pwc

Digital Operational Resilience Act

Laying the groundwork for digital resilience and transformation

Table of contents

Foreword

We live in an era of rapid technological change. Businesses globally are benefitting from the efficiency gains and growth brought about by digitalisation, data and AI. However, as always, new opportunities are accompanied by new challenges.

Today's digital landscape presents a complex array of risks that demand a more structured and resilient response from organisations. The Digital Operational Resilience Act (DORA) stands out not only for its breadth, but its comprehensive approach to embedding digital resilience into the core of organisational management. With more than twenty-two thousand financial entities that are directly in-scope of the regulation now, a host of ICT third-party service providers who will come in scope this year and countless other businesses who will choose to comply with some or all of the regulation, DORA is nothing short of transformative.

PwC Luxembourg's survey of financial entities is one of the first systematic inquiries into how the sector is digesting DORA. The aim of our report is to identify the challenges entities have faced in implementing this complex piece of regulation, but also the opportunities it has presented.

In looking at the hundreds of articles and paragraphs, it can be tempting to dismiss DORA as mere regulatory burden. However, we firmly believe that it has the potential to become the global gold standard for digital resilience.

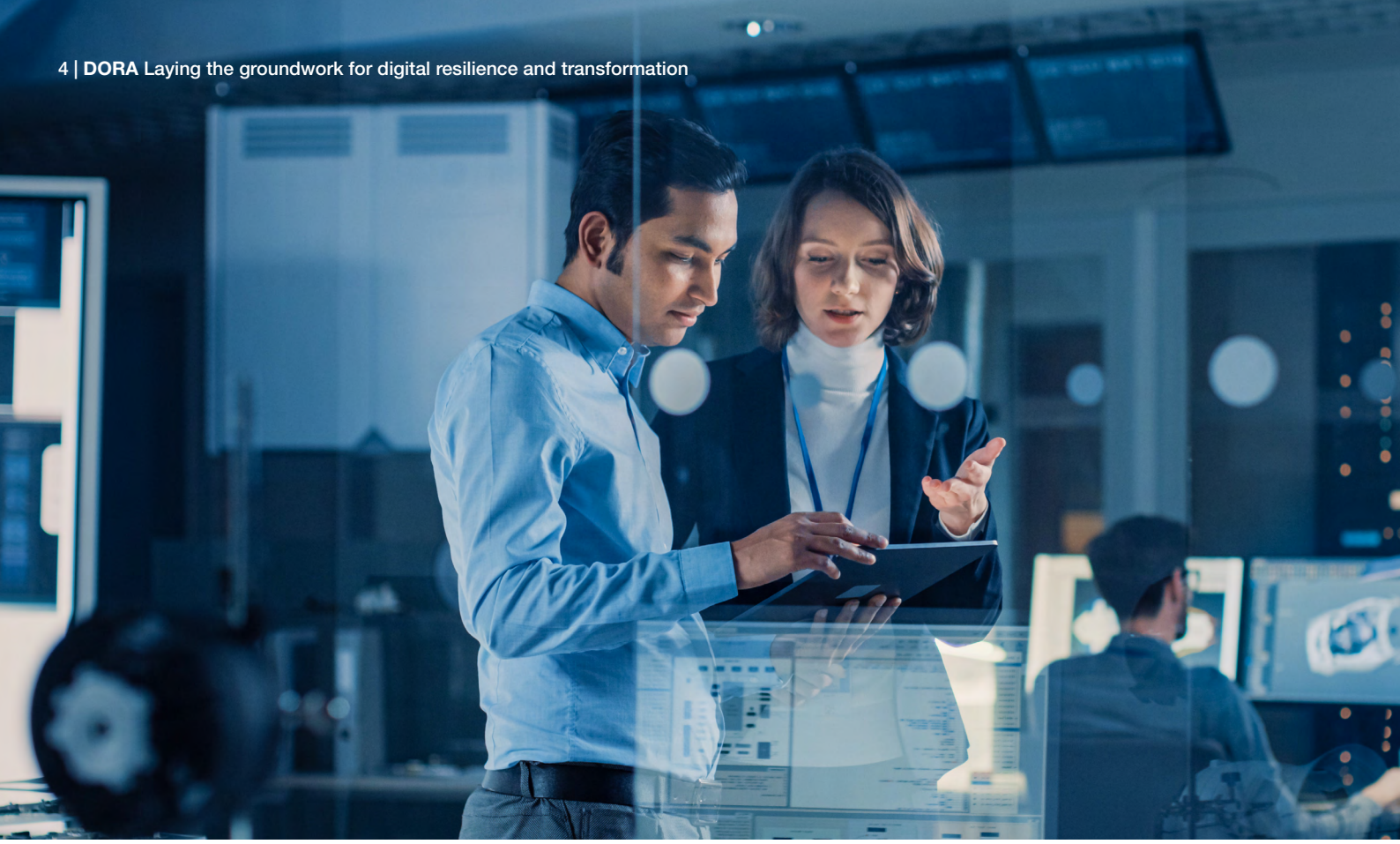
We hope this survey and its findings can act as a guide for you and your company in your digital resilience journey.

Olivier Carré

Deputy Managing Partner, Technology & Transformation Leader

Michael Horvath

Partner, Sustainability Leader & Regulatory Advisory



Executive summary

Since entering into force on 16 January 2023 and becoming applicable two years later, the EU's Digital Operational Resilience Act (DORA) has marked a pivotal shift in how financial entities and ICT third-party service providers (TPPs) across and beyond Europe approach and manage all digital-related risks.

12%

have a sound, well-designed data strategy.

49%

expect AI to reduce their cost base by at least 10%.

In fact, DORA did not emerge out of a vacuum. The financial sector's growing reliance and dependence on digital technologies and TPPs has exposed them to a whole host of new cyber threats, operational disruptions and system failures. If not adequately managed and mitigated, these risks could cause severe harms that could rapidly cascade into widespread macroeconomic and financial instability.

Therefore, DORA should be seen as a blueprint for building a robust, digitally-enabled financial sector. But it should not be seen as destination with a clear endpoint; instead, complying with its provisions is an ever-evolving journey towards laying the foundations for digital resilience and digitisation and continuously expanding on them, fuelled by the strategic use and management of data.

Published in January 2024, our first thought leadership report on the subject, **"DORA - What matters now for your business resilience"**, already made it clear: DORA is a shared responsibility across the C-suite. That initial report was an early call to action, urging the senior management of financial institutions to prepare proactively and embed digital resilience into their strategic agendas. Now, the time for preparation has passed. The focus must shift from planning to execution, and from compliance to competitive advantage.

As in-scope entities come to grips with the regulation and its numerous provisions, the senior management of financial entities and TPPs, alongside policymakers and regulators, need to keep a keen eye on several key matters:

CEOs: Act fast, think bold

84%

believe that failing to adopt AI and digitalisation within the next five years will negatively impact their business models.

DORA is accelerating structural shifts in the financial sector. Market consolidation is on the horizon, particularly among TPPs and smaller financial entities that struggle to comply with the regulation's many provisions, creating strategic openings for bold movers. But size is not the only determinant of new opportunities. Agility is essential, particularly when it comes to fully embracing AI. Failure to do so could leave existing players at risk of falling by the wayside as more nimble, AI-driven upstarts pose an existential threat.

In the January 2024 report, we highlighted the Chief Executive Officer's role in guiding strategic sourcing, defining critical business functions, and ensuring transversal implementation in the DORA implementation journey. That foundation remains essential as CEOs now must also navigate their firms' AI adoption and cost/income pressures in a more transparent, resilience-driven market.

- 84% of financial entities believe that failing to adopt AI and digitalisation within the next five years will negatively impact their business models, underscoring the urgency of transformation.
- Nearly half (49%) of respondents expect AI to reduce their cost base by at least 10%, highlighting its potential as a lever for efficiency.
- One in five (22%) view DORA as a key enabler that drives and accelerates the financial sector's digital transformation, while 30% see it as a trigger that catalysed it. While larger firms might be better equipped to utilise DORA, smaller firms still have the chance to catch up.

52%

believe DORA serves as a key enabler to the digital transformation to a "significant" or "great" extent.

45%

expect onboarding times for TPPs to increase by over 20%.

More than half expect spending

6-10

days per TPP annually.

COOs: Simplify to scale

Operational complexity is rising, and Chief Operating Officers are on the frontline. DORA introduces new oversight burdens and integration challenges that demand a disciplined approach to simplification. Onboarding TPPs is expected to become more time-consuming as oversight requirements intensify.

COOs must reassess their ICT landscapes, streamline internal processes, and embed resilience into the operational core. Cost efficiency and agility will be the defining traits of successful operating models under DORA. The earlier report emphasised the COO's role in aligning operational resilience with efficiency and long-term scalability. Today, that role has expanded to include structured data management and proactive vendor strategy as differentiators in a more regulated and digitised environment.

- Financial entities are preparing for increased friction in vendor management, with 45% of respondents expect onboarding times for TPPs to increase by over 20%.
- Oversight burdens are rising, with 56% anticipate spending 6–10 days per provider annually.
- Integration remains a major hurdle, with over half (51%) reporting challenges in embedding DORA into their existing policy and control frameworks.

55%

are in the process of developing methodologies to define critical ICT functions and assets.

66%

see GenAI as the most prominent emerging ICT risk.

CIOs: Build resilience by design

Chief Information Officers are tasked with translating regulatory expectations into robust, scalable digital infrastructure. DORA demands a clear understanding of critical ICT functions, a structured risk taxonomy, and proactive management of emerging technologies. While cloud infrastructure is central to this transformation, offering flexibility and scalability, it also introduces new risk dimensions.

CIOs must ensure that resilience is not an afterthought but a foundational design principle across systems, services, and third-party dependencies. In our January 2024 report, we positioned the CIO as the architect of ICT governance and vendor management. The new findings reinforce this role, with added urgency around harmonising fragmented systems and modernising infrastructure to meet resilience and innovation demands.

- Financial entities are still building foundational capabilities, with 55% in the process of developing methodologies to define their critical ICT functions and assets.
- 86% have implemented ICT risk taxonomies, indicating strong momentum in formalising risk governance.
- Cloud (74%) and GenAI (66%) are seen as the most prominent emerging ICT risks, reinforcing the need for CIOs to proactively manage infrastructure evolution and innovation.

CROs: Make risk measurable and strategic

For Chief Risk Officers, DORA is a call to embed ICT risk into the core of the firm's risk management strategy. Quantifying digital risk is essential for capital planning, insurance, and long-term resilience. As digital threats grow in scale and frequency, resilience investments must be framed as enablers of trust and agility, and not as sunk costs.

CROs must lead the charge in embedding quantitative-driven risk intelligence into decision-making and ensuring that resilience becomes a competitive advantage. Our first report already called on CROs to integrate ICT risks into enterprise risk management and reinforce the three lines of defence. The latest data confirms that this integration is still in progress – and more critical than ever.

- ICT risk quantification is still maturing: only 39% of financial entities have completed implementation, while 61% are still developing their frameworks.
- Investment in resilience is rising: almost three-quarters (73%) are increasing ICT security budgets.

61%

are still developing their ICT risk quantification frameworks.

73%

are increasing their ICT security budgets.

ICT Service Providers: Compete through compliance

17%

expect all their ICT TPPs to be DORA-compliant.

DORA is redrawing the boundaries of the market for ICT TPPs. Compliance has become a prerequisite for doing business with regulated entities, as TPPs that fail to meet expectations risk termination while those that align early will gain a competitive edge.

The message is clear: compliance with DORA is a commercial differentiator. TPPs must invest in transparency, governance, and resilience to remain relevant in a consolidating market.

- DORA compliance is becoming a market entry requirement: 68% of financial entities now require it for critical TPPs, and 17% extend this requirement to all providers.
- The consequences of non-compliance are real, as 26% of entities expect to terminate at least one third-party provider in 2025 due to DORA-related issues.

European policymakers & regulators: Enable innovation, focus on impact

Policymakers must ensure that DORA supports the EU's ambition to lead in AI and digital innovation. This means rethinking how the regulation fits into the broader strategy for start-ups and emerging technologies.

Regulators, meanwhile, must focus on material risks and streamline tools like the DORA register to ensure they are practical and effective. A balanced, innovation-friendly approach will be key to fostering both resilience and growth across the financial sector.

- Policymakers are encouraged to align DORA with the European Commission's strategies and action plans on AI, innovation and startups (e.g., **AI Continent Action Plan**, **Startup and Scaleup Strategy**) by creating a privileged category that allows innovative firms to access financial markets as clients.
- Regulators are urged to rethink the DORA Register and focus on material items to ensure the regulation remains practical, proportionate, and effective in its implementation.

External perspective

DORA Ecosystem

Internal perspective

CEO

Lead AI adoption and digital resilience strategy

1 Market consolidation and technological disruption are expected to reshape the financial landscape. The winners will be those who embrace AI and digital transformation swiftly—not just at scale, but with speed. DORA is more than a compliance hurdle; it's a strategic lever for growth, especially for firms ready to use it as a launchpad for reinvention.

COO

Optimise operations and ensure ICT compliance

2 COOs should focus on operational streamlining and cost discipline. DORA introduces new oversight and integration demands that require a leaner, more agile approach to managing ICT service providers.

Simplifying onboarding, tightening governance, and embedding resilience into core processes will be key to maintaining efficiency under pressure.

