Position Paper

Insurance Europe position on the European Commission proposal for a Digital Operational Resilience Act

Our reference:	EXCO-CS-21-031	Date:	22 February 2021
Referring to:	Financial services – improving resilience against cyberattacks (new rules)		
Contact person:	Áine Clarke, Policy Advisor, General Insurance	E-mail:	Clarke@insuranceeurope.eu
Pages:	12	Transparency Register ID no.:	33213703459-54

General comments

Cybersecurity is an issue that is of major importance to the European insurance sector. As the sector embraces the digital transformation, it is keen to ensure that this process comes hand in hand with measures to protect digital infrastructure from cyber threats. The importance of resilient information and communication technology (ICT) has been brought sharply into focus by the COVID-19 pandemic, which has resulted in an unprecedented acceleration of in cyber activity — bringing with it both challenges and opportunities. Against this background, Insurance Europe welcomes efforts to boost the cyber resilience of all sectors of the economy, including insurance. The European Commission's proposal for a Digital Operational Resilience Act (DORA) for the financial sector is an important step in this regard.

European insurers believe it is vital to put in place a risk-based cybersecurity framework established on key common principles, unified in one single piece of legislation. It is important to ensure that this framework takes account of the fact that the financial sector is very diverse, and, therefore, that a one-size-fits-all approach to boosting the cyber resilience of the sector is avoided. This position paper outlines Insurance Europe's views and recommendations on the European Commission's DORA proposal.

Alignment

Insurance Europe is fully in support of the envisaged goal of strengthening the ICT resilience of the financial sector, however it believes that this will only be achieved through the implementation of one single regime. Many requirements in the DORA proposal are covered by various other sets of rules — both existing rules (EIOPA guidelines on outsourcing to cloud service providers, Solvency II and Delegated Act (EU) 2015/35, the NIS Directive (where applicable)) and forthcoming rules (EIOPA guidelines on ICT security and governance, which European insurance companies will be required to have implemented by 1 July 2021). The same goes for thoroughly tested and widely used international standards in this field, eg, ISO27001, CIS21, NIST. Alignment and consistency between all initiatives will therefore be crucial. Because of this, Insurance Europe calls for a clarification that all elements of the insurance industry's digital operational resilience shall be exclusively regulated under the DORA, further to the *lex specialis* clause outlined under **Article 1.2** DORA.

Insurance Europe aisbl
Rue du Champ de Mars 23, B-1050 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

© Reproduction in whole or in part of the content of this document and the communication thereof are made with the consent of Insurance Europe, must be clearly attributed to Insurance Europe and must include the date of the Insurance Europe document.

Proportionality

While Insurance Europe welcomes the recognition that there are significant differences in size, business profile or exposure to digital risks between the companies in the scope of the DORA, in its current form, the level of detail required by the proposal stands contrary to the initiative's aim of encouraging growth and innovation in the financial sector. Proportionate requirements are essential because different types of entities are exposed to different types of risks and require different types of protection, and because different financial sector entities have a very different impact on the operational resilience, performance and stability of the EU financial system (ie, insurers vs. banks). In order to reflect the diverse landscape of risk profiles, it is therefore vital that requirements under the DORA follow a risk-based approach.

While the DORA references the principle of proportionality on several occasions, it is not clear what this means in practical terms and how this will alter the detailed requirements it proposes to introduce. Insurance Europe calls for the principle of proportionality, as treated under Solvency II, to be incorporated into all elements of the DORA proposal — creating rules that are proportionate to the nature, scale and complexity of the risks inherent in the business of an (insurance) undertaking. In order to apply this principle, Insurance Europe calls for more general requirements that can be tailored to the different company profiles across the financial sector. This applies in particular to the specification of deadlines or intervals for certain monitoring activities (among other things, there are currently requirements for at least an annual review of the entire ICT risk management framework, at least an annual review of ICT risk scenarios, at least an annual ICT risk assessment, at least an annual test of the ICT emergency plan and the ICT disaster recovery plan as well as all critical ICT systems and applications, at least an annual reporting obligation for all new ICT contracts, and threat-led penetration tests (TLPTs) at least every three years) and the very extensive and detailed documentation requirements (eg, the requirement to provide a detailed report on all new ICT contracts, ICT strategies, ICT framework, guidelines, emergency planning (ICT Business Continuity Plan), ICT Disaster Recovery Plan (DRP), documented processes and protocols). In these areas, more simplifications should be permitted, and a principle-based approach should be favoured over concrete, detailed requirements.

