Insurance Ireland's

Priorities

on the European Commission proposal

for

a Regulation of the European Parliament and the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) 600/2014 and (EU) 909/2014

(DORA)

EU Transparency Register ID: 978587826097-61

Paul Holohan
Manager Operational Planning and Reporting
p) +353 1 6447 783
e) paul.holohan@insuranceireland.eu

Florian Wimber
Head of European Affairs and International Insurance
p) +32 493 963623
e) florian.wimber@insuranceireland.eu

About us

Insurance Ireland is the representative organisation for the insurance sector in Ireland.

Ireland is a thriving global hub for insurance, reinsurance and InsurTechs. Ireland's insurance market is the sixth largest in the EU, and our Reinsurance market is the second largest. Our members represent around 95% of the companies operating in the Irish market, making Insurance Ireland a strong leadership voice for the sector.

Insurance Ireland members are progressive, innovative and inclusive, providing competitive and sustainable products and services to customers and businesses across the Life and Pensions, General, Health, Reinsurance sectors in Ireland and across the globe.

In Ireland, our members pay more than €13bn in claims annually and safeguard the financial future of customers through €112.3bn of life and pensions savings. Our members contribute €1.6bn annually to the Irish Exchequer and employ 28,000 people in high skilled careers.

The role of Insurance Ireland is to advocate on behalf of our members with policymakers and regulators in Ireland, Europe and Internationally; to promote the value that our members create for individuals, the economy and society; and to help customers understand insurance products and services so that they can make informed choices.

Insurance Ireland advocates for 135 member firms serving 25m customers in Ireland and globally across 110 countries, delivering peace of mind to individuals, households and businesses, and providing a firm foundation to the economic life of the country.

Insurance Ireland

Dublin Office
Insurance Centre
5 Harbourmaster Place, IFSC
Dublin 1, D01 E7E8

Brussels Office
Rue du Champ de Mars 23,
B-1050 Ixelles

1. Introduction

On 2nd October, the European Commission (EC) launched a consultation on a proposal for a Regulation of the European Parliament and the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) 600/2014 and (EU) 909/2014 (hereafter: ***DORA***). The initiative is part of the EC's Digital Finance Package and addresses the cyber resilience of the financial sector. Operational resilience and cybersecurity are central elements for the insurance industry, particularly in Ireland. Ireland is an international hub for financial services and technology. The insurance industry supports its customers along the full value chain of insurance and not only with the provision of cover. A sound and sensitive risk management and mitigation starts with the awareness for the risk, the individual preparedness of insurance clients and supporting clients in taking protective measures against potential threats, improving resilience to risks and, finally, providing insurance cover.

Therefore, it was a strategic and logical decision that the insurance industry was actively involved in the discussion on a digital operational resilience framework for financial services (now the DORA) from the beginning. The industry called for a proportionate and risk-based approach to strengthening the cyber resilience of financial institutions.

This paper identifies the main priorities of the Irish insurance industry on DORA.

2. General Comments

<u>Alignment</u>

Already at the beginning of the discussions about a operational resilience and cybersecurity framework, the industry emphasises the importance of alignment between the various ongoing initiatives in this area and the potential overlap and duplication with existing requirements, in particular the insurance supervisory regime Solvency II and the guidelines of the European Insurance and Occupational Pensions Authority (EIOPA) on outsourcing to cloud service providers and its guidelines on Information and Communication Technologies (ICT) security and governance.

Cyber security is an issue that is of major importance to the European and Irish insurance sector. Insurance Ireland and its members fully support the envisaged goal of strengthening the ICT resilience of the financial sector. However, we believe that this will only be achieved through the implementation of a single and consistent regime. Many requirements in the DORA proposal are covered by EIOPA's ICT Guidelines, which the European insurance sector will be required to have implemented by July 2021.

<u>Proportionality</u>

DORA will apply to a very broad range of financial services entities in the EU, including (re)insurers and intermediaries. (**Article 2 DORA**). The proposed rules do not go beyond what is necessary in order to achieve the objectives of the proposal. We welcome the recognition that there are significant differences in size, business profiles or exposures to digital risks between the companies in the scope of the DORA proposal. Nonetheless a stringent approach towards the proportionate application of DORA is indispensable, to encourage growth and innovation in the financial sector and ensure its competitiveness at global level. In its current form and the level of detail required by the proposals DORA might stand contrary to these objectives. The proportionate application of the provisions is essential because different types of entities are exposed to different type 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.

Some proposals are made on a more proportionate approach, e.g. on ICT risk management, digital resilience testing, reporting of major ICT related incidents and oversight of critical ICT third party service providers (i.e. cloud services). However, a more consistent approach is necessary.

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. Clarity in this area is particular needed, as well as 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, e.g the requirements on an at least annual:

- review of the entire ICT risk management framework, an
- review of ICT risk scenarios,
- ICT risk assessment,
- test of the ICT emergency plan and the ICT disaster recovery plan as well as all critical ICT systems and applications,
- reporting obligation for all new ICT contracts, and
- the thread-led penetration testings (TLPTs), at least every three years).