CIO

Manage ICT risks and protect critical technology

3 CIOs are tasked with embedding resilience into the digital architecture. This means clearly defining critical ICT assets, managing emerging risks like cloud and GenAI, and ensuring that risk taxonomies are implemented and actionable.

DORA is a chance to modernise ICT governance and future-proof the tech stack.

CRO

Quantify risks and boost cybersecurity investments

4 CROs must elevate ICT risk from a technical concern to a strategic priority. Quantifying digital risks is essential for informed capital allocation and long-term resilience.

DORA provides a framework to institutionalise this shift, transforming risk management into a driver of trust, agility, and competitive advantage.

ICT Third Party Providers

Ensure compliance to maintain client partnerships

5 For ICT service providers, DORA is a market filter. Compliance is now a competitive differentiator, not a checkbox.

Providers that proactively align with regulatory expectations will not only retain critical clients but also position themselves to capture new business in a consolidating market.

Policymakers & Regulator(s)

6 Policymakers must ensure that DORA supports Europe's ambition as a digital and AI leader. This means creating space for startups to thrive within the regulatory framework and ensuring that compliance tools like the DORA Register are focused, practical, and aligned with material risks. A balanced approach will foster both resilience and innovation.

EU policymakers:

Rethink DORA's role in the European Commission's Startup and Scaleup Strategy and AI Continent Action Plan; create a privileged category for startups to access financial markets.

Regulators:

Refocus the DORA Register on material risks, and streamline and prioritise what truly matters.

01

The EU's twin path to digital resilience and competitiveness

In today's rapidly evolving global economy, digital transformation has become a crucial driver for competitiveness. As digital technologies continue to reshape industries, organisations are faced with the imperative to embrace change in order to maintain relevance, drive growth, and enhance operational efficiency. This transformation is not solely a matter of technological adoption but also involves adapting business models, processes, and strategies to leverage the opportunities provided by the digital age. And in the European Union, this transformation is becoming more urgent than ever.

In March 2024, the European Round Table for Industry (ERT) published its Benchmarking Report which emphasised that Europe is losing ground in several areas and sectors. From technology and R&D, to infrastructure and industrial productivity, the report highlighted how the EU is lagging its competitors, and how it urgently needs a turnaround strategy to improve its competitiveness and bolster its industrial and digital strengths in order to secure its position on the global stage.[1]

The ERT's report was followed a few months later by the landmark Draghi Report, a comprehensive strategic blueprint authored by former European Central Bank president Mario Draghi which seeks to revitalise the EU's economic competitiveness through structural reforms and innovative policies. While not legally binding, the Draghi Report has greatly influenced the current Commission.[2]

Indeed, recognising that the ability of businesses and economies to adapt and innovate is crucial for long-term success in today's digital era, the European Commission has placed digital transformation at the forefront of its agenda. This commitment to fostering a digital economy is reflected in its policies, which emphasise the need for robust digital infrastructure, enhanced digital skills, and the creation of a supportive regulatory environment. These efforts are designed to equip businesses, public services, and individuals with the tools necessary to thrive in a connected, technology-driven world.

At the heart of this shift is the European Commission's Competitiveness Compass,[3] a strategic framework inspired by the Draghi report published in January 2025 which outlines the key factors for achieving and sustaining a competitive advantage in an increasingly digital world. This compass is essential for guiding organisations through the complexities of digital transformation and ensuring that they remain agile and responsive in the face of disruptive innovation and changing market dynamics.

The Competitiveness Compass points to the Cardinal Directions of movement to achieve European competitiveness. The focus on competitiveness is justified as a priority for a number of reasons:

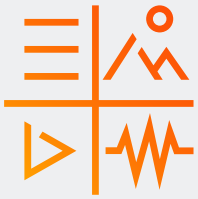
Stagnant Growth	Innovation Gap
Ageing population	Global geostrategic competition
Strategic autonomy	Defence pressures

1. European Round Table for Industry. (2024). *ERT 2024 Benchmarking Report: Europe's Competitiveness at a Critical Time.* https://www.global-counsel.com/insights/report/ert-2024-benchmarking-report-snapshot-europes-competitiveness-critical-time
2. Draghi, M. (2024). *The Future of European Competitiveness: A Competitiveness Strategy for Europe,* September 2024. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en
3. European Commission. (2025). *A Competitiveness Compass for the EU*, https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en

The Compass identifies three "Transformational Imperatives" to boost competitiveness: closing the innovation gap, creating a joint roadmap for decarbonisation and competitiveness, and reducing dependencies while increasing security. It also outlines five "Horizontal Enablers": simplifying regulations, leveraging the single market, financing through a Savings and Investments Union (SIU) and a refocused EU budget, promoting skills and quality jobs with social fairness, and better policy coordination at EU and national levels. These elements collectively aim at enhancing European competitiveness and drive sustainable economic growth.

5 horizontal enablers

Simplification	Single Market	Financing	Skills & Quality Jobs	Better Coordination



Pillar 1 – Closing the Innovation Gap

- Support startups in establishing and upscaling
- Develop and improve capital markets
- Ease talent mobility and retention
- Boost innovation and research

Pillar 2 – Decarbonisation & Competitiveness

- Integrated decarbonisation policies with industrial, economic, and trade policies
- Ensure access to affordable energy
- Strengthen the business case for a clean transition, including circular business models
- Boost competitiveness

Pillar 3 – Reducing excessive dependencies and increasing security

- Develop policies, partnerships, and investments to ensure economic security, resilience, and strategic interests
- Strengthen the defence industry
- Improve preparedness

However, competitiveness is not necessarily about deregulation or reducing oversight to foster business growth. Instead, it involves creating a robust and resilient framework where risk management, security, and regulatory standards work in tandem with innovation and growth. In fact, the European Commission has emphasised that achieving competitiveness must also come hand-in-hand with high standards for digital resilience and security.

As part of its broader agenda to strengthen digital resilience, the Commission has introduced initiatives like the Digital Operational Resilience Act (DORA). Designed to safeguard the financial sector, DORA ensures that financial entities can withstand and recover from disruptions stemming from information and communication technologies (ICT). This initiative is a key component of the Commission's Digital Finance Package, which aims to modernise the EU financial sector for the digital age. The Package seeks to remove fragmentation, enable interoperable digital identities, create a common European financial data space, and improve cross-border payment efficiency.

DORA specifically operationalises the 'digital resilience' pillar of this Package by harmonising ICT risk management requirements, establishing mandatory incident reporting, detailing resilience testing programmes and ICT risk management in relation to ICT service providers and its underbelly, the ICT services supply chain. As such, DORA is integral to any digitalisation effort, providing the foundation for a secure, resilient digital future in the financial sector.

ICT Governance

1. **Management body's responsibilities**
2. **ICT Risk Control Function**
3. **ICT audit function**
4. **Oversight role for ICT services providers**
5. **ICT knowledge and skills**

ICT Risk Management Framework

1. **Digital Operational Resilience Strategy**
2. **Business and Operational Mapping**
   (Functions – ICT assets – Information assets)
3. **ICT Risk Methodology**
   (Risk taxonomy, Identification, Assessment, Register)
4. **DORA required tools, processes and policies for mitigating ICT risk**
   - ICT asset management
   - ICT security management (incl. data/network/access rights)
   - ICT project and change management framework
   - ICT incident management
   - ICT business continuity management
5. **ICT Reporting**

ICT Incident Reporting

1. **Detection of incident**
   - In-house
   - Intra-group services providers
   - 3rd party services providers
2. **Classification of Major ICT incident**
   (DORA criteria and thresholds)
3. **Reporting to the Competent authority**
   - Initial notification
   - Intermediate report
   - Final report

Digital Operational Resilience Testing

1. **Testing Framework**
   - Testing Scope and Program
   - Testing methodologies
   - Requirements for tester
   - Testing Report
   - Testing requirements on 3rd party services providers*
2. **Advanced testing framework -**
   Threat-led penetration testing (TLPT) **

* This is not specific required however as per the art.8 the in-scope entities should also have an overview on the 3RD party services providers therefore the testing requirement should also be applied when relevant.

**TLPT framework is required upon the Competent Authority's notification (DORA art.26 §8)

Management of ICT 3rd Party Risk

1. **ICT third party risk strategy and ICT concentration risk**
2. **Classification of ICT services providers**
   (DORA definition)
3. **Identification of ICT services providers supporting critical functions**
4. **Pre-contractual requirements**
   - Due diligence
   - Conflict of interest assessment
   - Risk assessment
   - Contractual arrangements
   - Exit Strategy

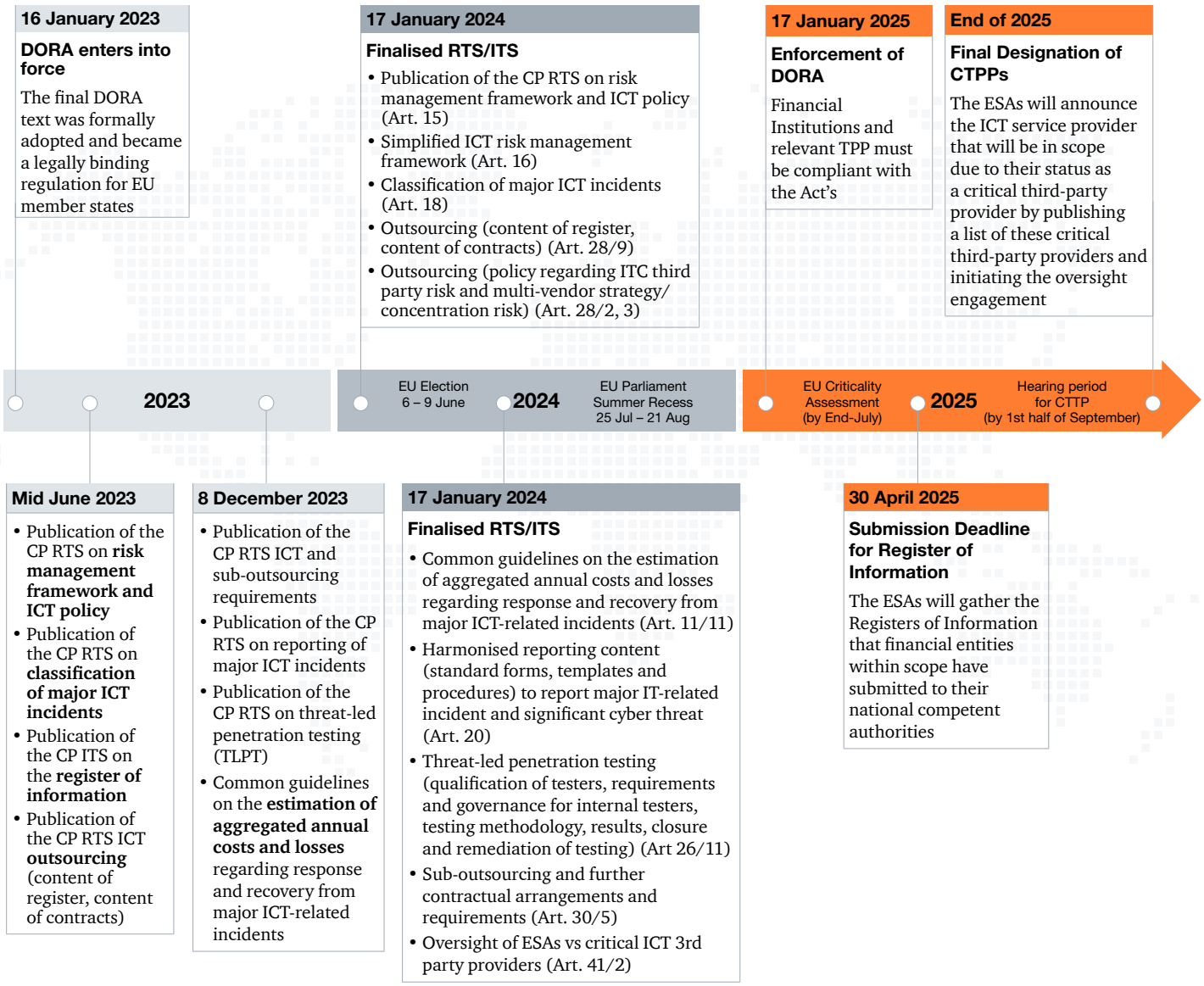
   Including sub-outsourcing
5. **ICT services provider monitoring**
   (Sub-contracting critical function)
6. **ICT Services Provider Register**

More than

22,000

EU regulated financial entities have to be compliant with DORA

Since 17 January 2025, more than 22,000 EU regulated financial entities have to be compliant with DORA. This marks a pivotal shift – not merely in compliance expectations, but in how financial institutions must structurally and operationally manage their digital ecosystems. The implications of DORA extend well beyond internal systems, as the regulation is having knock-on effects for ICT service providers supporting regulated financial entities. Given their role as critical enablers of financial operations, these service providers now play an integral part in the resilience of the financial industry.



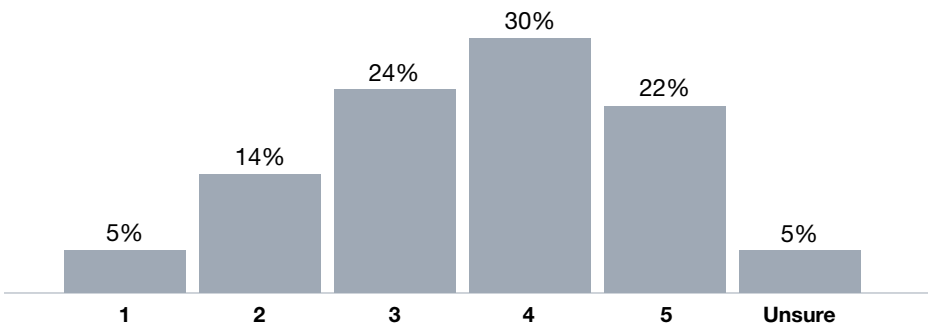
30%

believe DORA is a trigger that has catalysed the financial sector's digital transformation.

