level for every ICT outsourcing. Assessment at financial entity level makes sense for concentration risk only. For resilience purposes, third-party risks must be assessed globally and locally, linked together with an overall risk framework as set by second line of defence.
With regards to Article 6 (2) and conducting risk assessments, Insurance Europe would welcome more detailed guidance on how to apply these assessments. It is currently unclear how this provision is to be applied in cases where one group entity purchases services that are then used by the rest of the group.

With regards ton Article 7, it will be important to avoid overlaps with other pieces of legislation. For instance, Article 7 (1) e mentions Environmental, Social, and Corporate governance (ESG) and human rights principles. These principles are already covered in other (ESG) legislation and have no bearing on digital operational resilience.

Also with regards to Article 7, it will be important for the provisions to be more specific about the responsibilities of financial entities. It is, for instance, not clear which elements should be considered for the due diligence process.

Separate or substantially enhanced Due Diligence (if necessary) and implementation of intra-group Due Diligence would require aggregation of ICT TPP data at group level. This implies increased workload and, consequently, requires funding for additional resources.

In relation to Article 7 (1) a ("*appropriate organisational structure, including risk management and internal controls…*"), it should be noted that risk management and internal controls are not organisational units in a financial entity, but rather risk management concepts. It will therefore be important to be more precise about exactly what functions are in scope (for example using wording like "*the risk management function in the first line of defence*").

Furthermore, Article 7 (1) a (ICT third-party service providers in scope should "*have an effective and sound digital operational resilience framework*") requires clarification in terms of what is meant by ''*effective*" so that financial entities can determine what actions to integrate in their due diligence procedures. In addition, it will be important to ensure consistency with Article 7 (2), requiring that the policy shall "*specify the required level of assurance concerning the effectiveness of ICT third-party service providers' risk management framework for the ICT services to be provided by ICT third-party providers to support critical or important functions*" Insurance Europe proposes removing the parts from this paragraph that require "*effective and sound digital operational resilience framework*".

Furthermore, Article 7 is not sufficiently clear with regards to the extent to which Due Diligence applies to sub-contractors of ICT TPPs. Iit should be emphasised that imposing any obligation on companies to request System and Organization Controls (SOC) reports will further increase costs. While useful tools, SOC reports are already very costly (i.e. EUR 20k per SOC report) and should such reports also be required for sub-contractors and intra-group, the costs would become unreasonably high. As an alternative, companies may be requested to submit other documents, such as Transfer Pricing Documentation.

Article 7 (2) notes that the due diligence process must include an assessment of the existence of risk mitigation and business continuity measures, and how their functioning within the ICT third-party service provider is ensured. It must be noted that most suppliers consider business continuity plans as highly confidential and would not be willing to provide such information before the conclusion of the agreement, even under a non-disclosure agreement (NDA). This would mean ensuring compliance with this provision is expected to be challenging. A more feasible approach would be to require the vendor to submit a summary of its business continuity plan or by certifying their adherence ISO 22301 (or comparable international standard).

Finally, with regards to Article 7 (3) c i, the scope of the audits is unclear. It is important to clarify that undertakings are not required to perform full (on-site) audits prior to selecting/contracting ICT TPP (for instance by adding "if applicable or "if appropriate"). Not every ICT TPP that (somehow) supports a critical function must be audited in advance.

Q6. *Is article 8 appropriate and sufficiently clear?*

Insurance Europe would welcome guidance on "*conflict of interest*", with regards to the objective of identifying conflicts of interest and subsequently, the appropriate measures to identify, prevent and manage conflict of interests in the policy.

Q7. *Is article 9 appropriate and sufficiently clear?*

Insurance Europe would welcome some clarity as to why article 9 (1) only refers to Article 30 (2) of the Regulation with regards to elements to include in contractual arrangements for critical or important functions. Reference should be explicitly also made to Article 30 (3) of the L1 text because this article pertains directly to contractual clauses to be included in contracts with third-party providers providing critical or important functions.

Some clarity with regards Article 9 (3) would be welcome. On the one hand it states that the service recipient shall not "*rely solely on these reports over time*". On the other hand, the service recipient can rely on third party certification/report if conditions (a) to (h) are met.

