Cyber threats, insurance and DORA

Using DORA as a risk mitigation instrument

Eamonn Phelan, FSAI, CERA
Dennis Sieg, DAV
Hauke Stier

Milliman

Insurers today face a dual exposure to cyber risk as both targets of cyber threats and providers of cyber coverage. With the rise of digitalisation, the insurance sector must navigate an increasingly complex landscape of diverse cyber risks, including malicious attacks and non-malicious incidents that can result in significant financial losses. Regulatory frameworks, such as the Digital Operational Resilience Act (DORA), add another layer of compliance challenges on the one hand, whilst offering a useful, and structured, approach to managing cyber risks on the other. In this paper, we show that DORA can serve as a valuable guide in the field of cyber insurance, extending beyond the financial sector. By implementing strict policy conditions guided by DORA, cyber insurers can ensure that their clients adopt good cyber risk management practices. In this way, insurers can help their clients manage their own risk exposure whilst effectively managing and reducing the volatility in claims experience.

Introduction

In February 2023, the financial world received a stark reminder of its digital vulnerabilities when ION, a major trading services provider, was struck by a ransomware attack. For a few tense days, some of the world's largest banks and brokerages found themselves reverting to manual spreadsheets to record trades—an almost unthinkable throwback in today's automated markets.

The ongoing digital revolution presents great opportunities. However, failing to keep pace with developments also carries increased risks. Cyber-related threats are pervasive and have increased significantly in recent years. According to the 2024 report of the German Federal Office for Information Security (BSI) on the state of IT security in Germany[1], the threat level "*is still worrying and that it is up to us to improve it*."[2]. Incidents such as the ones above highlight the urgent need for financial institutions to strengthen their internal defences and the management of external software partners to ensure that a single breach does not cascade into widespread operational turmoil.

But the nature of these threats continues to grow more diverse. They often comprise malicious attacks, such as ransomware, phishing and hacking. However, non-malicious incidents, such as system failures, accidental data exposure or even physical damage to IT infrastructure, can also lead to serious consequences. For instance, in 2024, a global IT outage triggered by an error in a CrowdStrike update affected millions of Windows systems globally. Parametrix[3] estimated a total loss of more than USD 5.4 billion in the US alone. Only 10%–20% of the financial losses were covered by cyber insurance due to low policy limits and large deductibles.

1. Federal Office for Information Security (BSI). (2024, October). The state of IT security in Germany in 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2024.pdf?__blob=publicationFile&v=7.
2. Ibid., page 7
3. Parametrix. (2024). CrowdStrike´s impact on the Fortune 500: An impact analysis. https://cdn.prod.website-files.com/66f518fd44a840ad8d3d68cc/673ec8f01114d8c6d1497ee6_CrowdStrikes%20Impact%20on%20the%20Fortune%20500_%202024%20_Parametrix%20Analysis.pdf.

However, financial consequences do not arise only from these incidents themselves. Insurance companies are also subject to reputational risks and regulatory challenges. Within the European Union, DORA[4], which entered into force on January 17, 2025, establishes a comprehensive set of guidelines to strengthen the operational resilience of all entities in the financial sector. DORA harmonises the regulatory framework for financial entities, creating alignment where there was none before. For example, in Germany, there were different regulations for insurance companies (VAIT[5]) and banks (BAIT[6]). DORA replaces these regulations and sets different priorities in some areas, such as operational stability and third-party provider risk management. On the one hand, this creates a supportive framework. Disregarding it, on the other hand, can result in substantial fines, thereby exacerbating the economic impact of cyber threats.