It is a daunting task. The level of detail, organisation and expertise demanded by the regulation can be mind boggling. Yet more, DORA is not a set-it-and-forget-it exercise. It requires a fundamental rethinking of how organisations govern their data, processes, and third-party relationships. At its core, DORA is about ingraining digital resilience into the fabric of financial institutions, transforming it into an inherent business-as-usual capability.

In today's digitised financial landscape, DORA positions digital resilience as a strategic necessity, facilitating the continued effectiveness and adaptability of financial entities in an ever-changing technological environment. And the regulation is already proving transformative. Just months after coming into force, 30% of European financial entities surveyed believe that DORA is a trigger that has catalysed the financial sector's digital transformation, and 22% even see it as a key enabler of change that directly drives and accelerates digital transformation efforts.

Exhibit 1. On a scale from 1 to 5, to what extent do you think DORA serves as a key enabler or starting point for the financial sector's broader digital transformation journey?



1 – Not at all. DORA is mainly a compliance requirement, not a catalyst for transformation.

2 – Limited extent. DORA is in line with the industry's goals to evolve digitally, but it is merely in line with the current zeitgeist.

3 – Moderate extent. DORA has raised awareness and has highlighted the need for digital solutions, such as automation for data or operational checks, within the industry.

4 – Significant extent. DORA is a trigger as it has catalysed the industry's digital transformation.

5 – Great extent. DORA is a key enabler as it directly drives and accelerates the industry's digital transformation efforts.

Unsure – Uncertain how DORA fits into the industry's broader digital transformation strategy.

Note: Numbers might not add up due to rounding
Source: Global AWM & ESG Research Centre

Perceptions of DORA's potential as a driver of digital transformation may vary by entity size. Larger firms often have the capacity to view it as a strategic opportunity, while smaller entities may be more likely to approach it as a compliance obligation, reflecting differences in resources, digital maturity, and readiness to capitalise on regulatory change.

As such, DORA further hammers home one point that has become too evident in the last few years in the financial sector: size does matter, particularly when it comes to absorbing regulatory demands and associated costs.[4]

We can expect DORA to become another catalyst for M&A activities as smaller entities struggle to adequately comply with the regulation and reap its benefits, while their larger peers manage to seize the opportunities it presents. In fact, regulatory pressure is a key driver of M&A activity, as heightened compliance expectations prompt firms to reassess their operating models and pursue strategic acquisitions or divestments to remain competitive. DORA is likely to become yet another catalyst in this ongoing trend.

> "DORA is the trigger for our firm to change the way that we think about resilience, business continuity, disaster recovery and risk management […] we will need to better understand all of the concepts of resilience and weave those into the day-to-day. The foundation is there but we have some work to do.
>
> **Senior risk manager at an American asset management firm**

Digitalisation can fundamentally change a business, meaning it also fundamentally changes its risks and vulnerabilities. DORA must be seen as a starting point for organisations to streamline their processes, make more efficient use of their data, safeguard and rationalise their ICT supply chain and fully embrace the opportunities that AI offers, while being aware of evolving risks. Organisations that are not quick enough to adapt, will lose market share.

Our report on the status quo and the future of DORA looks at challenges. Challenges of implementing DORA. Challenges of ICT Risk management and the quantification of risks. Challenges with ICT providers and ICT incidents.

But our report also looks at opportunities. Opportunities to develop a culture of digital resilience. Opportunities to transform your data governance. Opportunities to streamline and simplify processes. Opportunities to update and make your IT landscape more economically viable. The report also wants to point out one necessity – firms will need to move swiftly on the opportunities brought to the foreground by AI to be able to survive and thrive in a digital-first world while balancing the emerging ICT risks.

Supplemented by a comprehensive survey of regulated financial entities in the scope of DORA across a range of countries in the European Economic Area (EEA), including Investment Firms, Alternative Investment Fund Managers (AIFMs), Credit Institutions, UCITS ManCos, Super ManCos,[5] Insurance or Reinsurance Companies, and Payment Institutions, as defined in Article 2(1) of Regulation (EU) 2022/2554, we can share observations on the status quo and a look ahead.

4. https://www.bayes.citystgeorges.ac.uk/__data/assets/pdf_file/0009/689931/1.-Regulatory-Exposure-M-and-A-synergies.pdf
5. A 'Super ManCo' is licensed as both an Alternative Investment Fund Manager and a UCITS Management Company, as defined in Article 2(1) of Regulation (EU) 2022/2554.

02

Regulatory side: how are DORA's wide definitions to be applied?

Since 17 January 2025, DORA is officially in force. This means that more than 22,000 regulated financial entities, from credit ratings agencies to investment banks, have to be in compliance.

Although the objectives are clear, the implementation process is complex. Financial entities now face the dual challenge of interpreting broad regulatory definitions and embedding resilience into their day-to-day business operations while simultaneously ensuring compliance obligations are extended across their supply chains worldwide.

One of the most imminent challenges of implementing DORA is interpreting its broad definitions. Indeed, the regulation requires in-scope entities to develop ICT risk frameworks based on self-identified *"critical or important"* ICT functions, for which good data is critical. In addition, DORA requires these entities to define their *"information assets."*

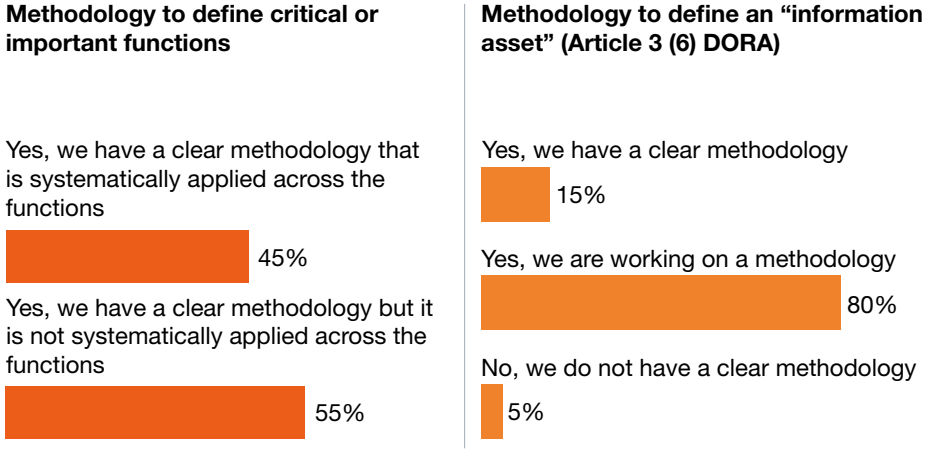
These terms are at the heart of the regulation, but applying them requires financial entities to exercise careful contextual judgement. While critical or important functions encompass any system, service or process that is vital to the ongoing operation, security and compliance of an organisation, information assets refer to any data, system or resource, tangible or intangible, worth protecting for an organisation.[6]

In our survey, we asked entities how far they had come in implementing DORA, as well as what challenges they faced and foresee facing in doing so. We found that entities had faced challenges related to the complexity of the regulation and its definitions, the timeline for implementation, recruitment and third-party management.

Findings

Nearly all entities surveyed either had or were working on a methodology to define critical or important functions and information assets. Although the majority (55%; 80%) are still in the development phase, only 5% indicated that they neither had nor were working on a methodology to define information assets.

Exhibit 2. Do you have a methodology to define your critical or important functions as well as an "information asset" (Article 3 (6) DORA)?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

6. Please refer to the Glossary at the end of the report for a full definition of both terms.

54%

consider mapping critical functions with information assets and ICT assets as the biggest DORA-related challenge they faced.

33%

have hired or plan to hire an ICT (Risk) officer and/or an ICT Third-Party/Outsourcing Officer locally.

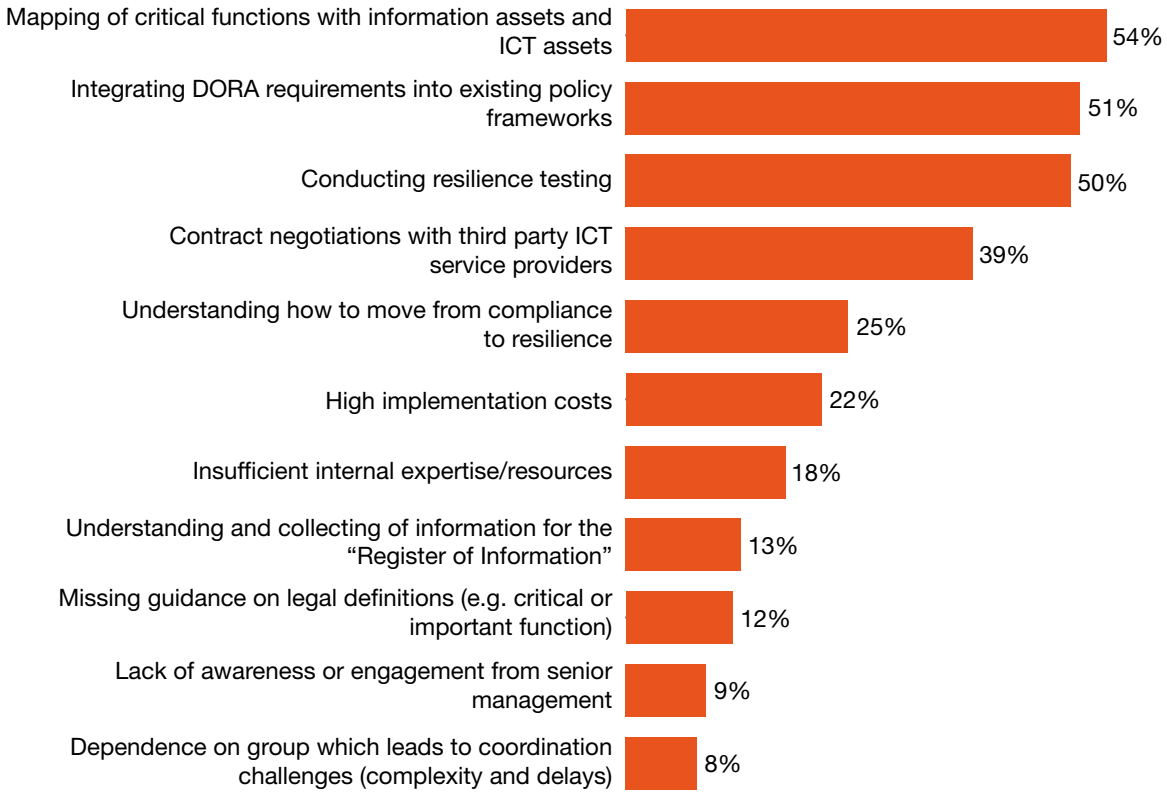
Financial entities have faced and continue to face significant challenges as regards the implementation of DORA. This should not come as a surprise, given the novelty of the threats, the complexity of the regulation and the short timeframes involved. However, teething issues are always to be expected, and the weak points revealed in this process can be taken as an opportunity to improve.

The areas in which entities faced challenges in implementing DORA are not equally distributed. We asked entities what they found the most difficult.

By far, 'Mapping of critical functions with information assets and ICT assets' as required by Article 8 of DORA (54%), 'Integrating DORA in existing policy frameworks' (51%), 'Conducting resilience testing' (50%) and 'Contract negotiations with third party ICT service providers' (39%) were rated as the most challenging aspects.

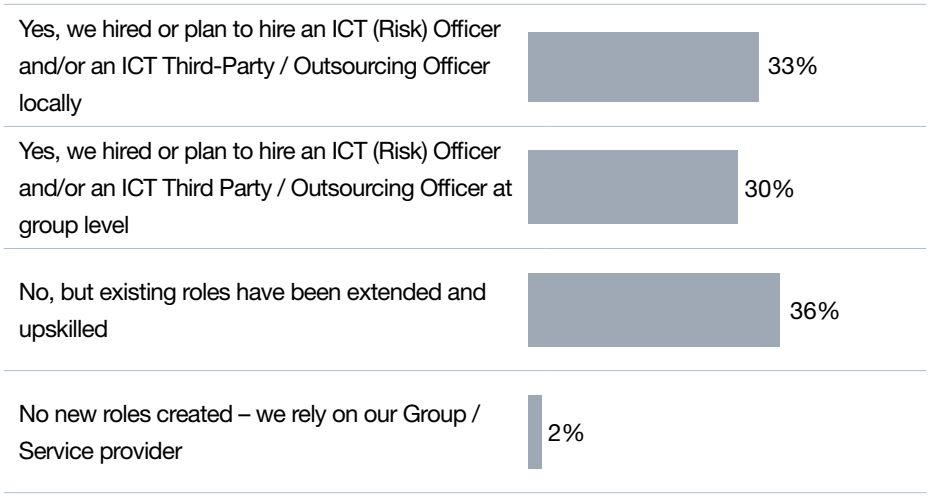
Surprisingly, the "DORA Register of Information" does not receive the notoriety that we would have expected. One reason might be the timing of the survey – March 2025 – as most problems and rejections on submissions occurred from April to May 2025.

