Insurers must demonstrate compliance with Europe's Digital Operational Resilience Act

By establishing a uniform, sector-specific compliance framework, Dora aligns insurance firms with the operational resilience expectations already applied to other finance entities

25 Apr 2025 | **ANALYSIS**

by Konstantinos Issaias and Zaphirenia Theodoraki

The era of digital resilience as a choice is over – for the insurance sector, accountability is now the standard

As operations become increasingly digital, and reliance on data and outsourced IT services grows, information and communication technology (ICT) risks have moved to the forefront of the operational stability concerns of insurers, reinsurers and intermediaries.

These risks now extend beyond internal processes to include third-party dependencies and cyber threats that can jeopardise both service continuity and regulatory compliance.

In response, the European Union has introduced a sector-specific framework: the Digital Operational Resilience Act (Dora). Dora aims to strengthen the digital resilience of all financial entities, including insurance undertakings, by establishing uniform rules for managing ICT risks, mitigating cyber threats, and responding to ICT disruptions.

Dora complements broader horizontal legislation – most notably the NIS2 Directive, which applies across multiple critical sectors, including finance. However, Dora functions as the specialised law for the financial sector, introducing tailored obligations for insurance entities and prevailing over the more general provisions of NIS2 where overlaps exist.

NIS2 expands on the original Network and Information Systems Directive, extending its coverage to 18 critical sectors including energy, healthcare, transport, water, and finance. It aims to ensure a high and common level of cybersecurity and resilience across these essential services.

Dual framework

While NIS2 adopts a horizontal approach by setting general cybersecurity requirements and national supervisory obligations, Dora takes a sector-specific stance, addressing the financial industry's unique operational models and digital dependencies. This distinction is particularly significant for insurance companies.

Insurers must remain mindful of NIS2's overarching principles, particularly where they provide nationally classified critical services. However, in areas of overlap, Dora's sector-specific provisions take precedence. For example, Dora introduces detailed requirements for classifying and reporting ICT-related incidents – requirements that go beyond those of NIS2 and are customised for the operational dynamics of insurers and reinsurers.

In practice, this dual framework positions Dora as the primary source of compliance architecture, while NIS2 informs broader cybersecurity strategy, including inter-sector cooperation and national reporting protocols. Insurers must, therefore, align their policies with both frameworks, giving operational priority to Dora, where applicable.

In terms of how Dora impacts the insurance sector, Dora applies broadly to insurance and reinsurance undertakings, insurance intermediaries, and ancillary insurance intermediaries. It also extends to ICT service providers supporting their operations, including cloud platforms, analytics firms, and software vendors – even when located outside the EU.

Importantly, Dora applies proportionality, considering the size, business model, and risk profile of each entity. Microenterprises (those with fewer than 10 employees and annual turnover or balance sheet totals below €2m) benefit from scaled-down obligations. However, no entity is too small to be a cyber target, and all must implement a core ICT risk-management framework.

For the insurance industry, where operations depend on safeguarding sensitive data and fulfilling a duty of care to policyholders, the integrity of ICT systems is not merely an operational issue, but a reputational and regulatory one.

Risk management

Under Dora, insurers must establish a comprehensive ICT risk management framework, approved and regularly reviewed by senior management. This includes: defining a clear digital operational resilience strategy; monitoring ICT systems in real time; and maintaining crisis communication plans for clients and stakeholders.

Dora also defines the criteria by which insurers must record and classify ICT-related incidents, including significant cyber threats. For incidents deemed "major", Dora mandates a three-stage reporting process to the competent authority: initial notification, intermediate update, and final report – each within prescribed timeframes.

This structured approach exceeds the general requirements under NIS2, enabling insurance supervisors to identify emerging systemic risks and coordinate responses more effectively.

To ensure that resilience is not just documented but validated, insurers must test their ICT systems and controls regularly. These tests may range from internal audits to threat-led penetration testing for larger or systemically important entities.

This reflects a shift from reactive compliance to continuous validation, aligning insurance with evolving best practices in the banking and investment sectors.

The insurance sector is increasingly dependent on outsourcing, particularly for cloud services, data processing, and AI-driven analytics. Dora introduces binding requirements for managing ICT third-party risk, including: maintaining a register of ICT contracts; conducting pre-contractual due diligence; and incorporating mandatory clauses related to security, service continuity, and regulatory access.

Crucially, Dora empowers supervisory authorities to designate certain ICT providers as "critical", placing them under direct regulatory oversight. This provision, absent in NIS2, is particularly significant for insurers who depend on large-scale vendors to manage claims, underwriting, or policyholder data.

Intelligence sharing

Dora also encourages the voluntary exchange of cyber-threat intelligence between financial entities. For insurers, this offers the potential to build collective defence mechanisms against advanced threats, although participation remains optional at this stage.

The insurance sector has voiced concerns about the compliance burden Dora may impose, particularly on smaller insurers and intermediaries – many of whom are small enterprises with limited staff and no dedicated ICT resources.

On November 15, 2024, Eiopa issued an opinion addressing this issue in the context of the ongoing Solvency II review. If proposed Solvency II reforms raise inclusion thresholds, many small and medium-sized insurers could be excluded from its scope. Whether similar flexibility will be reflected in Dora's application remains to be seen, especially ahead of the 2026 reforms.

Ongoing uncertainty also persists around the definition and scope of "ICT third-party providers," particularly where services blur the line between technology and regulated financial functions. While the European Supervisory Authorities (ESAs) have published technical standards to guide firms, grey areas remain, especially around cloud-based underwriting platforms and cross-border data services.

Dora marks a pivotal shift in how the insurance sector manages cyber and ICT risk. By establishing a uniform, sector-specific compliance framework, Dora aligns insurance firms with the operational resilience expectations already applied to other finance entities, while accommodating the unique structural characteristics of the insurance sector.

At the same time, the interaction between Dora and NIS2 highlights the layered nature of Europe's digital resilience regime: Dora provides the granular, sector-specific obligations, while NIS2 offers a strategic, horizontal framework for inter-sector resilience and national coordination.

With the regulatory application date of January 17, 2025 now passed, insurance entities have moved from preparation to execution. Boards and senior management must now ensure demonstrable compliance with Dora's requirements: robust ICT governance, third-party oversight, resilience testing, and continuous incident reporting.

The era of digital resilience as a choice is over; for the insurance sector, accountability is now the standard.

Konstantinos Issaias is a partner, and Zaphirenia Theodoraki is a senior associate at KG Law Firm, a member of Global Insurance Law Connect