Insurance Europe therefore proposes to reword the paragraph as follows: "*The policy referred to in paragraph 1 shall specify whether third-party certifications and reports as referred to in paragraph 2 (c) are adequate and sufficient to comply with their regulatory obligations and shall ~~not rely solely on these reports over time. In this regard, the policy shall~~ require that the financial entity shall use of the methods referred to paragraph 2 (c) only if it:*"

Alternatively, and as the requirement to not rely solely on these reports over time reflects EIOPA's guidelines on cloud outsourcing, a clarification could take the shape of a reference to the existing guidelines.

Furthermore, integrating the following changes would help to provide additional clarity:

- The wording of "*pool(ed) audit*" should be consistently used. Article 9 (2) b currently states "*pooled audit*", while Article 9 (3) h states "*pool audit*".
- Contractual arrangement should only be "*documented in one written document*", instead of using the wording "*shall be written*" (Article 9 (1)).
- It would be helpful to have clarity about what is meant by "*ICT testing*" in Article 9 (2) and (2) b.
- Article 9 (4) "*a written document*" should be changed to "*one written document*".

Q8. *Is article 10 appropriate and sufficiently clear?*

No, it is not clear how the requirements in Article 10 relate to the mandate in the L1 text. For the sake of clarity, Insurance Europe proposes that Article 10 makes a specific reference to the items in Article 30 (3) of the L1 text, which provides the mandate.

Article 10 (2) b and (2) e could be merged, given that both paragraphs require independent reviews.

With regards Article 10 (3), a risk assessment performed at financial entity level should not include details of performance management/assessment of individual ICT outsourcings. These are included in risk assessment at transactional level.

It will be important to clarify how frequently ICT TPPs must be audited. In this regard, clarity is needed on the extent to which internal audit needs to be involved and at what stage. Clarity would also be welcome as to whether companies need to rely on external parties to carry out audits.

In this regard, Insurance Europe wishes to stress that the overall Group Internal Audit Mandate is determined by the Board of Directors (BoD). Overwriting these governance principle takes the independence of the BoD's oversight away.

Q9. *Is article 11 appropriate and sufficiently clear*

Article 11 is not sufficiently clear about the extent to which the documented exit plan shall be set up for each ICT service or for each contractual arrangement evaluating each ICT service separately.

The testing of exit plans should be "*paper-based*" tests, as it would be impossible to test such plans in real conditions.

In addition, the requirement for a documented, reviewed, and tested exit plan should exclude intra-group service providers. Indeed, this requirement would represent an unnecessary administrative burden that would not be responding to an actual risk. The reason for this is that the risk of an unexpected need to exit the contractual relationship is greater with an external provider than with an internal provider given the close links with the internal provider, allowing for flexibility, communication, and alignment. Moreover, exiting a relationship with an intra-group provider would be the result of a decision taken by the entity, meaning that the entity can remain in control of the timeframe and conditions of the exit process. Finally, the decision to outsource all, or part of, the activity of an internal provider constitutes in principle a strategic decision involving a prior depth-assessment of the transaction, including an exit process.

Further guidance is needed on the exit plans and the testing of these plans. Do the ESAs envisage entities to develop detailed scripts or would a description of how an exit can take place suffice?

Finally, but more fundamentally, it will be important to distinguish exit planning from business continuity planning (BCP). Unlike an exit plan, a BCP can be periodically reviewed and tested. In case of service interruptions or failed service delivery, BCP needs to be invoked. In case of unexpected termination of contractual arrangement, the exit plan needs to be invoked.