Exhibit 3. In your opinion, what are the biggest challenges your organisation faces when it comes to DORA?



Note: Multiple choice question
Source: PwC Global AWM & ESG Research Centre

Exhibit 4. Has your organisation created or developed plans to create new roles or specialised functions dedicated to DORA?



Note: Numbers might not add up due to rounding
Source: Global AWM & ESG Research Centre

> We had to hire one new employee […] the search was pretty long and difficult because it's difficult to find someone with that profile. A person who has the right amount of ICT, risk and regulatory knowledge all together. Now we are seeing it more and more but last year it wasn't something common.

Head of ICT risk at a European asset management firm

Identifying and finding the right profile, either within the organisation or in the market, plays a crucial role in the successful implementation of DORA and the ongoing upkeep of its requirements.

As DORA needs to be implemented on a per-entity basis, local entities cannot afford to wait for group-level directives and guidance. They should consider taking on more responsibilities independently when possible, thereby enhancing their resilience. This includes finding, retaining and upskilling talent, which is becoming a critical priority for financial entities in light of DORA.

In fact, the regulation introduces a new layer of complexity that demands specialised expertise in areas such as ICT risk management, incident reporting, digital resilience testing, and third-party oversight. These are not one-off compliance tasks but recurring obligations that require sustained operational readiness. As such, financial institutions must not only identify current skill gaps but also invest in building long-term capabilities. Hiring or developing employees with the right digital resilience competencies will be essential—not just to meet DORA's initial requirements, but to embed resilience into the organisation's DNA for the future.

Whereas issues relating to ICT providers and resilience testing can be a question of time and experience, integrating DORA into an organisation's wider policy framework is an abstract challenge that can be difficult to grapple with.

Moreover, DORA also requires entities to uniformly reconsider their staffing to ensure they have the necessary skills and expertise to both be compliant and digitally resilient. As a result, it has had a major impact on hiring practices. Indeed, almost two-thirds (63%) of respondents have hired or plan to hire ICT risk staff in response to DORA, while 36% have opted to upskill existing staff. Only 2% have decided not to take any action on their staffing decisions related to DORA.

03

Operational side: what day-to-day DORA activities are practically expected?

It is postulated that, just like iron or oil before, information is the most important resource of our time. Like oil, information or data needs to be properly stored, processed and refined to be effectively exploited – a reality businesses ignore at their own peril.

Although it can be an expensive and onerous task, especially to those entities for whom data had not been a concern, systematic data collection and categorisation can bring enormous long-term benefits. Moreover, DORA also requires entities to implement certain digital resilience practices on an ongoing, business-as-usual (BaU) basis.

In our survey, we found that entities are somewhat far from reaching the stage where DORA-related processes are implemented on a BaU basis. In addition, although entities recognise the importance of data and methodology, we found that most are in the early stages of leveraging them.

Findings

Although very few entities (7%) have not yet started taking actions towards integrating their DORA-related processes and operations in BaU, equally few entities (4%) are executing all tasks and actions to reach BaU. The majority (65%) started assessing which tasks and actions are required to reach BaU stage, while close to a quarter (24%) had no problems in clearly defining the BaU tasks and actions across the organisation and will begin executing them this year.

Exhibit 5. DORA requires the integration and change of different operational processes to get to "Business as Usual" (BaU). How far are your BaU processes already?

Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

86%

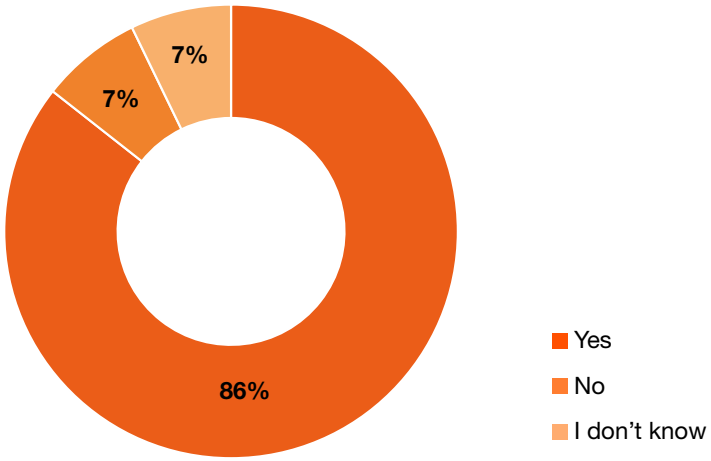
have implemented a taxonomy for ICT risks.

Smaller entities often face greater hurdles in defining and initiating their BaU activities under DORA. These challenges are largely driven by limited resources, expertise, and infrastructure – factors that tend to set them apart from larger, more mature organisations that are typically further along in their DORA implementation journey.

A strong methodology and taxonomy are essential for the successful ongoing implementation of DORA, as DORA-related functions and information assets will need to be updated on a regular basis.

The adoption of an ICT risk taxonomy is central to the effective and systematic detection and treatment of emerging threats and vulnerabilities. Entities have equally recognised the importance of a consistent taxonomy when it comes to ICT risks, as 86% have implemented such a taxonomy.

Exhibit 6. Has your organisation implemented a taxonomy for ICT risk to identify threats and vulnerabilities?

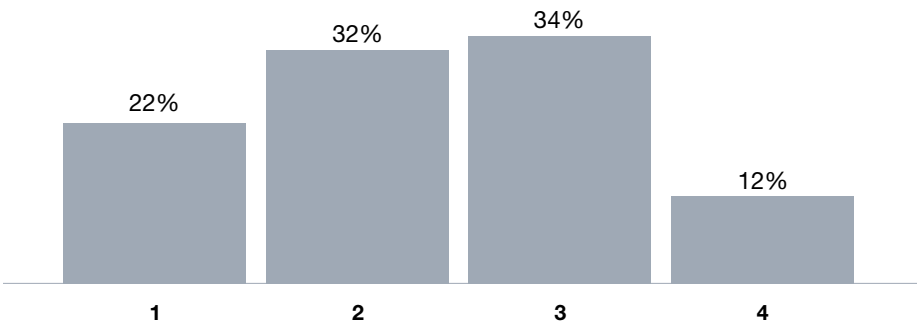


Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

But methodology and taxonomy without data are akin to a car without fuel. Data governance is essential to a successful DORA implementation as well as a successful digital transformation in general.

We found that whilst most entities have recognised the importance of data management, they are still working towards refining and maturing it. Almost half (46%) of respondents said they either have a solid or a well-designed data strategy, whilst 32% have set up some data management processes without having a comprehensive data strategy. None of the respondents identified as 'data champions' who can leverage data to be more cost-efficient than their peers, demonstrating the persistent difficulties financial entities still have with maximising their data leverage.

Exhibit 7. On a scale from 1 to 5, how would you assess the maturity of your data management and handling?



1 – Data is important, but we just started building our data management processes

2 – We have some data management processes in place, but no comprehensively designed data strategy

3 – We have a solid data strategy and are working towards improving it

4 – We have a well-designed data strategy and pushing this further in the organisation with good success

5 – Data is Gold: We are data champions and this is allows us to be more cost-efficient than others

Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

39%

already have a methodology to quantify ICT risks.

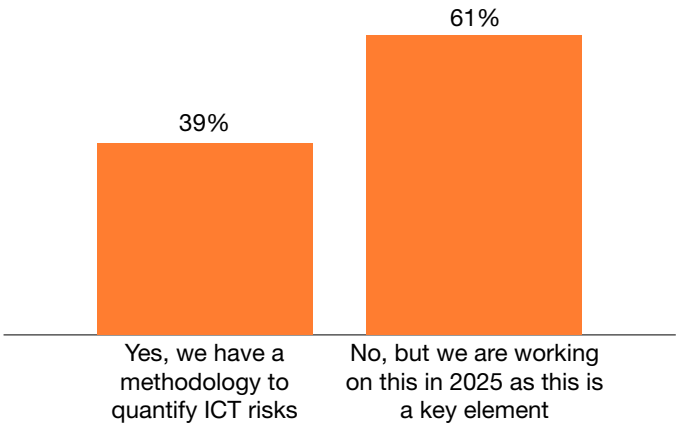
Mature data management requires significant time, expertise, and resources – conditions that are more often met by larger entities. Smaller firms, by contrast, may face greater challenges in scaling their data capabilities due to limited capacity and internal resources. This disparity not only affects compliance readiness but also adds to the broader consolidation pressure in the sector, as smaller players struggle to keep pace with increasingly data-intensive regulatory expectations.

Data management has a cross-sectional benefit to DORA and digital resilience, for example in risk quantification, which is one of the most sophisticated yet hardest to operationalise disciplines of risk management. While qualitative ICT risk assessment is possible using risk matrices or other tools, the most accurate and sustainable way to assess risk is quantitatively.

Indeed, regardless of an organisation's size, quantifying ICT risks can uncover potential savings while also providing an opportunity to operationalise the data. In fact, the data can be turned into actionable insights which enables organisations to approach ICT risks with confidence, ultimately driving long-term operational resilience and benefiting the business as a whole.

We asked entities if they have made efforts to quantify their ICT risk, and the survey results show that they have broadly recognised the value of this approach. In fact, all entities surveyed have either already implemented a methodology to quantify ICT risks (39%) or are currently working on such a methodology and expect to have it completed this year (61%).

Exhibit 8. Does your organisation quantify the ICT risks detected?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Market Research Centre

Larger entities tend to be further along in their DORA implementation, often due to more mature structures and greater resources. Smaller firms, while agile, may face steeper challenges in adapting to the regulation's complexity.

> DORA made us understand to what extent a quantitative approach could be beneficial.

Head of ICT risk at a European asset management firm

Data governance is more than a spreadsheet. It is a holistic approach to understanding how your organisation functions at a fundamental level. To be continually compliant with DORA, and for digital resilience generally, such an approach will only grow in importance. Bigger entities with more resources at hand clearly have a head start here. However, any organisation that is willing to put in the effort can still catch up or even get ahead. It can be a daunting task, but the benefits of good data governance will be felt at every level of the entity.

Quantifiable risks, quantifiable savings

Risk quantification can be difficult to implement, especially for businesses to which it has not traditionally applied. Industries like insurance have long understood its value and made it a core aspect of their business model. Not all companies will be able to benefit to quite the extent of insurance, however there are savings to be made especially in the context of cybersecurity.

- Insurance companies extensively quantify risk in order to properly allocate premiums and estimate payouts. For example, the likelihood and scale of damage due to natural disasters can be estimated in a highly accurate manner based on historical data and advanced modelling.
- One area in which the quantification of risk can create material benefits for banks is in the calculation of minimum capital requirements.

Generally, under Basel III rules, banks have two options by which to calculate their credit risk, a determinant of their minimum capital requirement. The Standardised Approach (SA) or Internal Ratings Based approach (IRB).

Under SA, banks are subject to generalised and conservative rules which tend to err on the side of caution, thus rendering high capital requirements. Under IRB, banks are permitted to use their own internal risk modelling to calculate the risk weighting of their assets, which can be much more accurate to their actual risk exposure and result in much lower capital requirements.

For illustrative purposes, let's suppose a bank holds a lot of low-risk loans on its balance sheet. Under SA, the risk of these loans is overestimated and its Minimum Tier one Capital requirement is set at €200mn. The bank then decides to hire quantitative analysts and use an IRB approach. Using more accurate internal models, the risk weighting of the loans is reduced and the bank reduces its capital requirements to €110mn, leaving €90mn surplus to invest or lend out.

Quantification of Cyber Risks

Just as credit or operational risks, cyber risks can be effectively quantified. This can range from the simple (e.g. estimating the time to restore systems after and outage) to the complex (e.g. calculating monetary cost if a system were to be compromised). If you haven't yet implemented such practices, don't worry. In our 2025 **Global Digital Trust Insights** survey of thousands of businesses globally, we found that only 15% were quantifying cyber risks to a significant degree. There's still time to get ahead of the curve, especially when building on DORA.

