The world is how we shape it

sopra steria

One year after **DORA** came into force

Initial lessons learned

Authors

Andrés Ortega
IT Project Manager for Banking,
Sopra Steria
andres.ortega@soprasterianext.com

Graziella Milanese
Financial Services Consulting Director,
Sopra Steria
graziella.milanese@soprasterianext.com

Isabella Sacchi
ICT compliance consultant,
Sopra Steria
isabella.sacchi@soprasteria.com

Marine Lecomte
Head of Offers & Innovations,
Financial Services Sopra Steria
marine.lecomte@soprasteria.com

Thea R. Gulbranson
Legal security advisor,
Sopra Steria
thea.gulbranson@soprasteria.com

Vincent Lefèvre
Regulatory Tribe Director,
Sopra Steria Next
vincent.lefevre@soprasterianext.com

Xhemi Malosmani
Cyber Security Banking Consultant,
Sopra Steria Next
xhemi.malosmani@soprasteria.com

One year after **DORA** came into force – initial lessons learned

One year after its entry into application, DORA (Digital Operational Resilience Act) has established itself as a structuring framework for the digital resilience of European financial institutions. Its requirements have primarily helped harmonise practices that were earlier highly heterogeneous across countries.

Two key issues have concentrated most of the efforts:

- Standardisation of relationships with ICT service providers, through the creation of a standardised register and the integration of strengthened contractual clauses (audit rights, incident notification, standardised metrics related to business continuity and disaster recovery such as RTO/RPO, transparency on data location and the subcontracting chain). This work has been particularly challenging for international providers.

- Implementation Threat-Led Penetration Testing (TLPT) has proved operationally demanding. Defining the critical scope, mobilising internal teams, and coordinating with service providers particularly cloud providers have required rigorous organisation and significant resources.

Beyond these two priorities, several areas remain under pressure:

- Stabilisation of Level 2 texts and clarification of regulatory expectations as dialogue with supervisors continues.
- Mobilisation of cybersecurity skills, which remain insufficient in many institutions.
- Mastery of incident notification timelines (4 hours), which requires a robust organisational setup.
- Anticipation of impacts related to the designation of critical service providers by authorities.

Although large institutions have made progress, the compliance trajectory is far from complete. The regulator itself acknowledges the complexity of the programme and is expected to grant several additional months to finalise the work.

DORA is no longer a novelty; it is now an operational reality for more than 22,000 financial entities across Europe. This report analyses the impact of DORA across different financial segments, highlighting specific challenges and opportunities. Our approach focuses on geographical differences and concrete use cases.

Drawing on our experience, we provide practical recommendations to help institutions adopt scalable and resilient strategies. By aligning with DORA, institutions can not only ensure compliance but also drive growth and strengthen customer trust, contributing to a more resilient European financial ecosystem.

Part 1:

A European perspective on DORA challenges for key financial sector players

DORA applies to more than 22,000 financial entities and aims to harmonise digital operational resilience across Europe. However, implementation remains complex due to differences in size, complexity, and technological maturity among institutions.

In this first part, we focus on three major segments that are particularly impacted by DORA:

- Tier 1 banks
- Tier 2 and Tier 3 banks, and neo-banks
- Insurance companies

For each segment, we analyse the main DORA-related challenges, illustrated by concrete European use cases, and highlight the differences observed across countries.

Tier 1 banks

The implementation of DORA has represented a significant but necessary challenge for large banks, involving not only technical upgrades but also strategic and cultural shifts. Banks must now foster a proactive cybersecurity culture and greater awareness of operational risks, to improve collaboration between IT, compliance, and risk teams, and to ensure smooth cooperation and optimal responsiveness in the event of incidents. Multinational banks face additional complexity in harmonising their efforts across borders, given past inconsistencies in local regulations.

DORA has also strengthened oversight of third-party providers, requiring banks to conduct rigorous risk assessments and ensure ongoing monitoring to guarantee compliance. These requirements come at a time when issues of digital sovereignty and geopolitical tensions raise strategic challenges in supplier management, making the subcontractor register more relevant to ensure effective visibility and control over the critical value chain.

One year after DORA's implementation, it appears that large banks benefited from a relatively solid foundation that facilitated adoption of the regulation, supported by more stable governance than that of smaller institutions. However, monitoring a large number of subcontractors remains complex, as does assessing their criticality. In addition, multi-entity Tier 1 banks face the challenge of managing entities with heterogeneous levels of preparedness, varying by size and geographic location.

Sopra Steria has positioned itself at the heart of DORA implementation for major European banks.

These use cases demonstrate that DORA goes beyond compliance: it strengthens governance, improves data management, and enhances the ability to respond effectively to incidents.

Use Case 1:
Ensuring the resilience of a complex application environment for a major French bank

The challenge

With an ecosystem of several hundred strategic and critical applications spread across multiple entities, this major French bank – also operating in several European countries – was facing significant challenges:

- **Regulatory compliance:** Meeting legal requirements, including DORA, to ensure resilience across sensitive scopes.
- **Data integrity and recovery:** Ensuring reliable backups and the restoration of secure, up-to-date data following an incident or disaster, while complying with RTO requirements.
- **Resilience testing:** Assessing and improving the ability to respond effectively to crises and incidents.