Annex IV

DRAFT ITS on Register of information of ICT third-party

General comments

- Overall, re/insurers are concerned about the fact that financial services providers may ultimately have to bear the costs of the stricter requirements imposed on ICT TTPs. Ultimately, this cost, which is caused by additional governance and which is not in line with the expectations of service recipients, may result in the risk being passed on to end- customers.
- More fundamentally, there is a genuine fear that smaller suppliers, vendors and/or IT companies will not be able or willing to fully comply with the DORA, causing them to exit the market. This might result in a larger concentration risk, while DORA was envisaged to counter concentration risks. In this regard, Insurance Europe urges the ESAs to consider the potentially negative impact of the registry on competition dynamics. The need to establish and maintain an excessively intricate ICT registry could lead to a significant financial burden for smaller financial entities, thereby possibly raising entry barriers within the financial market.
- Insurers could take several steps to enable small vendors - who offer a valuable service to the insurance sector but face challenges in meeting the detailed requirements - to remain in the market:
    - offer smaller providers threat led penetration tests, paying for professional testers;
    - apply strict data minimisation;
    - apply stricter than average monitoring;
    - have their own internal audit-department check the cyber security of such a company, helping them mature faster than they would normally be able to;
    - buy the company, thereby solving the challenge, but at the same time reducing the number of companies in the market.
- In terms of other practical challenges, each vendor has one point of contact that deals with requests from companies. It will be very challenging for them to manage the influx of requests for information from companies.
- The industry is also concerned about the practical implications of the draft ITS, notably in terms of the additional work for the ESAs and the heavy administrative burden stemming from the new requirements.
- In terms of other practical matters, the industry considers that existing templates may be leveraged, especially where they already achieve the envisaged objectives.
- With regards to financial implications for the industry, it will also be key for the ESAs to consider the high costs related to requiring audit and SOC2 reports (e.g. considering that EUR 20k per SOC2 report times 300 vendors would imply a disproportionate financial burden).
- It will be important to pay heed to the GDPR's principle of data minimisation, notably as there will be 120+ data points per transaction/30-40k data points to manage on an ongoing basis in the register of information. The range of possible security measures, such as encryption and applying new technologies, such as new quantum computing, can create unnecessary risks. In relation to the data points for the mandatory registers, it is recommended to elaborate on the usefulness and purpose of recording for each mandatory field.

- A key question arising is the extent to which the EU vendor market is sufficiently mature to step in when big players are pushed out of the market.
- The proportionality principle is not sufficiently enshrined in the draft ITS. Indeed, the assertion that a financial entity "*[FE] relying on a significant number of ICT third-party service providers has more information to report in the register of information than an FE depending on a small number or ICT third-party service providers*" does not adequately reflect the proportionality principle. The approach in applying the proportionality principle should rather be risk-based, meaning that higher-risk financial entities should be required to maintain a more comprehensive register, while lower-risk entities should be required to maintain a register that is simpler.
- While financial entities aim to implement the L2 measures as swiftly as possible given the importance of ensuring digital operational resilience, the overwhelming task to develop comprehensive registers and manually populate an extensive taxonomy, in addition to having to rely on third parties in this regard, means that financial entities will need at least two years (from the date of application) for full implementation.

Q1. *Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?*

ICT TPPs located outside the EU usually do not have a LEI, which means that it is important to allow for other identification sources, such as a VAT-number.

The requirement to provide a LEI could also be problematic for smaller services, for instance small standard SaaS solutions used for support functions which are procured online. In addition, it is important to consider that LEI numbers could change in the wake of mergers and acquisitions of ICT vendors.

Some of the larger insurance groups are key service providers for BUs which provide, among others, bundled services involving multiple external / internal service providers. It may be complicated to identify and provide LEI for all ultimate service providers in such circumstances. It is not clear how to log bundled services in the register.

Q2. *Do you agree with Article 4(1)b that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?*

Insurance Europe proposes that the identification and inclusion of subcontractors be implemented on a best-effort basis. It is almost impossible to include information of subcontractors of "rank" higher than two or three, because this level of information is often not (publicly) available. For instance, while it might be publicly known that a vendor is using Amazon Web Services (AWS) cloud, the exact name and registration details of the relevant AWS entity may not be accessible. There could be disproportionate costs involved, and it would be too burdensome to require information of subcontractors of rank higher than two or three.

While the ITS seems to require information of all subcontractors until the last contractor in the service supply chain (page 97), none of the examples exceeds rank three. A clear materiality threshold is missing. There should be a reasonable limit to rank of subcontractors which needs to be logged, presumably rank two or three. As a sidenote, the definition of "*material subcontractor*" is unclear and it is also not clear who should determine the extent to which a subcontractor is material. Only the ICT TPP can make this assessment.

Another challenge is the fact that cloud ICT service providers frequently reserve the right to change subcontractors to adapt to evolving services or other commercial considerations. As a result, providing and maintaining detailed information on each and every subcontractor across multiple ranks becomes particularly cumbersome, especially when procuring various services from a single vendor, such as Microsoft 365, Azure, and Dynamics. The administrative burden of filling out this data on a per-service or per-order basis can be disproportionate and divert attention from the core objective of ensuring digital operational resilience.