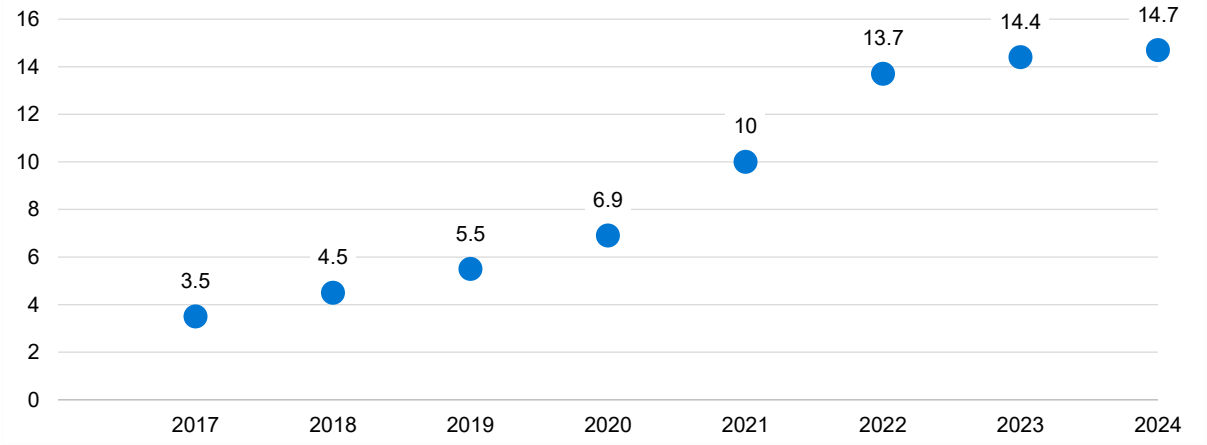
As the insurance industry is not only a target of cyberattacks but also a provider of cyber insurance coverage, this highlights the necessity for companies to manage these risks effectively. Cyber insurance, as a key risk management tool, is becoming increasingly important. As attacks become more frequent, costly and challenging, cyber insurance plays a crucial role in mitigating financial losses, enhancing organisational resilience and fostering market stability. Thus, the cyber insurance market is expected to grow significantly and become increasingly competitive.

In the next section, we provide a snapshot of the current state of the cyber insurance market and examine how the regulatory framework introduced by DORA complements and reinforces cyber risk management practices even beyond the financial sector.

Cyber insurance market

The cyber insurance market has expanded rapidly in recent years, driven by factors such as the increased frequency and severity of cyberattacks and greater awareness of the financial and operational consequences of cyberattacks. Compared to the US, which is the largest cyber insurance market in the world, Europe's cyber insurance market is still in its early stages of development.

FIGURE 1: GLOBAL CYBER INSURANCE PREMIUM IN BN USD



Source: Adapted from Swiss Re. https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/cyber-insurance-growth-shift.html

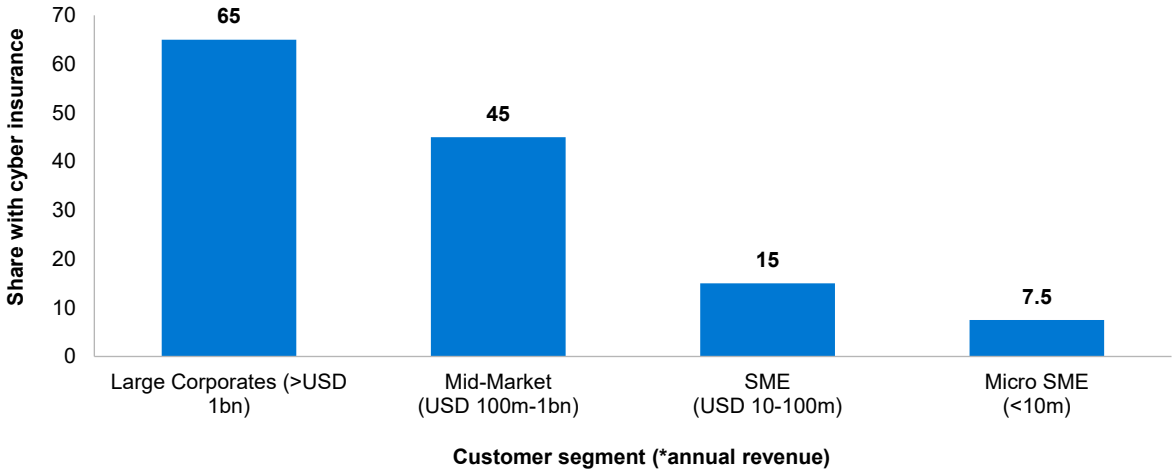
According to Swiss Re[7], global cyber insurance premiums reached USD 14.7 billion in 2024. North America dominates the market, accounting for 66% of global premiums. Europe and Asia/Oceania account for 21% and 10% of global premiums, respectively. After years of steep growth before 2022, growing market competition (offset by improving underwriting results) has resulted in lower growth rates of around 5%–10% per year. Munich

4. EUR-Lex. (2022, December 27). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022. European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.
5. BaFin. (2022, March 3). Rundschreiben 10/2018 (VA): Versicherungsaufsichtliche Anforderungen an die IT (VAIT). https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1810_vait_va_Aktualisierung_2022.html.
6. BaFin. (2024, December 16). Rundschreiben 10/2017 (BA): Bankaufsichtliche Anforderungen an die IT (BAIT). https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html.
7. Swiss Re. (2025, September 3). Shifting cyber insurance growth into the next gear. https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/cyber-insurance-growth-shift.html.