The application of the principle of proportionality to microenterprises — in effect, exempting them from requirements in certain areas — is welcomed by Insurance Europe. However, due to the narrow definition of microenterprise (less than 10 employees and sales or balance sheet total of less than €2m according to Article 2.3 of the Annex of the Recommendation 2003/261/EC), a large number of very small companies will still be fully covered by the requirements. In this regard, Insurance Europe would be in favour of raising the threshold for exemptions to SMEs as defined under Annex I, Article 2.2 of Recommendation 2003/261/EC (an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed €10m).

Furthermore, the DORA's requirements should cover only the critical and important functions of an undertaking: for this purpose, requirements regarding classification of ICT-related business functions (**Article 7**), protection and prevention (**Article 8**), advanced testing (**Article 23**), ICT third-party management (Chapter V) and — as is proposed in the text — reporting (**Article 17**), should be limited to such functions. It must always be the role of the financial entity to determine whether a function/activity is critical or important, on the basis of whether the undertaking would be able to deliver its services to clients (policyholders, in the case of insurers) without it. This definition, inspired by the EU legal framework applicable to outsourcing for insurers (Guideline 60 of EIOPA Guidelines on System of Governance), should replace the definition proposed in **Article 3.17**, which introduces unclear terms (such as "materially impair") and will generate legal uncertainty. Should the requirements under the ICT risk management framework not be limited to critical or important functions, it must be explicitly stated that all security measures under Articles 5 to 13 should be proportionate to the specific risk profile of the business.

Oversight of ICT TPPs

Insurance Europe welcomes the proposed monitoring framework for critical ICT service providers as a step in the right direction. Harmonised direct supervision of ICT service providers (eg, cloud providers) is important and should be accompanied by corresponding regulatory relief for users of these services. Unfortunately, by placing the responsibility for oversight of ICT service providers outside the scope of the oversight framework solely on

individual financial entities, the draft regulation falls short of introducing this relief. Instead, the draft proposes to introduce detailed, burdensome oversight requirements for individual companies (eg, audit, on-site inspections, contractual requirements, which are difficult or even impossible to obtain, and costly to carry out), which is likely to discourage the use of these services. In order to alleviate this burden, Insurance Europe is in favour of the development of certification schemes for all ICT third-party providers (TPPs) that could be used as a means of demonstrating compliance with the DORA (and NIS requirements regarding digital service providers). In this respect, Insurance Europe welcomes the candidate cybersecurity certification scheme for cloud services (EUCS) that is being developed by ENISA, however it calls for clarity on how this project will interact with the proposed oversight framework under the DORA, and how schemes such as the EUCS might reduce oversight demands on the clients of providers that make use of them (ie, insurance undertakings).

Furthermore, the scope of the DORA should be limited to the *outsourcing* of ICT services necessary for carrying out critical and important operational functions or activities and not simply to the *use* of ICT services provided by third parties. There may be material risks when critical functions or business operations are outsourced to third parties, notably if they are themselves of systemic relevance, but the use of certain services (eg, software services) poses limited risks, and it would therefore be disproportionate to subject every technology service to the same requirements under the DORA.

Detailed comments

- **CHAPTER I — General provisions (Articles 1-3)**

  - **Subject matter (Article 1)**

Insurance Europe supports the provision outlined in **Article 1.2** on operators of essential services. However, given that the DORA's requirements will fully replace all NIS requirements on financial entities that currently fall within its scope, it believes that recital 13 of the proposed NIS2 Directive should be copied into Article 2 DORA in order to clarify the interaction between the two texts. This will provide the necessary legal certainty that the NIS Directive (and any future revisions) will not apply to entities regulated under the DORA.

  - **Personal scope (Article 2)**

As drafted, **Article 2.n** triggers competition issues, as some financial intermediaries are not in the scope of the DORA (credit intermediaries covered by the Directive of 4 February 2014 concerning mortgage credit, tied agents as defined in Article 4 (29) of MiFID2, entities referred to in Article 4 (38) of Directive 2015/2366 on payment services), while others are. Insurance Europe believes that a blanket inclusion of insurance intermediaries in the scope of the DORA is disproportionate to the risks they pose and unrealistic regarding their capacities. According to the wording of the DORA proposal, ancillary insurance intermediaries would qualify as "financial entities" despite the fact that, by definition, their insurance distribution activity is not only ancillary to their main activity but can only relate to products that are add-ons to a good or service marketed in the context of their main business activity.

Insurance Europe therefore believes that **Article 2.n** should be amended as follows (introducing a threshold for insurance and reinsurance intermediaries and excluding ancillary insurance intermediaries from the scope entirely):

n) insurance intermediaries and reinsurance intermediaries as referred to in article 2.1 (3) and (5) of the Directive 2016/97 on insurance distribution which are legal persons AND employ more than 50 persons and whose annual turnover and/or annual balance sheet total exceeds €10m.