To strike a more balanced approach, it may be more proportionate and practical to require information only on subcontractors which may be critical to maintain confidentiality, availability or integrity of ICT service provision, such as hosting service providers. This approach would still be adequate in achieving the objectives of the standard without overwhelming financial entities with an excessive administrative load. Another alternative to consider, to avoid burdensome administrative requirements for financial entities, would be to provide financial entities with an option of working based on third-party certifications. Such a certification-based approach would be in line with "*Guideline 11 – Access and audit rights*" in EIOPA's Guidelines on outsourcing to cloud service providers:

"42. Without prejudice to their final responsibility regarding the activities performed by their cloud service providers, in order to use audit resources more efficiently and decrease the organisational burden on the cloud service provider and its customers, undertakings may use:
a. third-party certifications and third-party or internal audit reports made available by the cloud service provider;"

This approach would help to maintain high standards for digital operational resilience, while it would also keep the administrative burden for financial entities to a minimum.

The requirement to register all countries data processing can lead to confusion and overlaps. Typically, contracts with ICT service providers determine whether data processing is limited to countries with adequacy decisions, or if other countries outside adequacy can be used with the implementation of sufficient supplementary measures, as assessed in the Transfer Impact Assessment (TIA) under GDPR rules. The TIA already evaluates the detailed risk of non-adequacy countries, considering both their laws and practices, along with the existence of adequate supplementary measures as required by the European Data Protection Board (EDPB). Having a similar yet slightly different and simpler register (without detailing supplementary measures) with different focus creates unnecessary confusion, as it duplicates information already covered in the TIA requirements.

Finally, and while recognising the importance of an oversight framework and the need for information in the register to determine which providers are critical, Insurance Europe would recommend that once a provider

becomes part of the oversight framework, the lead overseer collects and consolidates the more granular information about this provider (including the existence of subcontractors). Indeed, requiring each financial entity each year to collect information about each provider would create an unnecessary administrative burden for both parties when the provider is already in the system.

Q3. *When implementing the Register of Information for the first time: What would be the concrete necessary tasks and processes for the financial entities?*

Concrete necessary tasks, include changing existing inventory processes, infrastructure and tools and implementing, maintaining, and updating the register of information, leveraging existing local inventories.

In terms of significant operational issues to consider, in addition to resource constraints and the issues outlined under Q1 and 2, key challenges include:

- Extensive time and manual effort are required to collect and populate the necessary taxonomy. Creating the register demands certain technical resources, but the main issue is that currently, insurance companies typically only possess the required information for critical and important service providers. As a result, to populate the registry comprehensively, a detailed review of contractual documents (including agreements and their appendices) is necessary, along with online investigations to identify subcontractors and relevant information for each service.
    - Given each agreement covering different services would require multiple reports, detailing various aspects such as the functions and entities within the group using the ICT service, the type of service provided, annual budget projections, the entire subcontractor chain across several ranks, information about alternative service providers, details about the ultimate parent of the ICT service provider, and a comprehensive list of countries where data processing takes place.
    - Furthermore, understanding the functions and insurance products associated with each service within the financial entity would require a burdensome investigation, as such information is not documented for non-critical services.
- It will be challenging to transfer existing ICT-Service-Contracts - possibly even physical paper documents - into the digital register with all the necessary information, and within the short timeframe.
- Considering the scale and complexity of gathering such detailed information, attempting to implement this for all ICT services within the proposed scope and timeframe (by January 2025) is not feasible. Financial entities need at least two years from the date of application to implement the requirements.
- In line with the proportionality principle and to avoid financial and operational burden, Insurance Europe favours a more realistic approach whereby registers for non-critical ICT services may be limited to essential details, such as service provider identification, the category of the ICT service, and the financial entity using the service.

Furthermore, as it is currently not clear how the register will have to be implemented in practical terms and how (technically) the information will have to be shared with NCAs, additional guidance, tools and (Excel) templates would be welcome to ease the transition and increase efficiency.

Q4. *Have you identified any significant operational obstacles for keeping information regarding contractual arrangements that have been terminated for five years in the Register of Information?*

No.

However, it should be clarified that contracts already terminated at the time the ITS starts applying are exempt.

Considering the amount of work to implement the register, it would be disproportionate to include contracts that have been terminated for five years in the second year of the register. The RTS should stipulate that until 2030, financial entities should indicate each year, which contracts are being terminated. By 2030, the register would then contain a five-year history of terminated contracts, without imposing a disproportionate administrative burden on financial entities in the second year.