Re, in its "Cyber Insurance - Risks and Trends" report[8] forecasts a return to higher growth rates and expects the cyber insurance market to double by 2030, with Europe taking a larger share of the total market. Munich Re even estimates that less than 5%, and potentially as little as 1%, of cyber risk exposure is currently insured[9], highlighting the huge potential for growth.

Although most large corporations have cyber insurance, less than 20% of companies with annual revenues of less than $100 million do, according to Swiss Re. Despite having limited cyber know-how and a tight insurance budget, this segment offers enormous potential. Small and medium-sized enterprises account for approximately 90% of all businesses worldwide.

FIGURE 2: SHARE OF COMPANIES WITH CYBER INSURANCE



Source: Adapted from Marsh. https://www.marsh.com/de/services/cyber-risk/insights/cyber-claims-report-2025.html.

According to the Marsh report, "The Evolution of Cyber Claims in Europe"[10], cyber claim notifications increased by 61% in 2024 (43% excluding the CrowdStrike event). Notably, non-malicious incidents played a substantial role, accounting for 28% of all notifications in 2024. Although claim notifications surged in many other industries in 2024, financial institutions saw a significant decrease of approximately one-third, indicating an increased resilience within the financial sector. One significant factor in this improvement may have been the DORA regulation, which was published in January 2023, with an implementation deadline of January 17, 2025.

Accordingly, a self-assessment on cybersecurity conducted by Marsh showed that financial institutions already demonstrate a higher cyber maturity level than any other industry. It is already evident that the improvements in the financial sector are having an impact on other sectors.

Improved collaboration between IT, security and risk management has led to the integration of insurance requirements into incident response plans. Companies are showing increased awareness of the value of cyber support, which has encouraged more timely reporting. This shift has prompted even precautionary notifications to insurers, regardless of whether incidents result in losses exceeding policy deductibles.

There are already indications that measures such as the integration of insurance requirements into incident response plans are having a positive effect. As reported by IBM[11], the global average cost of a data breach in 2025 was USD 4.44 million, which is a 9% decrease compared to 2024 and thus the first reduction in years.

8. Munich Re. (2025, April 3). Cyber insurance: Risks and trends. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html.

9. Wells, K. (2025, October 17). Closing cyber protection gap a critical societal responsibility: Munich Re. Reinsurance News. https://www.reinsurancene.ws/closing-cyber-protection-gap-a-critical-societal-responsibility-munich-re/.

10. Marsh. (2025, May 15). The Evolution of Cyber Claims in Europe. https://www.marsh.com/de/services/cyber-risk/insights/cyber-claims-report-2025.html.

11. IBM. (2025). Cost of a Data Breach Report 2025. https://www.ibm.com/downloads/documents/de-de/137a3e32273ed1f5.

INSURANCE POLICY CONDITIONS

For the purposes of this paper, we have focused on the German cyber insurance market and analysed publicly available policy documents from major German insurers, as well as the standard cyber insurance policy conditions published by the German Insurance Association (GDV)[12]. As the policy conditions that we reviewed largely align with the GDV's standard cyber insurance policy conditions published by the GDV guidelines, we refer only to these guidelines in the remainder of this section. In the appendix, we set out key aspects of the DORA regulation as they relate to cyber risk exposure and to the GDV guidelines. Our analysis showed that strict obligations are established to strengthen the resilience of the insured and to mitigate risk exposure. It is essential to dispel the notion that having cyber insurance absolves organisations of the responsibility of maintaining robust cybersecurity measures. In a highly digitised world, mere compliance is no longer enough; a proactive approach to cybersecurity remains crucial.

The GDV guidelines align quite well with the requirements under DORA, covering prevention, incident response plans and reporting of cyber events. In the next section, we provide an overview of the DORA requirements, the GDV guidelines and their relationship to each other, with a more detailed comparison in the appendix. Regarding the DORA regulation, it is important to note that all requirements are subject to the proportionality principle, which takes into account the entity's size and overall risk profile.