- **CHAPTER II — ICT risk management (Articles 4-14)**

  - **Governance and organisation (Article 4)**

Insurance Europe agrees that an efficient system of governance and organisation is vital for fostering digital operational resilience. However, it believes that it should be left to the company to determine the means of achieving this, whether by establishing an independent ICT risk management process within an independent ICT framework, or by supplementing ICT risk management practices in existing structures. Insurance companies already have comprehensive internal processes and guidelines for the use and outsourcing of information and cloud technologies, which have been fully integrated into existing risk management systems in order to meet existing requirements and expectations of supervisory authorities. The strength of these already well-established ICT risk management processes has been evidenced by the positive experience of European insurers when faced with the new COVID-19 working environment. If an additional ICT risk management process and an independent ICT risk management framework were to be required, as is proposed under the DORA, it would no longer be possible for many companies to uphold their integrated approach to ICT risk management. This would likely lead to the burdensome duplication of documentation and processes. Moreover, this could jeopardise established methods of integrated risk management and lead to unnecessary overlap, costs and, as a result, inefficiencies in the management of ICT risk. Insurance Europe therefore considers a company-specific method of governance and organisation — which would allow for existing integrated solutions to be maintained — to be more suitable, provided that a level of cyber resilience that matches their business needs, size and complexity (as referred to in **Article 5.1**) can be ensured.

Governance and organisation requirements should also leave more room for the delegation of tasks within the company, e g, to individual managers or company representatives. In the proposal's current form, only **Article 4.3** provides for this, and only in the context of oversight of ICT third-party risk exposure and relevant documentation. The possibility of delegation should be extended to other aspects of business organisation, for example information about outsourcing agreements (**Article 4.2.h**). As regards ICT training for the management body (**Article 4.4)**, the requirement for specific training should always correspond to the respective risk profile of the company in question.

- **ICT risk management requirements (Articles 5-13)**

Insurance Europe believes that some of the proposed requirements for ICT risk management go beyond what is necessary for financial entities to achieve the goal stated in **Article 5.1** ("a level of cyber resilience that matches their business needs, size and complexity"), focusing overly on compliance rather than on how financial entities can demonstrate outcomes through a risk-based approach.

Introducing strict security requirements for all ICT functions and activities — regardless of the risks that they pose — would amount to an unnecessary strain on a financial entity's resources and place heavy constraints on activities that are not essential to the core activity of the entity. Insurance Europe is therefore of the opinion that the DORA's requirements should focus only on critical and important functions of the undertaking. For this purpose, requirements regarding classification of ICT-related business functions (**Article 7**) and protection and prevention (**Article 8**) should be limited to such functions. As previously outlined, the definition of "critical or important function" should refer to a function that is essential to the operation of the undertaking as it would be unable to deliver its services to clients (policyholders, in the case of insurers) without that function. This definition, inspired by the EU legal framework applicable to outsourcing for insurers (Guideline 60 of EIOPA Guidelines on System of Governance), should replace the definition proposed in **Article 3.17**, which introduces unclear terms (such as "materially impair") and will generate legal uncertainty.

Many of the ICT risk management requirements go into technical detail and — either directly or indirectly — imply the implementation of burdensome processes without providing a clear explanation of how they will incorporate the principle of proportionality. The proposed contents of the ICT risk management framework indirectly require the implementation of a management system aligned with the ISO/IEC 27001 standard, which is not free to obtain and could be questioned from a proportionality perspective. With regard to the optional incorporation of internationally recognised standards into the ICT risk management framework, it is very unclear what "in accordance with supervisory guidance" (**Article 5.4**) will mean in practice, which could pave the way for different interpretations in different member states. **Article 5.5** requires segmentation of ICT management

functions. However, such functions within insurance companies are conclusively regulated under the Solvency II Directive, so it should be clarified that this Article does not require the mandatory establishment of further key functions.

Some of the ICT risk management requirements (**Articles 6-12)** cover procedures, eg, change management (**Article 8.4.e**), that are not always regarded as best-practice methods or widely used. Methods for change management should instead be flexible, as well as widely used and accepted. The same applies to the proposed requirement for testing of BCPs and DRPs after substantive changes to ICT systems (**Article 10.5.a**); an ambiguous requirement that can have adverse effects on risk management and that drives up costs, offering few benefits in terms of resilience. Furthermore, the purpose and benefit of reporting all costs and losses associated with ICT disruptions and ICT-related incidents to competent authorities is not clear and would place a disproportionate burden on regulated entities (**Article 10.9**).