Q5. Is Article 6 sufficiently clear regarding the assignment of responsibilities for maintaining and updating the *register of information at sub-consolidated and consolidated level?*

Article 6 lacks sufficient clarity with regards to assigning responsibilities for maintaining and updating the register of information at sub-consolidated and consolidated levels. The guidance on consolidated and sub-consolidated reporting is ambiguous, especially concerning scenarios where a service is centrally procured by one group entity A (which may not be a financial entity) but utilised by multiple financial entities B within the same group.

The uncertainty arises if reporting should be based on the contracting parties involved in the initial purchase, or on the entities that subsequently utilise the service. For example, it is unclear whether financial entities B should only register and report agreements that they have concluded with entity A on the provision of multiple ICT services. Clarity in relation to this aspect is crucial to ensure accurate and standardised reporting across financial entities, preventing potential inconsistencies and confusion in the reporting process.

Q6. *Do you see significant operational issues to consider when each financial entity shall maintain and update the registers of information at sub-consolidated and consolidated level in addition to the register of information at entity level?*

No, given that the parent undertaking is responsible for defining the scope of consolidation and sub-consolidation.

Q7. *Do you agree with the inclusion of columns RT.02.01.0041 (Annual expense or estimated cost of the contractual arrangement for the past year) and RT.02.01.0042 (Budget of the contractual arrangement for the upcoming year) in the template RT.02.01 on general information on the contractual arrangements? If not, could you please provide a clear rationale and suggest any alternatives if available?*

Yes.

Q8. *Do you agree that template RT.05.02 on ICT service supply chain enables financial entities and supervisors to properly capture the full (material) ICT value chain? If not, which aspects are missing?*

It is almost impossible to include information of subcontractors of "*rank"* higher than two or three. While the ITS seems to require information from all subcontractors until the last contractor in the service supply chain (page 97), none of the examples exceeds rank three. A clear materiality threshold is missing. There should be a reasonable limit to rank subcontractors which needs to be logged, presumably rank two or three.

The template RT.05.02 on the ICT service supply chain aims to enable financial entities and supervisors to capture the full (material) ICT value chain. However, this requirement poses a disproportionate burden, particularly in terms of the need to have to gather extensive information on all subcontractors across several ranks, as well as practical challenges:

- Many ICT service providers do not consider their group entities subcontractors and, consequently, may not report such information.
- ICT providers typically indicate that they are using AWS as hosting service provider, without detailing which AWS entity they have contracted. Subsequently, identifying and registering countries for all subcontractors becomes an overwhelming task, without clear benefits in terms of achieving the objectives, especially given the complex supply chains prevalent in the ICT industry. The standard does not provide clear guidance on how many ranks down the supply chain should be registered.

While GDPR-related practices have prompted ICT service providers to make information on sub-processors (rank 2) publicly available, this standard aims to cover not only sub-processors but also any subcontractors, adding additional complexity to the reporting process. Moreover, information on subcontractors beyond the second rank may not be available even to the direct ICT service provider itself.

Given these challenges, Insurance Europe urges the ESAs to bring this reporting requirement in closer alignment with established GDPR practices, limiting it to subcontractors involved in processing personal data, including those handling encrypted personal data (e.g. hosting service providers) and therefore covering all major risks. By focusing on these critical aspects, the reporting process would be more practical, relevant, and consistent with existing data protection measures.

Q9. *Do you support the proposed taxonomy for ICT services in Annex IV? If not, please explain and provide alternative suggestions, if available?*

No. As regulatory consistency across jurisdictions (beyond the EU context) is currently lacking, the proposed taxonomy should contribute to achieving an aligned approach, also granting clarity for all third party and ICT services.

In addition, it should be noted that the services and other products listed below are not per se ICT services as defined by DORA Level 1: "*ICT services'means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services*

which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone service":

- S1 "*Software licensing*" that runs on premises is not a service and therefore not an ''*ICT service*'', regardless of whether it concerns rental of software;
- S8 "*physical onsite security"*;
- S16 "*ICT consulting*" and "*ICT Project Management*" are not ICT services as it does not rely on ICT systems (it is a different type of service) and are provided by humans.

Insurance Europe would suggest removing "*ICT project management*", "*ICT Development*", and "*ICT Consulting*", "*physical onsite security*", and "*software licensing*" from the taxonomy of "*digital or data services provided through ICT systems*" to ensure clarity and proper alignment with the mandate given to the ESAs under Article 28 (9) of DORA.