DORA as a risk mitigation instrument

Although DORA applies exclusively to financial entities, given the sector's heavy reliance on technology and heightened exposure to cyber risks, it can serve as a valuable benchmark or foundational framework for other industries seeking to strengthen their digital resilience.

Based on our analysis of publicly available cyber insurance policy documents, we examine the potential alignment between DORA's key requirements and cyber insurance policy conditions to assess whether regulatory compliance and cyber insurance policy requirements are aligned, helping companies to establish a solid risk management framework as required by DORA through the use of cyber insurance.

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) RISK MANAGEMENT

This requirement emphasises the need for an internal governance and control framework to manage ICT risks effectively. The management body plays a central role in this process, being responsible for defining, approving, monitoring and implementing the entire ICT risk management framework. The implementation of an ICT-related incident management system that comprises anomaly detection mechanisms, restoration and recovery policies and reporting plans is critical.

In contrast, the GDV guidelines define the management body as representatives of the policyholder, thereby making them responsible for fulfilling all contractual obligations. Policyholders are required to maintain IT security measures, including access control management, firewalls, malware protection, patch management and regular data backups.

Notably, the DORA framework and GDV guidelines are closely aligned in their emphasis on the ICT risk management and monitoring framework.

INCIDENT MANAGEMENT

DORA mandates the establishment of an effective incident management system that enables monitoring and reporting of incidents through a comprehensive framework. Financial entities must implement processes to detect, manage and notify the relevant parties of ICT-related incidents. The regulation requires systematic classification of incidents based on specified criteria, such as the number of affected clients and the duration of the incident. Major incidents require mandatory reporting to supervising authorities through a single, streamlined framework across the EU.

The above aligns well with GDV guidelines, where policyholders are typically obligated to notify insurers of incidents within 24–72 hours, provide detailed reporting within one week for third-party claims and maintain full cooperation throughout the damage assessment and mitigation processes, creating a natural mutual reinforcement between regulatory compliance and insurance coverage requirements.

12. Gesamtverband der Versicherer. (2024, February). Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber). https://www.gdv.de/resource/blob/6100/a0fed56c4947751cdc20b5206c171d98/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung-avb-cyber--data.pdf.

TESTING DIGITAL OPERATIONAL RESILIENCE, INCLUDING THREAT-LED PENETRATION TESTING (TLPT)

DORA requires financial entities to implement a comprehensive, layered testing strategy to ensure system resilience, identify vulnerabilities and evaluate the effectiveness of defensive mechanisms. This encompasses a wide range of tests (including both physical and network security assessments, vulnerability assessments, scenario-based testing, and performance testing).

In addition to those tests, DORA mandates the use of TLPT for larger firms. TLPT involves two separate teams – a so-called “Red team” which seeks to mimic a targeted, real-life attack on critical systems within the financial undertaking, and a so-called “Blue team”, which seeks to successfully defend these systems and maintain their integrity. TLPT must be conducted at least once every three years; however, supervising authorities may adjust the frequency based on the entity's risk profile.

In the GDV guidelines, policyholders are not required to conduct similar testing procedures to those mandated in DORA. Instead, they are specifically required to maintain regular, effective backup tests and recovery processes, which represent only a small portion of the testing framework in DORA.

In some cyber insurance policies, the deductibles can be reduced if certain measures, such as regular training sessions for all employees, are implemented. Accordingly, there is potential to include similar obligations regarding comprehensive testing procedures in these contracts. Since DORA already offers a comprehensive framework for testing, it can serve as a guideline in this context.

MANAGING ICT THIRD-PARTY PROVIDER RISK & MONITORING FRAMEWORK FOR CRITICAL THIRD-PARTY PROVIDERS

DORA requires financial entities to assess and monitor ICT third-party provider risks throughout the entire contract lifecycle, including pre-contract due diligence to identify dependencies, risks and costs. Contracts must stipulate incident support and exit strategies for critical functions, whereas all service agreements must be catalogued in an information register. This enables supervisory authorities to identify critical ICT providers that could pose systemic risks to the financial sector.

The lead supervisory authority has several competencies and manages incidents related to third-party providers, including information, control and supervisory audit rights. In the case of noticeable problems, the supervisory authority can make recommendations to the third-party provider or seek to terminate the contract with the service provider.

In contrast, the GDV guidelines lack clarity on how the policyholder is expected to monitor each software application or service provided by third-party entities. Instead, the GDV guidelines exclude coverage for failures caused by third-party service providers.