The annex to this paper contains a list of proposed requirements from Chapters II, IV and V on which Insurance Europe would like clarification that they can be applied in a way that can be tailored to different business and risk profiles.

- **Further harmonisation of ICT risk management tools, methods, processes and policies (Article 14)**

Under Article 14, the ESAs, in consultation with ENISA, will be required to develop draft RTS further specifying elements of the ICT risk management framework, eg, further specifying the components of the ICT Business Continuity Policy (**Article 10.1**) and further specifying elements to be included in the ICT security policies, procedures, protocols and tools (**Article 8.2**).

Insurance Europe strongly believes that digital operational regulation should be principle-based to be flexible enough to keep abreast of technological developments and emerging threats. Therefore, it is crucial that each entity can choose the security procedures and tools that are most effective to meet its specific risk profile based on the entity's own risk assessment. If relevant elements included in procedures, protocols and tools cannot be tailor-made to suit the specific organisation due to rigid and detailed demands (ie, cannot be applied in a risk-based manner) there is a danger that investments and resources allocated to risk management will not be allocated efficiently.

Insurance Europe is therefore concerned by the list of technical standards delegated to the ESAs under **Article 14** of the DORA proposal and invites the European Commission to assess the likely negative impact on innovation if the DORA empowers EIOPA to draft ICT management tools, methods, processes and policies in a very detailed way. In Insurance Europe's view, unless the mandate to the ESAs in this area is sufficiently clear, the broad provisions of Article 14 will stifle innovation in the area of ICT in the EU — while innovation continues elsewhere in the world.

Given that many requirements in the areas listed under **Article 14** are covered by EIOPA guidelines on ICT security and governance, which European insurance companies will be required to have implemented by July 2021, Insurance Europe believes that these guidelines should not enter into force, so as to avoid a piecemeal regulatory environment. Furthermore, given that many of the requirements under Article 14 are covered by existing NIS national implementation texts, these texts should be modified in light of the proposed DORA requirements.

- **CHAPTER III — ICT-related incidents (Articles 15-20)**

The proposal introduces a general requirement for financial entities to establish and implement a management process to monitor and log ICT-related incidents, as well as an obligation to classify them based on criteria developed by the ESAs through a common ICT-related incident taxonomy that should specify materiality thresholds.

Insurance Europe agrees that sharing information on ICT-related incidents is fundamental to enabling a collective understanding of the overall landscape of ICT-related incidents and, in turn, strengthening Europe's cyber resilience. However, any requirements that the DORA proposes to introduce should take account of pre-existing and well-established national incident reporting systems within the insurance sector.

Article 16 (classification of ICT-related incidents) calls for a high level of detail for the classification of incidents and it is unclear how this requirement can be applied proportionately. This is especially true seeing as, for smaller entities, time spent classifying the incident may be at the expense of timely and efficient management of the incident itself.

- **Reporting of major ICT-related incidents (Article 17)**

It is essential that reporting of major ICT-related incidents is centralised, ie, an incident need only be reported to one single authority. Therefore, reporting requirements under different pieces of legislation (eg, DORA, GDPR) should be harmonised to avoid unnecessary duplication of efforts (eg, the same incident reported to multiple competent authorities, in different formats and with different time periods). This requirement should be explicit in the mandate to the ESAs. It is also of paramount importance that the reporting information and templates are harmonised as per **Article 18**, in order to ensure a consistent approach to incident-reporting across the EU.

Under the DORA proposal, insurers must report to their national competent authority (as per Article 41.l and Article 30 Solvency II) "major" ICT-related security incidents that will be identified as such by materiality thresholds to be developed by the ESAs. **Article 17.3** lays down rigid time periods for the notification and reporting of an incident, which do not leave room for application in a way that is proportionate to the nature and size of the incident in question. This applies to the requirement for initial notification of the incident, which **Article 17.3.a** requires be done "without delay"; a requirement that makes little sense given that such a notification requires prior testing (in comparison, the GDPR introduces a 72-hour notification requirement which already poses a challenge). If this requirement is to be kept in its current form, it must be clarified that the initial notification requirement amounts to no more than a simple notification (a warning, with no further detail — although the added value of such a notification is unclear).

In the same vein, the arbitrary value of one week for the submission of an intermediate report (**Article 17.3.b**) is meaningless; the text should instead require an update only when significant changes have taken place. Similarly, as regards the submission of a final report, the one-month period referred to in Article **17.3.c** should begin only from the date of resolution of the incident. There are no risk-based arguments behind a very short timeframe for notifications. Rather, reporting timeframes must be proportionate to the need for real-time availability of the services provided. Regarding the role of supervisory authorities in this process, under **Article 20**, supervisory authorities are only required to respond to the reporting financial entity with necessary guidance or feedback "as quickly as possible", suggesting that the speed of the supervisory response will depend on the incident in question (a more flexible approach).