Cybersecurity, a more threatening landscape

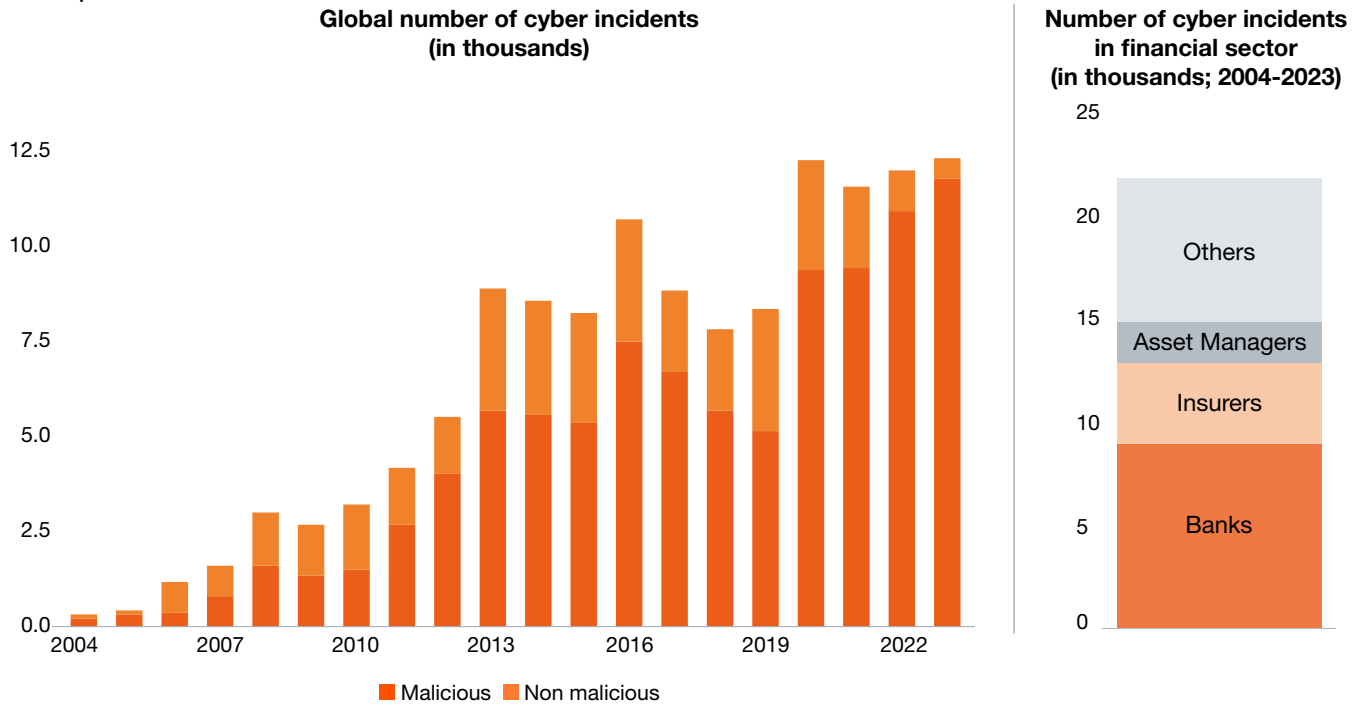
The incidence and size of cyber attacks is growing year on year, and there is no reason to believe it will slow down as criminals become more sophisticated and potential rewards become more lucrative. These attacks can take the form of simple scams carried out by individual criminals all the way up to intricate digital hostage events orchestrated by fully-fledged criminal enterprises. As custodians of highly sensitive and strategically important data, financial entities are in the crosshairs of all kinds of cyberattacks.

In response to these mounting risks, the EU has introduced legal instruments such as Directive (EU) 2022/2555[7], also known as the NIS II Directive. Designed to tighten cybersecurity requirements across critical sectors, the directive broadens the scope of regulated entities and imposes stricter risk management, incident reporting and governance standards. Malicious cyberattacks – such as extortion attempts and data breaches – have nearly doubled compared to levels seen before the COVID-19 pandemic.

The financial sector has been particularly exposed, accounting for nearly one in five incidents.[8] Within this sector, banks have been the most frequent targets, followed by insurers and asset managers, according to an IMF analysis based on Advisen data. That said, a major cyberattack on a key financial institution could pose a serious threat to macrofinancial stability by damaging trust, disrupting critical operations, and spreading through highly interconnected financial systems.[9] The financial and economic costs of such attacks can be substantial.

7. European Parliament (2022). Directive (EU) 2022/2555. 14 December 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
8. The IMF defines cyber incidents as events – malicious or not – that compromise the security of information systems or the data they handle, leading to cyber risk. This includes attacks like ransomware, data breaches, phishing, and system disruptions, while excluding privacy breaches aimed primarily at individuals.
9. IMF (2024). Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks. Chapter 3: Cyber Risk: A Growing Concern For Macrofinancial Stability, April 2024, https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024?cid=bl-com-SM2024-GFSREA2024001

Exhibit 9. Global number of cyber incidents financial sector exposure



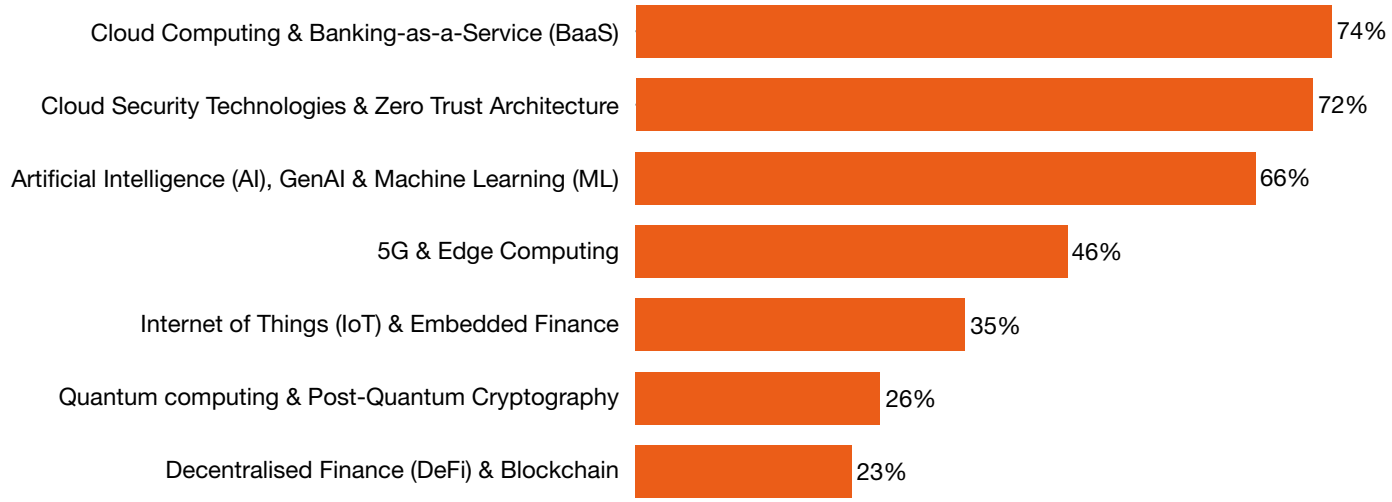
Note: Panel 1 Cyber-events are classified according to Advisen. Delayed reporting may lead to underestimation of cyber-events in more recent periods.
Source: Advisen Cyber Loss Data; Capital IQ; IMF, WEF

66%

see AI as an area with significant ICT risk potential.

As such, the evolving cybersecurity landscape also brings with it significant new risks that cannot be overlooked. When asked about the factors that will impact the industry the most, entities surveyed identified Cloud Computing and Banking-as-a-service (74%), Zero Trust Architecture (72%) and GenAI and Machine Learning (66%) as areas with significant upcoming ICT risk potential.

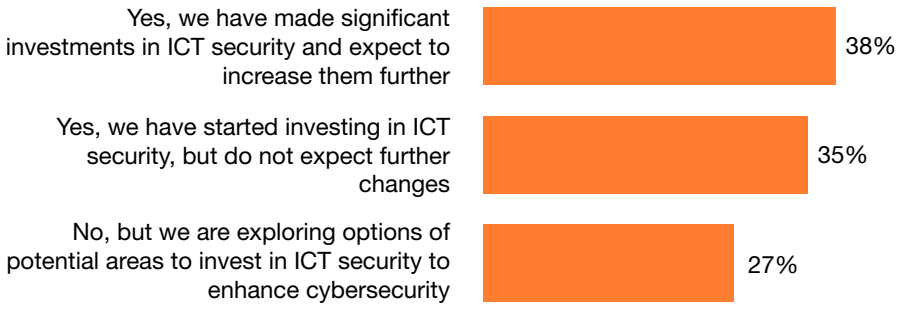
Exhibit 10. In your opinion, which factors will have the most impact on ICT risk in the coming year?



Note: Multiple choice question
Source: PwC Global AWM & ESG Market Research Centre

Accordingly, businesses are taking cyberthreats seriously. The vast majority of surveyed entities (73%) have made or plan to make investments in cybersecurity, with none of them leaving their ICT security systems unchanged.

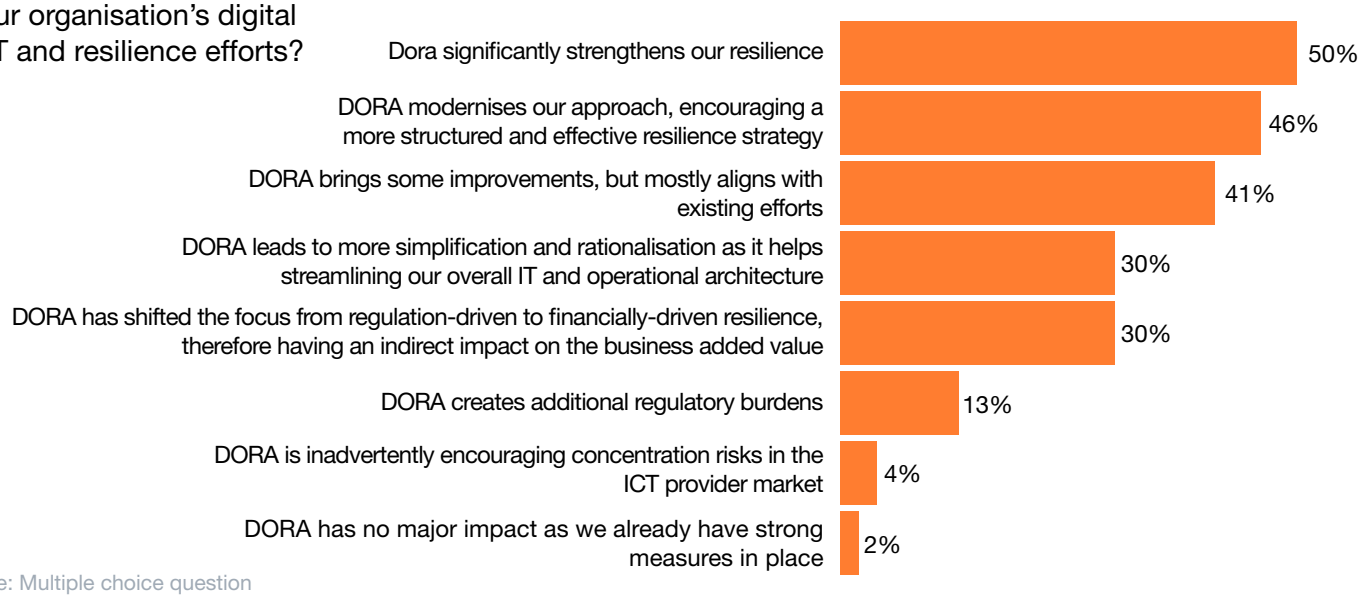
Exhibit 11. Has your organisation changed or is expected to change its investments in ICT security as a response to DORA?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

DORA appears to have been a significant enabler in this journey, with half of respondents stating that the regulation has significantly strengthened their resilience. Closely behind, 46% of respondents see DORA as a moderniser of their current approach. In general, entities seem to be pleased with the overall direction and purpose of DORA. Only 13% stated that DORA creates additional regulatory burdens and 4% thought it encourages concentration in the service provider market.

Exhibit 12. How do you expect DORA to impact your organisation's digital ICT and resilience efforts?



Note: Multiple choice question
Source: PwC Global AWM & ESG Market Research Centre

Cyberattacks: a harsh reality

Cyberattacks are no longer phishing emails or scam calls looking to make a bit of easy money. They are sophisticated and serious operations. Here are just a couple of examples of the range of forms and gravity of consequence of cyberattacks:

- In 2023, the CEO of a small bank in the United States fell victim to a sophisticated online scam. He was convinced to invest in a fraudulent investment scheme, ultimately wiring USD 47.1mn from the bank's funds to the scammers. This massive embezzlement led to the collapse of the bank, affecting both customers and shareholders. While the bank's customers were reimbursed thanks to federal insurance, about 30 local shareholders lost a combined USD 8.2mn.[10]
- On 7 May 2021, the ransomware group 'DarkSide' infiltrated and managed to gain control of the IT systems of the company that operates the largest fuel pipeline in the United States and supplies almost the entire East Coast. The disruption caused widespread fuel shortages and panic buying. To regain control of their systems, the company had to pay a hefty ransom.[11]

> "For sure, DORA was beneficial for us. We were already going towards increasing our security and digital resilience, but DORA gave us a kind of blueprint to follow.
>
> **Head of ICT risk at a European asset management firm**

10. FBI (2025). FBI recovers $8 million swindled from failed bank's small-town investors. https://www.fbi.gov/news/stories/fbi-recovers-8-million-swindled-from-failed-kansas-banks-small-town-investors
11. CISA (2023). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

04

Third-party service providers: will DORA be a disruptor?

The regulation of ICT Third-Party Service Providers (TPPs) is the lynchpin of DORA and its most challenging aspect. Within the context of a digitalised world, TPPs have become as essential to financial institutions as wood is to a carpenter. Just as a batch of rotten wood can ruin a carpenter's work, poorly managed TPPs can open up entities to serious material vulnerabilities.

Financial entities are now required to track, manage and report which of their important and critical functions are outsourced to TPPs. The registration and vetting of TPPs will be one of DORA's most important recurring tasks. Establishing a clear and repeatable process can prevent headaches down the road. Ensuring that TPPs understand what they need to deliver is just as important as having a clear understanding of what is expected of the financial entity.

In short, financial entities need to know what services they are getting and from whom they are getting them.