Further, some of the extensive and detailed documentation requirements could be applied more proportionately, e.g. the requirement to provide a detailed report on:

- all new ICT contracts,
- ICT strategies,
- ICT framework,
- guidelines,
- emergency planning (ICT business, continuity policy, BCT),
- ICT Disaster Recovery Plan (DRP),
- documented processes and protocols.

In all these areas, more simplifications should be permitted, and a principle-based approach should be favoured over concrete detailed requirements.

One additional specific area to highlight is the application threshold of DORA. The exemption of microenterprises from requirements in certain areas is welcomed. However, due to the narrow definition of microenterprise (less than 10 employees and sales or balance sheet total of less than EUR 2 million according to Article 2 (3) of the Annex of the Recommendation 2003/261/EC), the overall impact is limited. Other (very) small companies will still be fully covered by the requirements. In this regard, Insurance Ireland suggests raising the threshold to SMEs (as defined under Annex I, Article 2 (2) of Recommendation 2003/261/EC).

Finally, we would like to underline the importance of a not purely size-based approach to proportionality. The risk-based proportionality principle of Solvency II (Article 5 of Directive 138/2009/EU) has proofed its value. The current review aims at strengthening the principle and the application of the regime proportionate to nature, scale and complexity of risks inherent in an insurers' business.

3. ICT Risk Management (Chapter II, Articles 4-14 DORA)

Insurance Ireland believes that an efficient system of governance and organisation is vital to fostering digital operational resilience. ICT risk management requirements form a set of key principles revolving around specific functions (identification, protection and prevention, detection, response and recovery, learning and evolving and communication). Therefore, we believe that it should be left to the individual company to determine the means of achieving an efficient and effective structure, whether by establishing an independent ICT risk management process within an independent ICT framework, or by supplementing ICT risk management practises in existing structures. Insurance companies already have comprehensive internal processes and guidelines for the use and outsourcing of ICT, 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 jeopardize established methods of integrated risk management and lead to unnecessary overlap, costs, and, as a result, inefficiencies in the management of ICT risk. We, therefore, consider a company-specific method of governance and organisation – which would allow for maintaining existing integrated solutions – to be more suitable, provided that a level of cyber resilience matching business needs, size and complexity (**Article 5 (1) DORA**) can be ensured.

We believe that some of the proposed requirements for ICT risk management go beyond what is necessary to achieve the identified objective of "a level of cyber resilience that matches their business needs, size and complexity" (**Article 5 (1) DORA**). The requirements overly focus on compliance rather than on how financial entities can demonstrate outcomes through a risk-based approach. Many of the 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 content of the ICT risk management framework indirectly requires the implementation of a management system aligned with the ISO/IEC 27001 standard. This standard 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) DORA**) will mean in practice. We are concerned that this provision will lead to substantial diversification across Member States.

Article 5 (5) DORA requires segmentation of ICT management functions. However, such functions within insurance companies are conclusively regulated under Directive 2009/138/EU, so it should be clarified that this Article does not require the mandatory establishment of further key functions in addition to the ones established under Solvency II.

Some of the ICT risk management requirements (**Articles 6-12 DORA**) cover procedures, e.g. change management (**Article 8 (4) (e) DORA**), that are not always regarded as best practices 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 disaster recovery plans (DRPs) after substantive changes to ICT systems (**Article 10 (5) (a) DORA**). Such a requirement is ambiguous and

can have adverse effects on risk management and drive costs, while 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 (**Article 10 (9) DORA**). We are concerned that it would place a disproportionate burden on regulated entities.

Harmonisation of ICT risk management tools, methods, processes and policies (**Article 14 DORA**)

Insurance Ireland strongly believes that digital operational regulation should be principle-based to be flexible enough to keep abreast of technological developments and emerging threats. As such, it is crucial that each entity can choose the security procedures and tools that are most effective to meet its specific risk profile according to the outcome of 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 (i.e. cannot be applied in a risk-based manner) there is a risk that investments and resources allocated to risk management will not be allocated efficiently.

We are concerned by the list of technical standards delegated to the European Supervisory Authorities (ESAs) under **Article 14 DORA** and invite the European Commission to assess the likely negative impact on innovation if DORA empowers ESAs to draft ICT management tools, methods, processes and policies in a very detailed way. Unless the mandate to the ESAs in this area is sufficiently clear, the broad provisions of **Article 14 DORA** will stifle innovation in the area of ICT in the European Union – while innovation continues elsewhere in the world. The competitiveness of the EU financial services sector is fundamental for a swift and sustainable recovery from the Covid-19 crisis and a prerequisite for the success of the Irish economy in particular. Any measures undermining the competitiveness of the EU industry at global level must be avoided.

Given that requirements in the areas listed under **Article 14 DORA** have also been covered by EIOPA's ICT Guidelines, alignment and consistency between both initiatives will be essential. European insurance companies will have to comply with these guidelines by July 2021. Any divergence will lead to unnecessary and unjustified costs.