Insurance Europe would also propose reducing the number of categories and avoid overlapping categories. For insurance, it would be sufficient to have one category covering all types of cloud services. Cloud services are continuously evolving, leading to challenges in easily distinguishing between strict categories. Furthermore, certain services fall into hybrid categories, for instance, blending features from Software as a Service (SaaS) and Platform as a Service (PaaS). Consolidating all cloud services in one category will simplify the classification process and provide a clear understanding of the scope and nature of cloud-related activities.

Q10. *Do you agree with the instructions provided in Annex V on how to report the total value of assets and the value of other financial indicator for each type of financial entity? If not, please explain and provide alternative suggestions?*

No comment.

Q11. *Is the structure of the Register of Information clear? If not, please explain what aspects are unclear and suggest any alternatives, if available?*

The proposed structure of the Register of Information is complex and raises concerns, particularly regarding the assessment of actual implementation costs. Rather than opting for a single-level simpler (flat structure) approach, which could be seamlessly integrated as additional information fields within existing contract archives of financial entities, the proposed approach would require the creation of multiple registers. This would demand substantial IT development and require a separate IT system to accommodate the relational structure. The cost implications of this complex approach seem to have been overlooked.

Some of the larger insurance groups are key service providers for BUs which provide, among others, bundled services involving multiple external/internal service providers. It may be complicated to identify and provide LEI for all ultimate service providers in such circumstances. It is not clear how to log bundled services in the register.

Insurance Europe would welcome clarification as to whether all functions should be identified and filled in in template RT.06.01, or whether RT.06.01 refers only to critical or important functions. It would be helpful to get

clarification about the extent to which a function can be assessed as time under RT.06.01.0070 but still not be a critical or important function under RT.06.01.0061. Clarification about the interrelation between these two would be helpful.

Q12. *Do you agree with the level of information requested in the Register of Information templates? Do you think that the minimum level of information requested is sufficient to fulfil the three purposes of the Register of Information, while also considering the varying levels of granularity and maturity among different financial entities?*

The minimum level of information requested in the Register of Information templates is extensive and will lead to significant administrative costs for financial entities. At the same time, it remains unclear what tangible benefits such a comprehensive register would yield. In view of ensuring a practical and cost-effective approach, conducive to the objectives of achieving digital operational resilience, the register should include information that is strictly necessary and in line with the mandate given to the ESAs pursuant to Article 28.9 of DORA.

In line with the proportionality principle and to avoid financial and operational burden, Insurance Europe would favour a tailored template for service providers not supporting critical or important functions, based on their level of criticality.

For instance, requiring multiple reports for low-value and low-risk services used by UX designers, including reporting all supply chain as well as internal recipients of services, will lead to unnecessary administrative overhead. It is also important to note that certain information, such as subcontractors (especially ICT service provider's affiliates), is subject to frequent changes.

Finally, Insurance Europe wishes to reiterate that it is almost impossible to include information of subcontractors of "*rank*" higher than one or three. While the ITS seems to require information of all subcontractors until the last contractor in the service supply chain (page 97), none of the examples exceed rank three. A clear materiality threshold is missing. There should be a reasonable limit to rank subcontractors which needs to be logged, presumably rank 2 or 3. There could be disproportionate costs involved and it would be too burdensome to require information of subcontractors of rank higher than two or three.

Q13. *Do you agree with the principle of used to draft the ITS? If not, please explain why you disagree and which alternative approach you would suggest.*

The principle underpinning the draft ITS is not in line with the DORA Level 1 mandate. It also places unnecessary burdensome obligations on financial entities. While recognising the importance of registering and reporting ICT agreements, the ITS as it currently stands requires a disproportionate effort to develop comprehensive registers, manually populating an extensive taxonomy, and ensuring the continued monitoring and review of this data. Insurance Europe would favour a more realistic, risk-based, and proportionate approach.

Q14. *Do you agree with the impact assessment and the main conclusions stemming from it?*

Yes.

In addition to the consultation questions above, for each column of each template of the register of information, the following is asked:

a) Do you think the column should be kept? Y/N : Yes
b) Do you see a need to amend the column? Y/N: No
c) Comments in case the answer to question (a) and/or question (b) ”No”.

It is challenging to understand the usability and practicality of the templates without having yet used them. More broadly, the volume of information required appears to exceed what is necessary to achieve the DORA’s objectives. Insurance Europe would therefore welcome clarification on the intended usage of the data in each column.