Under **Article 17.4**, entities may also delegate reporting obligations to a service provider. Insurance Europe calls for clarification of which party is responsible in terms of compliance with reporting requirements (timeframes, etc.).

- **Centralisation of reporting of major ICT-related incidents (Article 19)**

Article 19 provides for the possible establishment of a single EU Hub for the centralisation of major ICT-related incident reporting. In principle, Insurance Europe welcomes such an initiative, given that a collective understanding of the overall landscape of ICT-related incidents is fundamental to increasing the EU's cyber resilience. As a general remark, any such initiative should aim to encourage best practices and refrain from establishing new requirements, such as additional information channels or multiple layers of reporting. Therefore, national competent authorities should have full responsibility for the coordination of additional information-sharing with the EU Hub. It is also vital that incidents be reported in an anonymised/pseudonymised format to avoid reputational damage for the financial entities involved.

- **Supervisory feedback (Article 20)**

Given the considerable effort associated with reporting ICT-related incidents, it is disappointing that the supervisory feedback mechanism outlined in **Article 20**, whereby data on incidents is anonymised, aggregated and fed back to entities, has been limited to a once-yearly exercise. It is doubtful that the proposed approach would provide reporting entities with any information of high strategic value that would assist them in preparing for future threats. A more regular feedback mechanism — or indeed a continuous open channel of communication — would therefore be welcomed.

- **CHAPTER IV — Digital operational resilience testing (Articles 21-24)**

While Insurance Europe welcomes the risk-based approach to digital operational resilience testing outlined in **Article 21** (whereby financial entities must establish, maintain and review, with due consideration of their size, business and risk profiles, a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework), in general, the requirements introduced in Chapter IV are very detailed and prescriptive. As a consequence, they are not suited to tailoring to the wide variety of risk profiles to be found across the financial sector. For example, **Article 22** requires a comprehensive test portfolio among other strict requirements (eg, vulnerability assessment before deployment) for annual testing of all critical systems. A more proportional alternative, better suited to the insurance industry, is expressed in the EIOPA guidelines on ICT security and governance, where organisations need to define and implement a security testing framework and test systems based on the business criticality and security requirements, where sufficiently skilled and independent internal testers can be used.

- **Advanced testing of ICT tools, systems and processes based on threat-led penetration testing (Article 23)**

In this area, the proposal claims to incorporate the principle of proportionality into the requirements to perform advanced testing (TLPTs). Critical entities, to which this requirement would apply, would be identified by the criteria that will be determined by the ESAs, according to **Article 23.4**. However, the relationship between this article and **Article 23.3** is unclear, as the latter already lists a number of criteria that competent authorities should take into account when identifying financial entities that will be subject to such advanced testing. As a consequence, further RTS do not appear necessary.

Furthermore, when identifying companies that will be required to carry out such advanced testing, it must be taken into account that TLPTs are extremely burdensome on resources (costing in the six-digit range, with required preparation time of up to a year). Such advanced testing should therefore only be mandatory for major financial institutions. As mentioned above, a more proportional alternative, better suited to the characteristics of the insurance industry, is expressed in the EIOPA guidelines on ICT security and governance. The fact that there is a limited number of external testers available for TLPTs must also be given due consideration in this context.

As regards **Article 23.2**, the requirement that "threat lead penetration testing shall cover at least the critical functions and services of a financial entity and shall be performed on live production systems supporting such functions" could be highly inappropriate for many financial entities. Rather, this should be performed in environments equal or representative to live production systems, or alternatively on live production systems, if deemed appropriate by the entity. Under the same provision, the requirement for documentation of reports and remediation plans to be provided to competent authorities at the end of each test for the purpose of issuing an attestation introduces security challenges (if sensitive details are to be shared) and logistical challenges for both parties. It would be more practical for the entity to retain this information and present it on the request of the competent authority.

The implementation of some of the requirements under **Article 23.3** remains unclear. For example, more clarity would be welcomed on what "certifications or formal codes of conduct or ethical frameworks" for the testers mean. Any changes should avoid disruption to existing contractual arrangements with third parties.