Hence, the GDV guidelines differ from those of DORA in this regard. However, companies in the insurance sector and beyond commonly rely on third-party software or services to manage nearly all aspects of their business. Due to this widespread reliance, third-party risk features as a key aspect of DORA. There is considerable potential to update the GDV guidelines using the comprehensive DORA framework as a guideline for third-party risk.

EXCHANGES OF INFORMATION ON CYBER RISKS AND CRITICAL INCIDENTS

DORA encourages financial entities to voluntarily share information regarding cyberattacks and ICT incidents. This collaborative approach reflects the understanding that a resilient and collaborative ecosystem is essential for maintaining a healthy and competitive financial market.

Unlike DORA, the GDV guidelines are not designed to improve the digital operational resilience of the entire financial sector and therefore do not include provisions for voluntary information exchange between entities.

Conclusion

As outlined above, DORA plays a crucial role in cybersecurity. First, insurers must enhance their own cyber resilience, which is directly impacted by DORA. However, DORA should not be viewed exclusively as a regulatory burden; it also provides essential guidance for the field of cyber insurance, extending beyond the financial sector.

By implementing strict policy conditions, cyber insurers can ensure that their clients adopt good cyber risk management practices. In this way, insurers can help their clients manage their own risk exposure whilst effectively managing and reducing the volatility of cyber claims. Our research has revealed that many existing cyber insurance policy conditions closely align with the DORA requirements regarding the key areas of ICT risk mitigation and management, as well as ICT incident detection and response, providing additional legal footing and guidance in this regard.

However, insurers' clients also have an interest in minimising the severity of incidents by responding more quickly and effectively to them, as not all losses are covered by insurance. Through effective policy conditions, DORA can provide essential guidance for policyholders to enhance their cyber resilience. By increasing overall cyber resilience, the need for blanket cyber insurance can be reduced (with more focused cover taking its place instead, if necessary). Therefore, DORA creates a solid and sustainable ecosystem for insurers and clients.

The overlap between DORA and the GDV cyber insurance requirements is not coincidental; it reflects the convergence between regulatory requirements and commercial risk management. However, there is potential for further improvement. Gaps remain in cyber insurance policies regarding third-party providers and testing procedures. Including further regulations on testing in the policy conditions could increase overall resilience and reduce volatility in claims. Additionally, given the current heavy reliance on external software solutions, there is an excellent opportunity for new developments in the area of third-party providers. This could also open up the market of small and medium-sized enterprises.

When well-executed, DORA acts as a shield in a cyber war. Although it may not eliminate cyberattacks, it not only significantly strengthens a company's defence mechanisms, making it more resilient, responsive and prepared to withstand digital threats, but it also helps with early identification of potential vulnerabilities. Detection and rapid response are key elements of a company's ability to withstand cyber threats. By enforcing high standards of operational risk governance, DORA helps reduce cyber risk exposure, not only for financial institutions but also for the broader economy through its ripple effects.