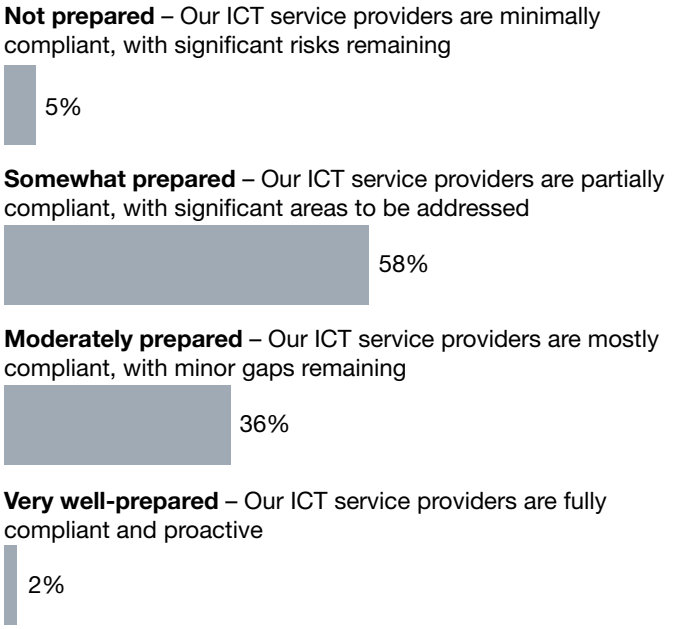
As part of their reporting requirements, entities are required to submit a 'register' of information on who their TPPs are and which functions they oversee. This register had to be submitted to European Supervisory Authorities by the 30 April 2025.[12] Based on this register, a list of 'critical' TPPs, which are responsible for a large number of critical functions over a large number of entities, will be compiled by the European Commission, expected by the end of 2025. These critical TPPs will then themselves become in-scope of DORA.

12. EBA. `The ESAs announce timeline to collect information for the designation of critical ICT third-party service providers under the Digital Operational Resilience Act`. November 15, 2024. https://www.eba.europa.eu/publications-and-media/press-releases/esas-announce-timeline-collect-information-designation-critical-ict-third-party-service-providers

Findings

There are numerous challenges resulting from the stricter regulation of TPPs imposed by DORA. More than half of the entities surveyed (58%) reported that their TPPs were only somewhat prepared for DORA, with significant gaps remaining that need to be addressed.

Exhibit 13. How would you assess the preparedness (on average) of your ICT service providers in relation to DORA?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

26%

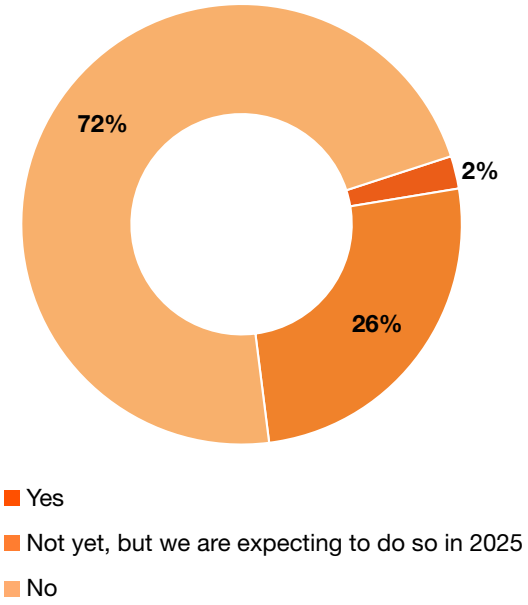
are planning to terminate an ICT service provider due to DORA-related reasons.

Crucially, TPPs who are currently *de jure* out of scope are *de facto* in-scope by virtue of handling the critical or important functions of their clients. Communicating these new requirements to these critical TPPs and why they must comply with certain DORA elements has proved especially challenging for the entities we spoke to. This fact was also borne out in the data which showed that contract negotiations was overall one of the most challenging aspects of DORA so far (see Exhibit 3).

Register and TPP compliance

Due to stricter regulation, entities have had to reorient their TPP strategy to align with regulatory expectations. Although very few entities (2%) had terminated a TPP due to DORA, we found that a quarter (26%) expected to this year. This shows that DORA has already started having a spillover effect on the way TPPs are being impacted by the regulation.

Exhibit 14. Did you terminate any ICT service providers in relation to DORA?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Market Research Centre

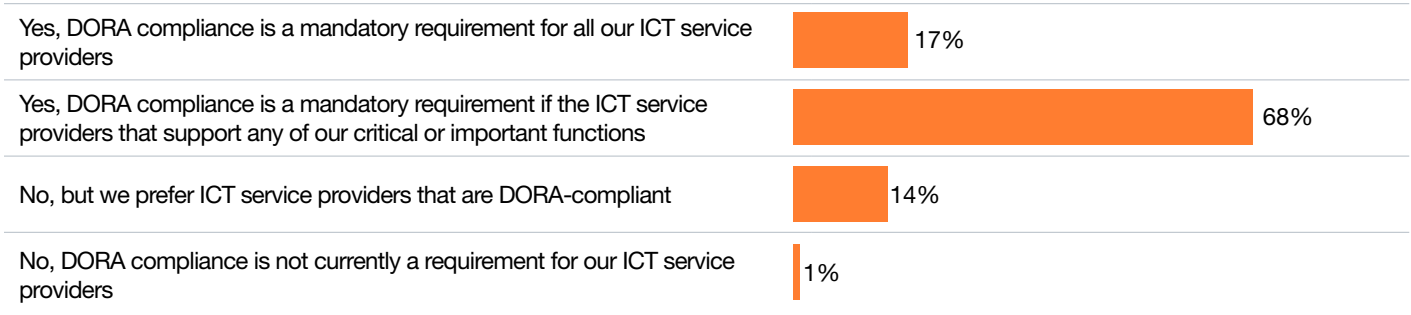
Moving forward, the majority of entities said DORA compliance would be necessary to some degree for TPPs they engage with. More than two-thirds (68%) stated that compliance with DORA is a mandatory requirement for ICT service providers that support any critical or important functions, whilst 17% even require all ICT service providers to be DORA compliant, regardless of their service.

These figures highlight the direct and potentially disruptive impact of DORA on TPPs and their business opportunities. With an increasing number of financial institutions now requiring upfront compliance in order to streamline their own DORA compliance processes, this shift could potentially impact market competition and lead to increased concentration, as only those TPPs that can meet these stringent requirements will remain viable partners.

17%

expect all ICT service providers to be DORA-compliant.

Exhibit 15. Do you require ICT service providers to be DORA-compliant before entering into a contract with them?

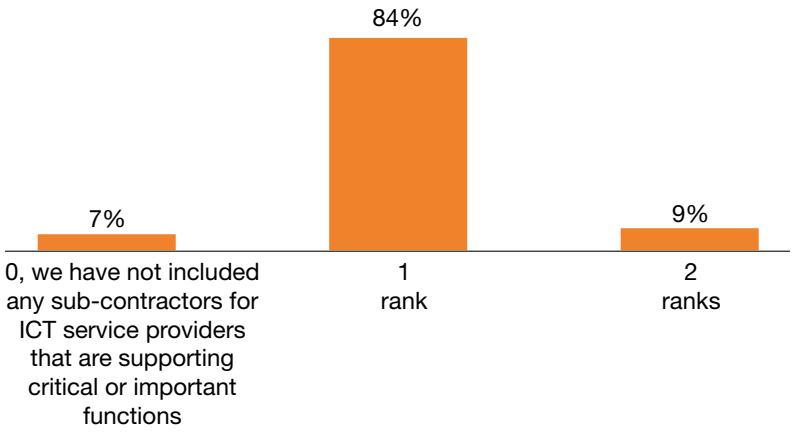


Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

Completing and submitting the information register has been identified as one of the most challenging aspects of DORA compliance for financial institutions, with the deadline for submitting the DORA register of information already passed.

An often-overlooked aspect of engagement with (and reliance on) TPPs, is the cascading web of further reliance that firms may inadvertently expose themselves to. We asked financial entities how many further 'ranks' (sub-contractors of directly engaged TPPs) they investigated. 86% of entities surveyed reported having gone through one rank beyond the TPP that supports critical or important functions, and 9% probed up to the second rank.

Exhibit 16. For an ICT service provider that is supporting critical or important functions: How many ranks AFTER the ICT service provider have you gone through in general?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Market Research Centre

> "It was really understanding what goes where, what the point of each field was, and what information should go in there to make sure we're doing it correctly. [The DORA register] was very challenging. It might have been one of the most difficult things that I've worked on in my career.
>
> **Senior risk manager at an American asset management firm.**

56%

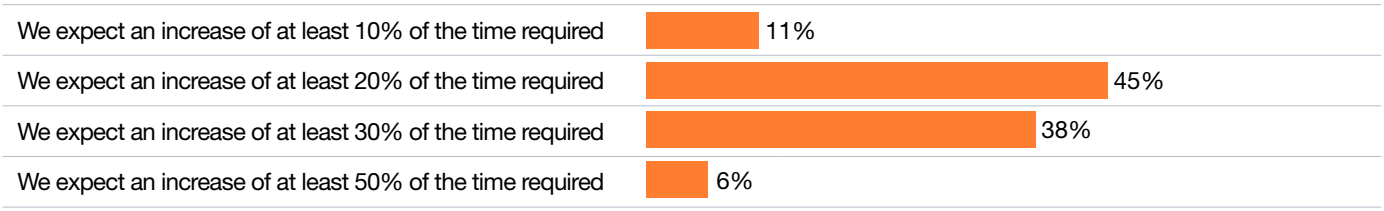
expect to allocate between 6 and 10 business days to conduct due diligence and oversight of ICT service providers.

TPP onboarding and cost

DORA has changed the time and costs associated with onboarding and retaining ICT TPPs.

Due to the enhanced requirements imposed by DORA, all entities surveyed are expecting longer selection and onboarding times for TPPs to a certain extent, with the plurality (45%) expecting an increase of at least 20% in the time required, whereas more than a third (38%) even expect a time increase of at least 30%.

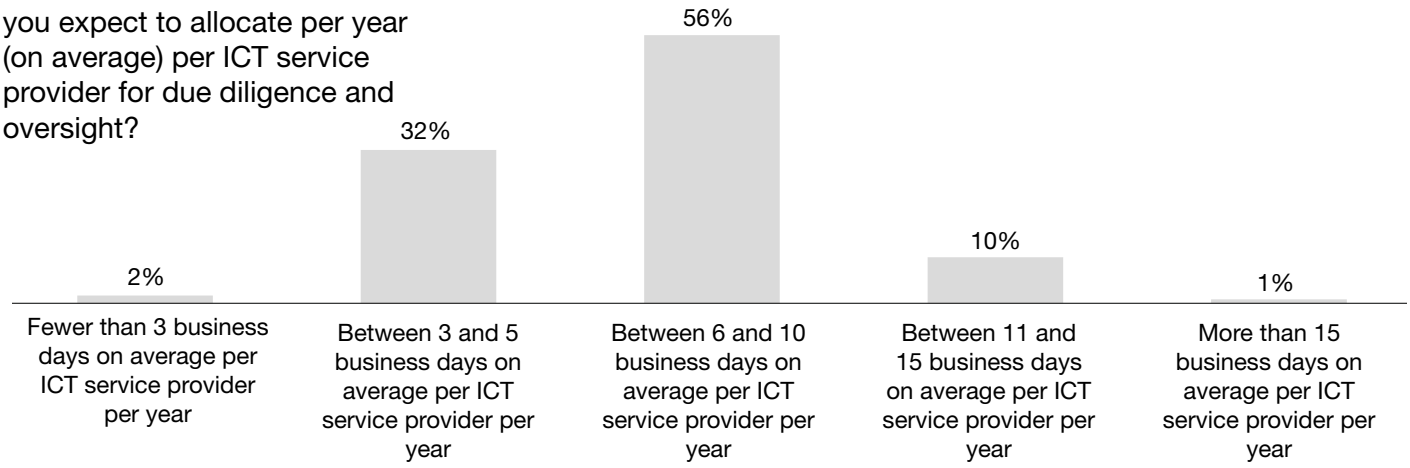
Exhibit 17. What impact do you expect DORA to have on the ICT service provider selection and onboarding process?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Market Research Centre

Conducting due diligence and oversight of existing providers also takes considerable time. More than half of the respondents (56%) expect to spend 6 to 10 days per service provider per year, with around a third (32%) estimating about 3-5 business days per year. This underscores the resource investment necessary to maintain ongoing compliance and effectively manage third-party relationships.

Exhibit 18. How much time do you expect to allocate per year (on average) per ICT service provider for due diligence and oversight?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Market Research Centre

66%

expect their ICT service provider costs to increase moderately (6-15%) over the next three years.

Entities also expect the cost associated with engaging TPPs to rise in the coming years. Whilst over the past three years, most entities (62%) experienced only a moderate increase in TPP costs, nearly a quarter (22%) foresee a material escalation in expenses over the next three years. Only 9% expect costs to remain stable.

Exhibit 19. How have your costs related to ICT service providers changed in total over the last three years and how do you expect your costs related to ICT service providers to change over the next three years?

	Change in costs over the **last** three years	Expected change in costs over the **next** three years
Remained stable (change within ±5%)	31%	9%
Moderate increase (between 6 – 15%)	62%	66%
Material increase (between 16 – 25%)	6%	22%
Significant increase (>25%)	0%	2%

Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Market Research Centre

As reflected in our findings, DORA will have a major impact on financial entities' relationships with their service providers. Not only will onboarding and prices go up in general, but existing providers will need to be continually vetted as part of ongoing digital resilience practices demanded by DORA. Furthermore, as the registers continue to come in and when the Commission designates the critically important TPPs, DORA will have a ripple effect across the entirety of the ICT service industry.