- **CHAPTER V — Managing of ICT third-party risk (Articles 25-39)**

As the management of ICT third-party risk is an area that is already covered under other pieces of legislation (eg, Solvency II and its delegated acts) and supervisory guidelines (eg, EIOPA guidelines on system of governance, EIOPA guidelines on outsourcing to cloud service providers), it is essential that a harmonised and consistent approach can be ensured at the level of Articles 25, 26 and 27. Insurance Europe also notes the ongoing work of the European Commission to develop standard contractual clauses for cloud outsourcing by financial institutions, which would allow financial institutions to better reflect their sectoral regulatory constraints, eg, Solvency II in the case of insurers, in their contractual agreements with cloud service providers. Given this initiative, Insurance Europe calls for clarification on how these model clauses may be used alongside Article 27 of the DORA.

Insurance Europe welcomes the proposal in Chapter V to establish an oversight framework for critical ICT providers as a step towards remedying the asymmetrical relationship between financial entities and large ICT service providers. However, it believes that this chapter should further strengthen the principle of proportionality by limiting its requirements (key contractual agreement, reporting, register, inspection and audit rights, termination and exit strategies, etc.) to critical and important operational functions or activities (as in the sector-specific EIOPA Guidelines on Outsourcing to the Cloud). This terminology is consistent with the definition provided in Guideline 16 of the EIOPA Guidelines on System of Governance. In other words, the use of ICT services for non-critical or non-important operational functions or activities should fall outside the DORA's scope, since to include all types of ICT services in the DORA's scope would subject undertakings to burdensome requirements that seem disproportionate to the risks stemming from the ICT services that do not support critical and important operational functions or activities.

Therefore, in accordance with Article 49 of the Solvency II Directive, only if there are certain risks associated with the use of ICT services that may have an impact a) on the insurer's ability to comply with its regulatory requirements, or b) its customers, should the ICT services be regarded as related to critical and important operational functions and covered by the requirements established under DORA. This rule should apply regardless of whether the services are provided by non-critical third-party service providers or by critical (large) third-party services providers as designated under section II.

EIOPA's final report on Public Consultation n° 13/008 on the proposal for guidelines on the system of governance (EIOPA/13/413 27 September 2013, n° 5.175) gives examples of activities that cannot be considered critical or important operational functions or activities), to which the DORA should make direct reference:

- the purchase of standardised services, including market information services and the provision of price feeds;
- the provision of elements of human resources support, such as processing the payroll.

Other examples include:

- Solvency II services and portfolio analyses of business investment
- Printing of documents

Furthermore, it is important to distinguish between critical operational functions (the financial entity's own critical functions) and critical ICT service providers, which can be deemed as such due to their size and market share. It will also be important to differentiate between ICT third-party providers and *intragroup* ICT third-party providers, as the cybersecurity of the latter will be easier for an individual company to monitor and oversee.

- **General principles (Article 25)**

Article 25 states that financial entities' management of ICT third-party risk shall be implemented in accordance with the principle of proportionality. However, it places full responsibility on financial entities for ensuring that ICT third-party service providers that fall outside the scope of the oversight framework comply with the requirements laid out in the DORA. Despite the reference to proportionality, this Article contains several detailed requirements that leave limited scope for company-specific implementation. As outlined above, these requirements should only apply to the outsourcing of critical and important functions.

Article 25.4 of the draft requires a comprehensive register of all ICT third-party provider agreements, which differentiates between critical and non-critical functions, requiring this register to be maintained at a consolidated level. The regulatory added value of this complex documentation method is not clear, as the DORA already requires that the responsible supervisory authorities be informed about ICT third-party provider agreements through notification obligations in the case of important functions or activities and can request further information, if necessary. It should therefore be left to the supervised companies to decide how this information is documented. Given the obligation to notify the competent authority of planned contracts with critical ICT functions, the additional annual reporting obligation should also be removed.

In EIOPA Guidelines on Outsourcing to Cloud Service Providers, documentation requirements are principle- and risk-based. The guidelines set out certain information that is to be recorded only for critical or important operational functions outsourced to cloud service providers, which is aligned to the set of information required by the EBA guidelines. There is also no requirement for a formal register in the EIOPA guidelines. EIOPA has indicated that the requirements of these guidelines are also applicable only in the case of cloud outsourcing of critical or important operational functions or activities.

A prior determination of the frequency of audits and inspections (**Article 25.7**) should not be necessary in every case but should rather be risk-based, distinguishing between critical and non-critical functions (as outlined above). The need for on-site inspections could be reduced through the use of certification mechanisms — developed by ENISA, for example. In this area, Insurance Europe welcomes the possibility to carry out collective tests as well as to commission an external third party to carry out tests.