CONTACT

Eamonn Phelan
eamonn.phelan@milliman.com

Dennis Sieg
dennis.sieg@milliman.com

Hauke Stier
hauke.stier@milliman.com

Appendix

FIGURE 3: COMPARISON OF THE KEY ASPECTS OF DORA AND THE GDV GUIDELINES

DORA[13]	GDV GUIDELINES	ALIGNMENT
ICT RISK MANAGEMENT		
The management body is responsible for defining, monitoring and implementing the ICT risk management framework. Leaders must be sufficiently qualified and can be held personally accountable for an entity's failure to comply. (Art. 5).	The policyholder is represented by the management body, thereby making it responsible for fulfilling all contractual obligations.	✔
Ensure only authorised users can access information and ICT assets. Implement policies, procedures and controls to address access rights (Art. 9.4 (c)).	Differentiation of individual users and authorisation levels. Administrative access is reserved exclusively for administrators and solely for performing administrative tasks.	✔
Require authentication mechanisms (e.g., multi-factor authentication) and secure management of cryptographic keys to protect sensitive data and systems (Art. 9.4 (d)).	Technical access control with complex passwords, unique user accounts, differentiation of privileges and admin-only access for administrative functions.	✔
Organisations must implement and maintain comprehensive ICT security policies, procedures and tools that ensure resilience, continuity and availability of ICT systems. (Art. 8, 9.1).	The GDV conditions require protection against unauthorised access malware using firewalls, two-factor authentication for servers, encryption of mobile device data carriers, virus scanners, application firewalls or similarly effective measures.	✔
Organisations must have appropriate and comprehensive documented policies for patches and updates (Art. 9.4 (f)).	Organisations must have an appropriate patch management procedure that ensures the immediate installation of relevant security patches that reduce a risk to the security of the policyholder's information processing systems.	✔
Financial institutions must (at least annually) conduct a risk assessment on all legacy systems (Art. 8).	The GDV policy conditions lack clarity on this point. In some policy documents, the operation of legacy systems in an isolated network environment is required, without direct internet access and with continuous monitoring of data traffic.	✘
DORA requires mechanisms to detect anomalous activities and initiate response processes (Art. 10).	Elimination of hazardous circumstances upon insurer's request within a reasonable period is required.	✘
Undertakings must set up backup systems and restoration and recovery procedures. Backup systems shall be physically and logically segregated from the source network (Art. 12).	The GDV guidelines require at least weekly backups with physical separation of backup media. In the event of a claim, originals and duplicates must not be accessible simultaneously.	✔
INCIDENT MANAGEMENT		
Organisations shall implement a business continuity policy to quickly, appropriately and effectively respond to and resolve incidents (Art. 11).	The policyholder must take all reasonable steps to prevent and minimise the damage. In doing so, the policyholder must follow the insurer´s instructions.	✔
DORA requires transmission of information to relevant staff and external stakeholders. Major ICT-related incidents shall be reported to relevant authorities (Art. 11, 19).	The policyholder must notify the insurer of the occurrence of a loss and of any judicial proceedings immediately. Potential liabilities to a third party must be reported within one week. All information that is necessary to determine the insured event must be provided.	✔
Financial entities must submit an initial notification, an intermediate report after the status of the incident has changed significantly and a final report to relevant authorities (Art. 19).	GDV conditions require policyholders to provide the insurer with detailed and truthful damage reports and assist the insurer in assessing and settling the claim. All circumstances that are important for processing the claim must be disclosed.	✔

13. Article references in this table relates to the Digital Operational Resilience Act (European Parliament, "REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL", 2022).

DORA[13]	GDV GUIDELINES	ALIGNMENT
TESTING OF DIGITAL OPERATIONAL RESILIENCE		
Organisations must establish, maintain and review a comprehensive digital operational resilience program; that includes a range of assessments, tests, methodologies, practices and tools (Art. 24).		✗
Tests shall be conducted by independent parties at least once a year (Art. 24.6).		✗
The testing program includes vulnerability assessments and scans, network security assessments, gap analyses, physical security reviews and source code reviews (Art. 25).		✗
Large financial institutions must carry out threat-led penetration testing at least once every three years, in which the company´s critical systems are subjected to a controlled, bespoke and intelligence-led test (Art. 26).		✗
DORA requires regular testing of the backup procedures and restoration and recovery methods (Art. 12).	The policyholder must ensure that the backup and recovery process functions properly by conducting regular checks at specified intervals.	✓
MANAGEMENT OF ICT THIRD-PARTY PROVIDER RISK		
ICT third-party risk is an integral part of the overall ICT risk management framework under DORA. Financial entities remain fully responsible for regulatory compliance, regardless of use of outsourcing (Art. 28).		✗
Entities must have a third-party risk strategy and maintain updated registers of all ICT service contracts, distinguishing critical or important functions and must disclose this information if necessary (Art. 28.3).		✗
Before contracting, entities must assess the criticality of the function, conduct due diligence and evaluate risks. Only ICT third-party providers meeting required security standards may be contracted, with higher standards required for critical or important functions (Art. 28.4-5).		✗
Contracts must allow termination under specific circumstances (e.g., breach, risk issues) and financial entities must have tested exit and transition plans to ensure continuity and regulatory compliance. Contracts for critical services must include detailed service levels, contingency plans, audit rights and data recovery provisions (Art. 28, 30).		✗
DORA establishes a comprehensive oversight framework for identifying critical ICT third-party service providers based on the systemic impact of service disruptions (Ch. V Sec. II).		✗
EXCHANGE OF INFORMATION		
Financial entities are required to establish processes for learning from ICT-related incidents. To enhance the resilience of the financial sector, companies are encouraged to share information on cyber threats on a voluntary basis (Art. 45).		✗