However, in the long-term, the risks incurred by poor oversight of TPPs providing critical functionality is greater than the costs associated with vetting and reporting. This is especially true of those subsidiary entities, many of which may only for the first time be getting familiar with the providers who run their entire ICT infrastructure. As the register, oversight, onboarding and other practices become integrated into entities' BaU processes, we can expect costs and lead times to stabilise.

Risks of poor TPP management

Poor knowledge of how TPPs are integrated into your organisation's processes can be devastating.

Ransomware attack

In late 2023, a major cloud computing provider to credit unions in the US, fell victim to a major ransomware hack targeting their downstream services.

As a result, more than 60 Credit Unions across the US went offline, with customers being unable to access their accounts, some for multiple weeks. Customer data was confirmed to have been compromised and the full extent and consequence of the attack has yet to be realised.

Are you aware not only of your direct service providers, but your providers' providers? And your provider's providers' providers? The ICT service supply chain can be mind-bogglingly complex, and at one end can send ripples up the chain.

Update outage

In 2024, another large cloud computing provider often used with Windows, pushed an update to their servers that caused more than eight and a half million Windows machines to crash. Although the mistake was quickly rectified, its scale caused business continuity issues for weeks or even months afterwards.

05

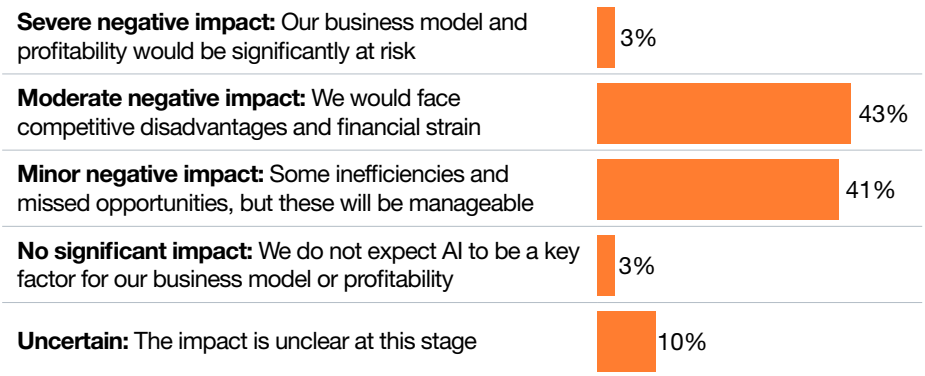
Tomorrow's world, powered by AI

Seatbelts came long after the car. The necessity of digital resilience comes as a solution to and a consequence of the new pressures introduced by the digital transformation more generally. Generative AI has recently brought an entirely new element to this transformation, alongside new risks.

DORA needs to be understood in this wider context. Digital resilience will inevitably become a topic globally, be it due to business pressures or regulation. A close cooperation between industry and regulators in Europe, alongside an understanding of the need for digital resilience to accompany digitalisation, could make DORA the gold standard globally for cybersecurity regulation. Thus, to understand the seatbelt, one needs to understand the car. We asked our survey respondents about digitalisation, digital resilience and AI.

Most entities (84%) surveyed believe not adopting AI and digitisation in the next 5 years will have a moderate to minor negative impact on their competitiveness, whilst only 3% said they expect no impact. The industry seems ripe for disruption and DORA might open the floodgates.

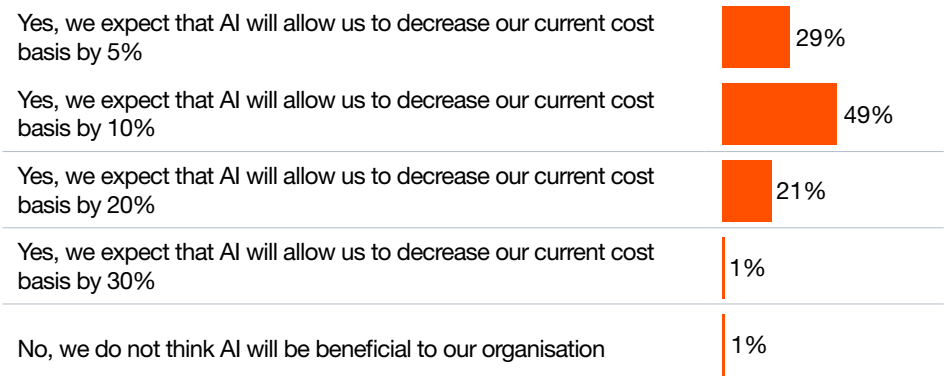
Exhibit 20. What do you think will be the impact on your business model in the next five years if your organisation does not embrace AI and digitalisation more broadly?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

Conversely, while not embracing AI may prove to be detrimental to businesses, its adoption does have its upsides, such as in terms of costs. All the companies surveyed expect to see a reduction in their cost base, with nearly half (49%) predicting a 10% reduction over the next few years as a result of AI, and more than a fifth anticipating a decrease in costs by 20%

Exhibit 21. Do you believe that AI will be a transformational force for your organisation in the coming years?



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

While size matters when it comes to absorbing regulatory costs, it is speed – particularly in adopting AI and digital capabilities – that is increasingly defining competitive advantage. If a new firm were launched today, fully digital and AI-native, many established players could quickly find themselves outpaced, which is why agility and innovation are critical. DORA may favour larger firms in terms of compliance capacity, but it is those who move fastest with AI that will shape the future of the financial sector.

AI and digitalisation are now central to the growth of any business. While the profit potential can make it tempting to adopt AI technologies quickly, often bypassing the necessary due diligence, the companies that prioritise responsible AI integration alongside rapid innovation will be the ones that thrive in the long run. Balancing both speed and responsibility will define the leaders of the AI-driven future.

06

The future of DORA and digital resilience

Sitting at north of seventy pages, DORA implementation is no mean feat. Neither is it a mean feat to avoid the growing myriads of scams, hacks, ransoms and more.

In this survey we looked at implementation and we found that most financial entities are still not fully confident in their implementation of DORA. Elements involving the management of TPPs pose particular issues as does the transition to the BaU phase.

We looked at entities data collection and processing. We found that entities understand the vital importance of data, but they are in the early stages of fully leveraging it, especially smaller companies. However, entities are enthusiastic about the possibilities of techniques like risk quantification and work is ongoing behind the scenes.

We looked at ICT service providers. We found entities rely significantly on service providers for many critical functions, leaving them open to serious vulnerabilities if the providers aren't properly managed. For the most part entities are not fully confident in their providers and moving forward, most will require their TPPs to also be DORA compliant.

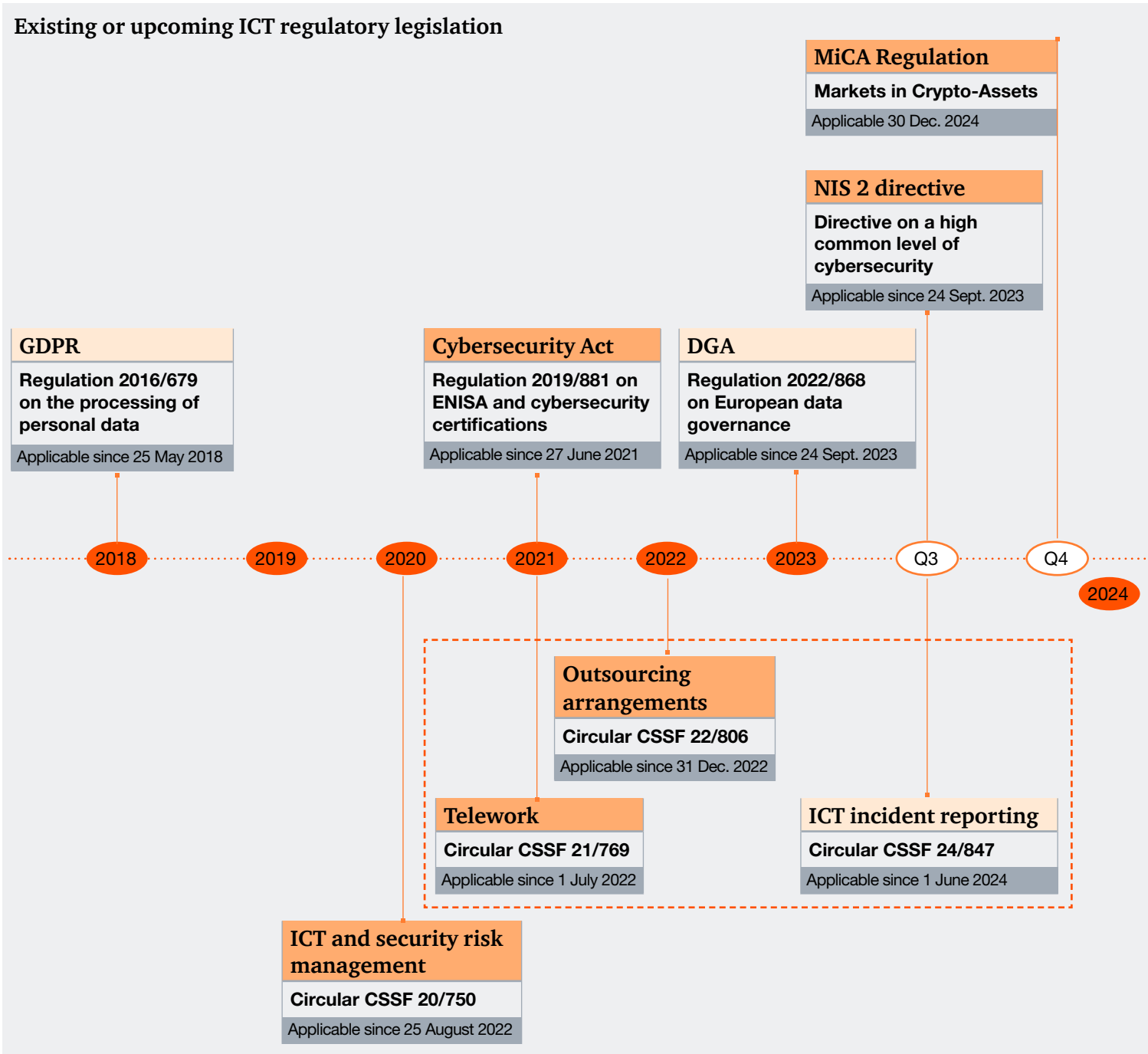
We looked at how entities are thinking about the digital transformation. We found they were enthusiastic about AI and its potential but wary of its threats. They are highly optimistic about DORA's positive impact on their digital resilience and potential within the broader context of their digital transformation.

But DORA is a difficult and expensive regulation to implement upfront. Integrating its recurring processes such as the register and vetting of TPPs will also pose an ongoing challenge. However, rather than seeing it as a sunk cost, entities should and are seeing it as a future investment, one which, if nurtured, will soon deliver daily dividends in the form of real resilience against ever-growing digital threats. As it stands, DORA is the gold standard in global cybersecurity process.

DORA is far from being an insular regulation within the financial sector. In fact, it is an integral part of an already well-established and sophisticated regulatory framework designed to meet the emerging demands of the digital transformation. ICT regulation has long been shaping the broader economy, with key pieces such as the GDPR (effective since 2018) governing the processing of personal data or the Cybersecurity Act (effective since 2021) establishing critical security standards, among others.

More recently, the European Commission published the 'Competitiveness Compass,' which introduced further initiatives to accelerate the EU's digital agenda.[13] In this context, DORA enhances and complements these existing regulations by placing emphasis on operational resilience, risk management and third-party oversight, thereby strengthening the regulatory ecosystem driving the digital trajectory of the sector.

Existing or upcoming ICT regulatory legislation

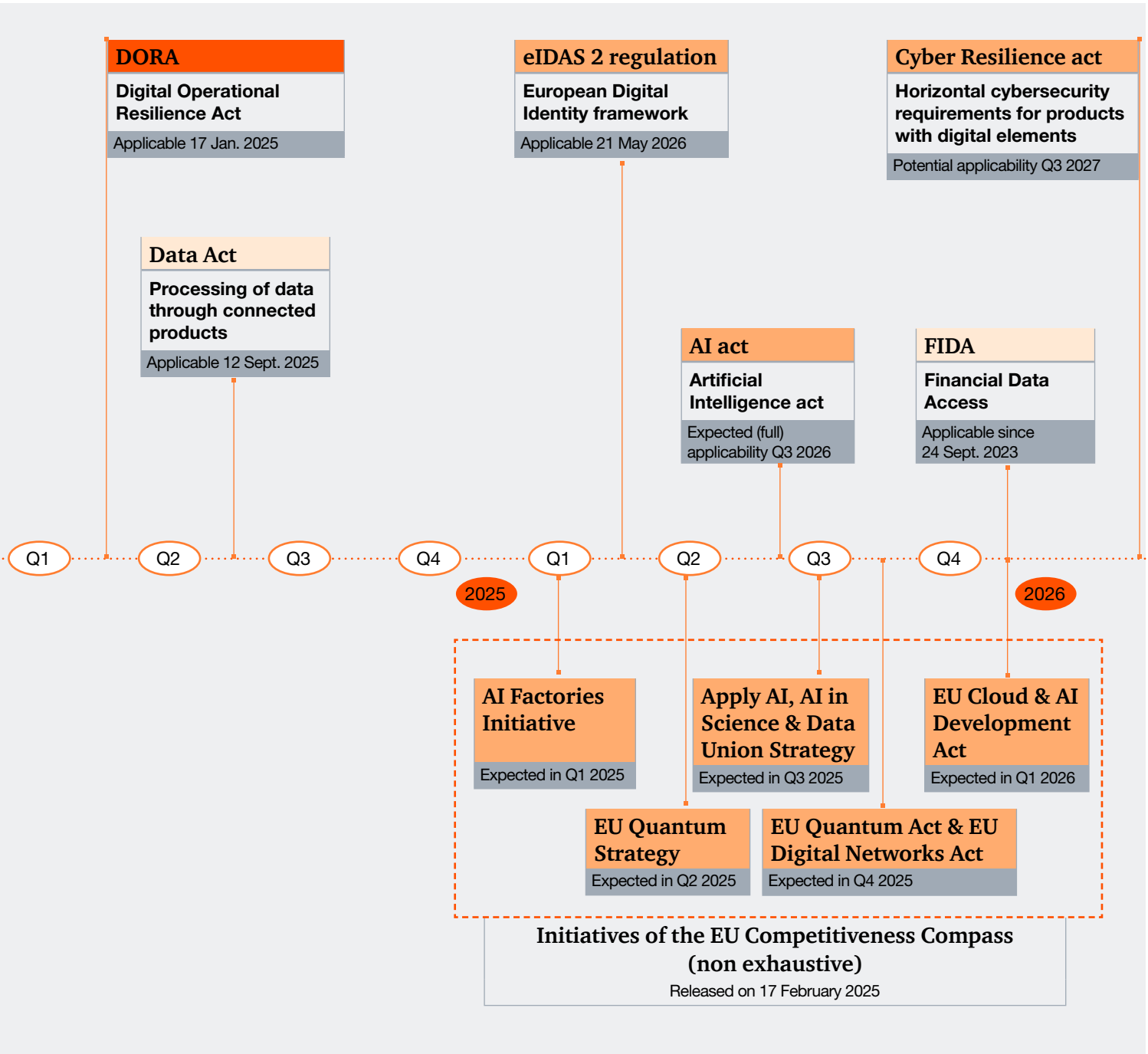


13. European Commissions. 'Digital initiatives under the Competitiveness Compass'. January 29, 2025. https://digital-strategy.ec.europa.eu/en/news/digital-initiatives-under-competitiveness-compass