As regards termination of contracts (**Article 25.8**), this should be optional rather than immediately mandatory, allowing room for both ICT providers and financial entities to evaluate all possible remedies before resorting to termination. Given the lengthy and resource-intensive process of searching for suitable providers and negotiating contracts, this would be both a more appropriate and a safer option than immediate termination. The circumstances under which the proposal requires that a contract be terminated, ie, in Article 25.8.d. "circumstances where the competent authority can no longer effectively supervise the financial entity as a result of the respective contractual agreement" are rather unclear, and Insurance Europe suggests that this passage be deleted.

- **Key contractual provisions (Article 27)**

Many of the provisions outlined under **Article 27** are practically impossible to enforce, as insurance companies (like other financial entities) are not always in a position to negotiate contractual provisions with ICT providers, and so the contract tends to take the form of a standard term agreement. As one of the main goals of the proposal in this area is to address the asymmetrical contractual relationships between financial entities and third-party providers, it is important that the burden on individual entities is not such that it prevents them from making use of certain service providers or puts them at a disadvantage vis-à-vis non-EU entities, hampering the competitiveness of the European financial industry. For example, on-site audit and inspection rights (**Article 27.2.i)** will be very tough to obtain contractually and costly to execute for both financial entities and third-party providers. In fact, by stating the requirements under **Article 27.2** as minimum requirements, it is unclear how the principle of proportionality could be applied to less sensitive ICT transactions. It should be clarified that these requirements are only minimum requirements for ICT services for critical or important functions (eg, regulatory notification of change of data location in **Article 27.2.b**).

As regards **Article 27.1**, it does not make sense to require the agreement between the financial entity and the ICT third-party service provider to be contained in one written document. Complex outsourcing agreements can comprise over 1000 pages and are often split into sub-documents to manage the agreement effectively. Forcing such agreements into one document would be counterproductive.

In light of **Articles 28-39**, there should be a provision in A**rticle 27** stating that its obligations will not be enforceable until the oversight framework is established and fully operational.

Lastly, it is strongly encouraged that the obligation of the ICT third-party service provider to fully cooperate with the competent authorities arises directly from the regulation, not from the contract.

- **Oversight framework of critical ICT third-party service providers (Articles 28-39)**

Insurance Europe strongly supports the proposed union oversight framework for monitoring of critical ICT third-party providers that will be identified by the ESAs based on a set of quantitative and qualitative criteria outlined in **Article 28.2**. In the area of cloud technology in particular, the insurance industry has been calling for direct supervision of cloud service providers for a long time, due to their cross-industry importance and high market share. A centralised union oversight framework offers much in terms of efficiency and is preferable to the numerous and steadily growing sector-specific requirements. To be of maximum benefit, the establishment of the oversight framework should bring a corresponding relief from the requirements for financial entities when using the critical ICT third-party service providers that fall under its scope, if the particular assurance is already provided by the framework. Direct supervision will also enable easier access to cloud solutions by removing barriers to their use, such as the requirements for on-site inspections, which are considered by insurers to be very burdensome. More widespread development and use of certification mechanisms would also greatly help financial entities to make use of ICT and cloud solutions. In this regard, the ENISA certification scheme that is currently under development is to be welcomed, although direct certification by ENISA, for example, would be even more useful.

Under the proposed framework, each critical ICT TPP will be appointed a Lead Overseer (EBA, ESMA or EIOPA), depending on whether the total value of assets of financial entities making use of the services of that critical ICT third-party service provider represents more than half the value of the total assets of all financial entities making use of the services of the critical ICT third-party service provider, as evidenced by the consolidated balance sheets, or the individual balance sheets where balance sheets are not consolidated, of those financial entities. In the context of the insurance industry, Insurance Europe points to the potential need for a modification of EIOPA's mandate to enable it to perform the duties of a Lead Overseer.

The requirement laid down in **Article 28.9** regarding ICT third-party providers from third countries should be removed, as it implies that the individual financial entity alone must determine the criticality of the service providers it uses, whereas this is the responsibility of the supervisory authorities. Without reasonable justification, this also restricts the individual entity's freedom of contract. It is also unlikely that a sufficient selection of providers based within the EU will always be available for use in all cases. Furthermore, it is not clear whether this would impact "ICT sub-contractors established in a third country" as well (as per **Article 26.2**).

- **Follow-up by competent authorities (Article 37)**

According to **Article 37.3**, compliance by critical ICT third-party service providers with recommendations issued to them by Lead Overseers is not mandatory, and competent authorities shall monitor whether financial entities take into account the risks identified in the recommendations to the ICT third-party service providers and may require financial entities to temporarily suspend ICT services until the identified risks have been addressed. It is the ICT third-party service provider that should be responsible for exploring possible means of addressing the identified risks, however, since they are best placed to do so. This should not be a mere recommendation, but an enforceable obligation.