4. ICT Related Incidents (Chapter III, Articles 15 -20 DORA)

The DORA 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.

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

It is essential that reporting of major ICT-related incidents will be centralised i.e. an incident need only be reported to one single authority. As such, reporting requirements under different pieces of legislation (e.g. DORA, GDPR) should be harmonised to avoid unnecessary duplication of efforts (e.g. the same incident reported to multiple competent authorities, in different formats and with different time periods).

Under the DORA proposal, insurers must report to their national competent authority (as per Article 41 (1) and Article 30 Directive 2019/138/EU) 'major' ICT-related security incidents that will be identified as such by materiality thresholds to be developed by the ESAs. **Article 17 (3) DORA** 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. The notification period proposed seems unrealistic from a practical perspective. Particularly the deadlines for initial notification of the incident, which **Article 17 (3) (a) DORA** requires be done "without delay", which makes little sense given that such a notification requires prior testing. Insurance Ireland suggests alignment with the GDP requirement – in within 72 hours.

In the same vein, the arbitrary value of a deadline of one week for the submission of an intermediate report (**Article 17 (3) (b) DORA**) 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) DORA** 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 DORA**, 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) DORA**, entities may also delegate reporting obligations to a service provider. A call for clarification of on which party the responsibility lies in terms of compliance with reporting requirements (timeframes etc.) is indispensable to ensure the avoidance of unnecessary compliance risk.

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

Article 19 DORA provides for the possible establishment of a single EU Hub for the centralisation of major ICT-related incident reporting. The advantages of such a hub are unclear and should be assessed and reported. On a side note, insurers would benefit from the single hub as it can assist cyber underwriters to get a better understanding of the type of risk to be insured and priced accordingly.

Insurance Ireland 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. **Article 19 DORA** makes reference to a single EU Hub for collecting this information. 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 – interoperability should be the aim rather than a duplication or replacement.

Nonetheless, 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. It is also paramount that incidents be reported in an anonymised/pseudonymised format so as to avoid reputational damage for the financial entities involved. Overall, we are of the view that national competent authorities have a better understanding of the national market and, consequently, reporting should remain at national level and only consolidated through national competent authorities.

5. Digital operational resilience testing (Chapter IV, Articles 21-24 DORA)

We welcome the risk-based approach to digital operational resilience testing outlined in **Article 21 DORA** whereby financial entities must establish, maintain and review, with due consideration to 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 V DORA** are very detailed and prescriptive. As a consequence, they are not suited to be tailored to the wide variety of risk profiles to be found across the financial sector. For example, **Article 22 DORA** requires a comprehensive test portfolio among other strict requirements (e.g. vulnerability assessment before deployment) for annual testing of all critical systems.

A more proportional alternative, and better suited to the insurance industry, is expressed in the EIOPA guidelines on ICT security and governance, where organizations need to define and implement a security testing framework and test systems based upon the business criticality and security requirements, where sufficiently skilled and independent internal testers can be utilised.

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

In this area, the DORA 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 as such according to criteria that will be determined by the ESAs (**Article 23 (4) DORA**). However, the relationship between this paragraph and **Article 23 (3) DORA** 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.

Furthermore, when identifying companies that will be required to carry out such advanced testing, it must be taken into account that TPLTs 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, and better suited to the specificities 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) DORA**, 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 upon request by the competent authority.

Finally, the implementation of some of the requirements under **Article 23 (3) DORA** 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.

6. Managing of ICT third party risk (Chapter V, Articles 25 – 39 DORA)

As the management of ICT third-party risk is an area that is already covered under other pieces of legislation (e.g. Solvency II and its delegated acts) and supervisory guidelines (e.g. 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 DORA**.

We welcome the proposal in **Chapter V DORA** to establish an oversight framework for critical ICT providers as a step into the right direction to remedying the asymmetrical relationship between financial entities and large ICT service providers. However, we believe 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 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 of DORA's scope. Including all types of ICT services in DORA's scope would make undertakings subject to burdensome requirements that seem disproportionate to the risks stemming from the ICT services that do not support critical or important operational functions or activities.

Therefore, in accordance with Article 49 Directive 2009/138/EU, 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. More clarity is required.

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

Insurance Ireland 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) DORA**. 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 cross-industry importance and high market concentration.

A centralised union oversight framework offers much in terms of efficiency and is preferable over the numerous and steadily growing sector-specific requirements. In order to be of maximum benefit, the establishment of the oversight framework should bring corresponding relief of requirements on financial entities when using the critical ICT third-party service providers that fall under its scope, to the extent that the respective 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, 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.

The requirement laid down in **Article 28 (9) DORA** regarding ICT third-party providers from third countries must be removed, as it implies that the individual financial entity alone must determine the criticality of the service providers it uses, however 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 (**Article 26 (2) DORA**). If so, it would create an impractical and burdensome requirement to identify the chain of all sub-contractors and whether they are established in a third country.

Brussels/Dublin, January 2021