An encouraging outcome of our survey is that entities are beginning to view DORA in the context of digitalisation as a whole. Many of the challenges of digitalisation – data management, ICT skills, management of externals contractors – are the same as the ones accompanying digital resilience.

These operations, and thus their risks, are inherently interlinked and codependent. Thus, for entities that want to get ahead and stay ahead, DORA should only be the first step. It is a long first step, but nonetheless the beginning of a journey. True digital resilience is more than a regulatory framework. It is a culture. It is a mindset. It is diffused through every cog and gear of an organisation.

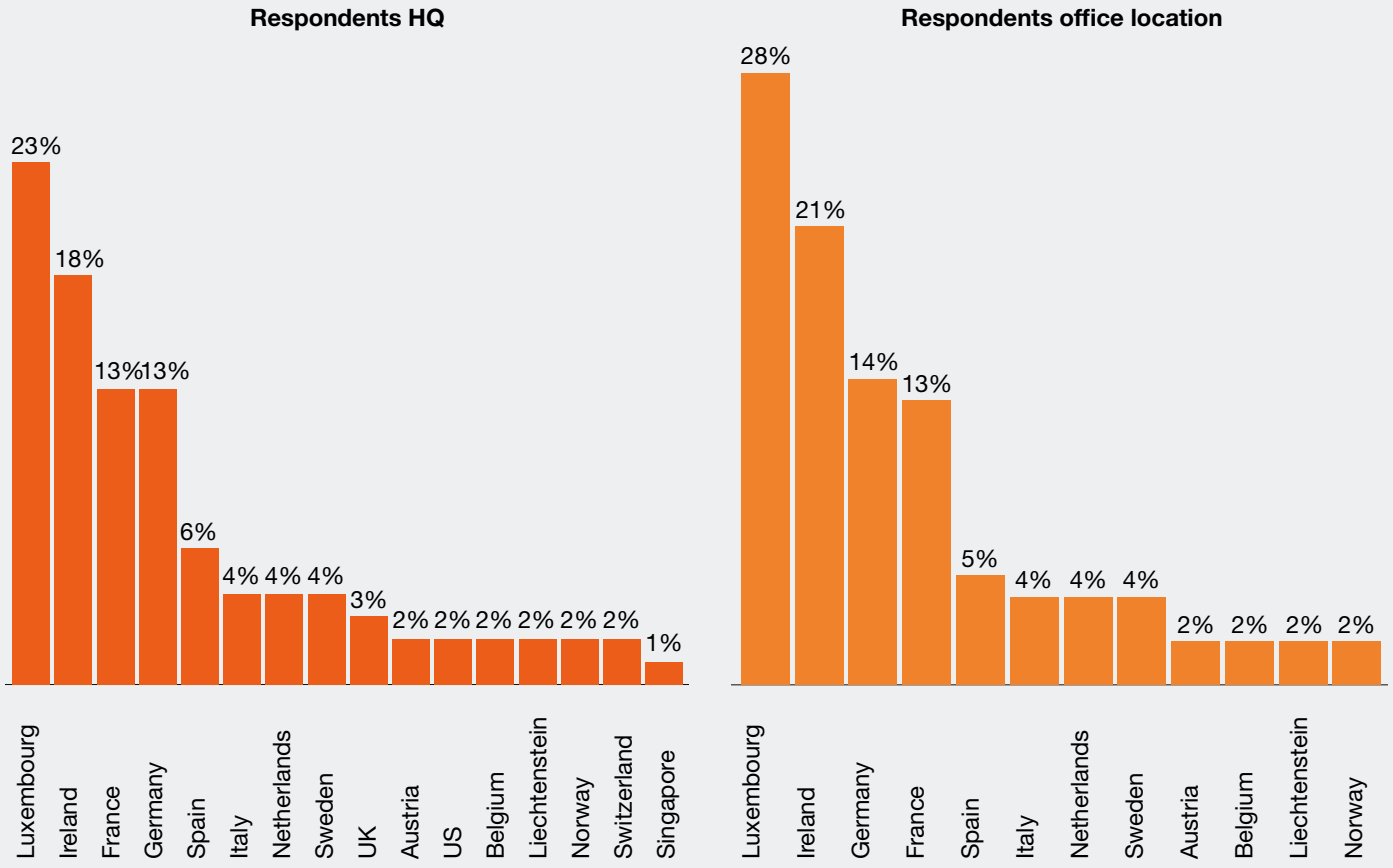
DORA has unleashed a host of challenges, but equally a host of opportunities. Now it is up to you to take the lead.



Survey methodology

The survey was conducted in March 2025. The respondents were financial entities required to have operations in selected countries across the EEA, which ensured that they fall under the scope of DORA. They are characterised as follows:

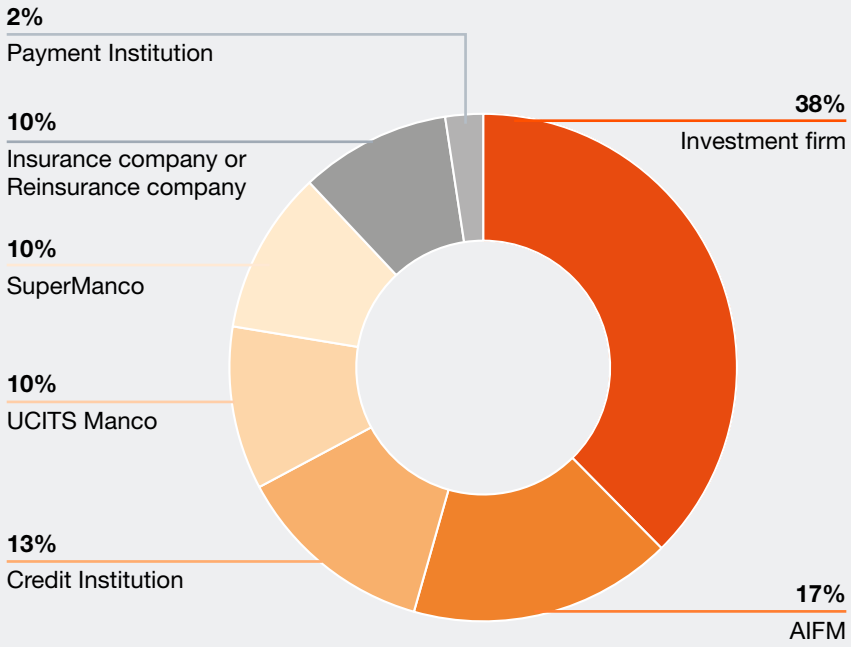
Exhibit 22. Respondents by HQ and office location



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

In terms of regulatory status, respondents were quite balanced across the different types of organisations.

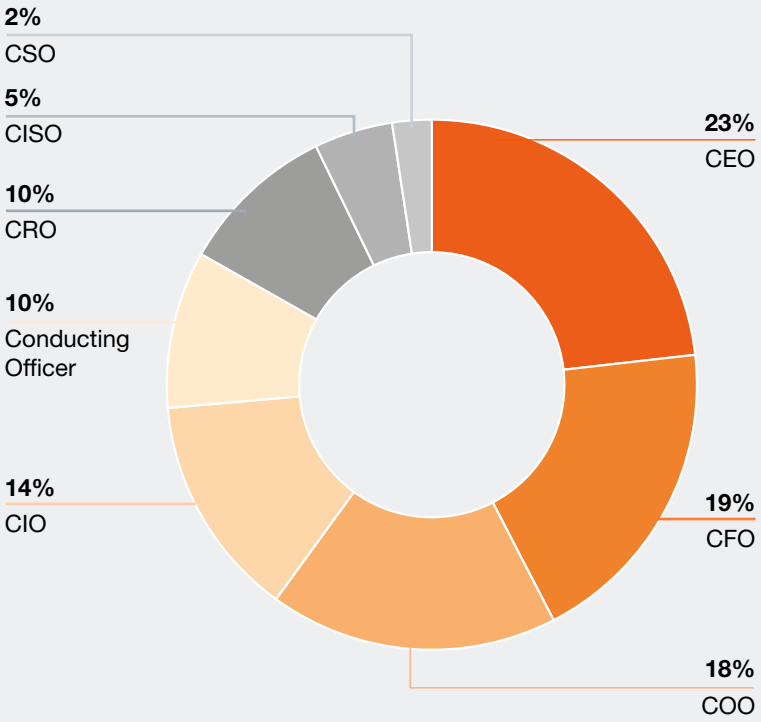
Exhibit 23. Respondents by type of regulatory status



Note: Numbers might not add up due to rounding. 'Super ManCo' refers to a UCITS management company which is also appointed as an AIFM to at least one AIF.
Source: PwC Global AWM & ESG Research Centre

Survey respondents were also well-distributed among the C-Suite, with no category taking dominance over the other.

Exhibit 24. Respondents' position within the C-Suite



Note: Numbers might not add up due to rounding
Source: PwC Global AWM & ESG Research Centre

Glossary

Critical ICT third-party service provider	TPSP designated as essential to the stability, continuity and quality of financial services.
Critical or important function	A function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.
Digital Operational Resilience	The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions.
Financial Entity	21 types of entity from credit institutions to management companies. Full list in Chapter I Article 2 of the regulation.
Information Asset	A collection of information, either tangible or intangible, that is worth protecting.
ICT risk	Any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.
ICT third-party service provider (TPSP)	An undertaking providing ICT services.
ICT Services	Digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.
Register	A centralised database that records all contractual agreements between financial entities and their ICT third-party service providers. It is used to monitor dependencies, manage risks, and ensure supervisory oversight of critical ICT services.

Contact us

Olivier Carré
Deputy Managing Partner,
Technology & Transformation Leader,
PwC Luxembourg
+352 621 334 174
olivier.carre@pwc.lu

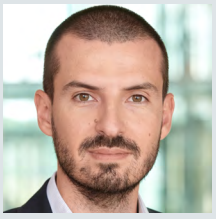
Michael Horvath
Advisory Partner,
Regulatory & Change Management,
PwC Luxembourg
+352 621 333 612
michael.h.horvath@pwc.lu

Cécile Liégeois
Clients & Markets Leader,
Regulatory Advisory Partner,
PwC Luxembourg
+352 621 332 245
cecile.liegeois@pwc.lu

Patrice Witz
Advisory Partner,
Technology Partner and Digital Leader,
PwC Luxembourg
+352 621 333 533
patrice.witz@pwc.lu

Xiaoyi Fang
Senior Manager, Advisory,
PwC Luxembourg
+352 621 332 505
xiaoyi.fang@pwc.lu

Vojtech Volf
Senior Manager, Advisory,
PwC Luxembourg
+352 621 334 132
vojtech.volf@pwc.lu



Maxime Pallez
Cybersecurity Director,
PwC Luxembourg
+352 621 334 166
maxime.pallez@pwc.lu

Thomas Wittische
Managing Director,
PwC Luxembourg
+352 621 334 181
thomas.wittische@pwc.lu

Notes

PwC Luxembourg (www.pwc.lu) is the largest professional services firm in Luxembourg with over 3,800 people employed from 90 different countries. PwC Luxembourg provides audit, tax and advisory services including management consulting, transaction, financing and regulatory advice. The firm provides advice to a wide variety of clients from local and middle market entrepreneurs to large multinational companies operating from Luxembourg and the Greater Region. The firm supports its clients in creating the value they are looking for by contributing to the smooth operation of the capital markets and providing advice through an industry-focused approach.
At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 370,000 people in 149 countries. Across audit and assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com and www.pwc.lu.