- **CHAPTER VI — Information-sharing arrangement (Article 40)**

To raise awareness of ICT risk, minimise its spread and support financial entities' defensive capabilities and threat-detection techniques, the DORA allows financial entities to set up arrangements to exchange cyber-threat information and intelligence among themselves. While Insurance Europe welcomes this provision, it is not clear what effect (if any) this may have, ie, will the EU provide support to such initiatives with guidelines, templates etc.? Insurance Europe would also be in favour of the creation of a database for storing this information at EU level, which would be particularly helpful in terms of risk assessment.

- **CHAPTER VII — Competent authorities (Article 41-49)**

The competent authorities as outlined in Article 30 of the Solvency II Directive will be responsible for the compliance of (re)insurers with the requirements of the DORA. Insurance Europe supports maintaining the current well-functioning insurance supervision architecture, which involves direct supervision by national competent authorities alone.

- **Financial cross-border exercises, communication and cooperation (Article 43)**

One of the major impediments to cross-sectoral and cross-border testing exercises is the reputational issues associated with sharing the results of such exercises, since these results could affect an organisation's relationship both with its supervisor and with its peers. The success of any exercise is therefore conditional on it being carried out on an anonymous or pseudonymous basis. Other impediments to establishing these exercises include: the degree of fragmentation of both information-collecting and information-sharing practices both across different financial sectors and across different jurisdictions; and the lack of a common taxonomy on cyber risk, which may complicate the development of streamlined reporting templates.

- **Publication of administrative penalties (Article 48)**

Article 48 requires that the identity of the responsible persons be published in the event of a sanction, but Insurance Europe does not consider this to be necessary in general, aside from certain justified exceptional cases. Because of the considerable effects of such publication, a reverse design to that proposed in the text would be more proportionate - also taking into account the personal rights of those affected.

- **CHAPTER IX — Transitional and final provisions (Articles 51-56)**

- **Entry into force and application (Article 56)**

The general implementation period of 12 months is too short to allow financial entities to implement the far-reaching requirements proposed under the DORA. As already envisaged for **Articles 23 and 24**, the timeline should be extended to 36 months.

- **CHAPTER II — ICT risk management**
  - **Article 4.2** Tasks of the management body (*comment: it is not the role of the management body to define the details of ICT risk management arrangements. This should rather be left to the ICT security function*)
    - **(d)** Approval and regular review of an ICT Business Continuity Policy" and an "ICT Disaster Recovery Plan"
    - **(e)** Approval and regular review of an "ICT audit plan"
    - **(g)** Approval and regular review of a policy on arrangements regarding the use of ICT services provided by ICT third-party service providers
  - **Article 5.6** Review of the ICT risk management framework at least once a year, following a major incident, or following supervisory instruction (*comment: to ensure proportional implementation, regular reviews should be sufficient)*
  - **Article 5.7** Audit of the ICT risk management framework (*comment: the wording suggests regular audits by external ICT experts, but this would be disproportionately cost-intensive)*
  - **Article 5.9** Development of a "Digital Resilience Strategy"
    - **(g)** A "holistic ICT multi-vendor strategy" (*comment: for smaller companies, the effort required to implement such a strategy would detract from its added value*)
    - **(h)** The implementation of "digital operational resilience testing"
    - **(i)** A "communication strategy in case of ICT-related incidents"
  - **Article 8.4.a** Development and documentation of an "information security policy"
  - **Article 8.4.b** Requirement for the implementation of automated mechanisms to isolate affected information assets in case of cyber-attacks; **Article 10.3** Independent review of the "ICT Disaster Recovery Plan"
  - **Article 10.5.1** At least annual tests of the "ICT Business Continuity Policy" and the "ICT Disaster Recovery Plan"
  - **Article 10.9:** Requirement to report all costs and losses caused by ICT disruptions and ICT-related incidents (*comment: this should be limited to major disruptions/incidents)*
  - **Article 13.1** Development of "communication plans"
  - **Article 14.d** Development of a "human resources policy"

- **CHAPTER IV — Digital operational resilience testing**
  - **Article 21.4** Requirement that tests be undertaken by independent parties (*comment: operational teams that maintain the security systems must be involved in testing since they will be required to intervene in a real-life incident. Only the evaluation of the effectiveness of the tests should be independent)*
  - **Article 23.1** makes reference to §4 for the identification of financial entities required to conduct TLPTs. §4 mentions §6 of Art.23 which does not exist.

- **CHAPTER V — Managing of ICT third-party risk**
  - **Article 25.3** Development and regular review of a "strategy on ICT third-party risk"
  - **Article 25.9** Development of "exit plans" and "transition plans"