Approach and benefits

Sopra Steria excelled thanks to its deep understanding of the client's data governance needs, resulting in a tool-based solution fully integrated into the information system. This solution enables the effective mapping of thousands of applications while complying with regulatory and security constraints in a controlled production environment.

By integrating into a constantly evolving ecosystem, Sopra Steria ensures compliance audits, business support, and continuous adaptation to regulatory requirements. It strengthens crisis governance through key indicators (KPIs) derived from testing, enabling faster and more accurate decision-making. In addition, coordination across business lines has improved thanks to optimised simulation exercises.

Use Case 2:
Aligning incident reporting with new DORA requirements for a major Italian bank

The challenge

Within the complex landscape of payment systems and faced with a highly complex legacy architecture, this major Italian bank encountered the following challenges:

- **Regulatory compliance:** Defining an incident management framework by designing a harmonised process and integrating reporting solutions to reduce incident resolution costs.
- **Data integrity:** Launching a relevant data quality initiative to produce reliable, high-quality incident reports.

Approach and benefits

By combining expertise in data management, process efficiency, and architecture design, Sopra Steria Next developed a reporting solution designed to prevent and manage cyber incidents and threats.

Improved data quality enabled the client to define and implement a communication plan for all stakeholders, allowing rapid activation of action plans in the event of an incident.

Use Case 3: Optimising BIA reporting – from raw data to decision support with Power BI

The challenge

When conducting a BIA, organisations often generate large datasets that must be consolidated into a comprehensive report. This major Norwegian bank faced the following challenges:

- **Data management:** Handling large volumes of raw data stored in extensive Excel files was cumbersome and poorly suited to visualisation or effective decision-making.
- **Visual presentation:** Executives needed clear and concise visualisations to quickly understand key results and dependencies.
- **Search and filtering:** The organisation required a solution enabling targeted searches and data filtering by processes, dependencies, and suppliers to gain deeper insights.

Approach and benefits

By optimising existing tools such as Power BI, the organisation developed a scalable and efficient solution to manage and present BIA data:

- **Enhanced data visualisation:** Raw data from Excel files was transformed into interactive dashboards and dynamic visualisations, making complex datasets accessible and actionable for decision-makers (with targeted search and filtering capabilities to highlight critical processes, dependencies, and supplier relationships).
- **Sustainability and ease of use:** Maintaining the BIA framework required a flexible and user-friendly approach, without the need to purchase new systems or undertake major developments.

By leveraging existing resources and avoiding the acquisition of new software, the organisation maintained a cost-effective and easy-to-maintain solution, demonstrating the value of data analytics in supporting more informed decision-making.

Tier 2 and Tier 3 banks, and neo-banks

One year after its entry into force, DORA plays a key role in strengthening the security and operational resilience of financial institutions, particularly smaller banks and neo-banks. These players — often constrained by limited resources, highly dependent on third-party providers, and operating with small teams — must now embed security and resilience at the core of their operations, while balancing regulatory compliance with operational efficiency.

Levels of compliance maturity vary widely and remain a work in progress. Large banks and major IT providers already had robust cybersecurity frameworks in place, which they were able to adapt to meet DORA requirements. In contrast, smaller entities — such as certain funds or small institutions have had to undertake significant structural changes, including the implementation of vulnerability testing, strict third-party management, and the integration of new systems with legacy infrastructures. For many, DORA compliance remains an ongoing process, perceived as both complex and costly, placing additional pressure on teams and potentially affecting innovation.

Despite these constraints, DORA represents a strategic opportunity: it strengthens governance, optimises risk management, and reinforces customer trust, transforming a regulatory requirement into a lever for positioning institutions as reliable players in a market where digital trust is a key success factor.

Sopra Steria has supported this market segment, illustrated by two specific use cases detailed below:

Use Case 1: International ambitions with limited resources in a strict DORA context

The challenge

A Tier 2 regional bank with international ambitions was facing increasing regulatory requirements and operational constraints. Despite a moderate asset base and a broad range of financial products, the institution had to cope with the complexity of compliance and digital transformation. Regulations such as DORA required significant investments in IT security, risk management, and vendor oversight, while integrating new systems with a legacy infrastructure proved time-consuming and technically complex. Limited budgetary and staffing resources further complicated the path to compliance and operational efficiency.

Approach and benefits

- **Robust regulatory compliance framework:** Introduction of real-time monitoring and reporting systems to proactively identify gaps and resolve them quickly.
- **Risk management and IT security:** Deployment of advanced cybersecurity measures, including real-time monitoring, penetration testing, and continuous vulnerability assessments.
- **Resource optimisation:** Careful evaluation of resource allocation to efficiently meet regulatory requirements, supported by targeted training and upskilling programmes to strengthen internal teams.
- **Robust third-party risk management system:** Clear contractual agreements and defined audit rights to ensure ongoing accountability of service providers.

This comprehensive approach not only ensures regulatory compliance but also drives operational efficiency, enabling the bank to successfully address the challenges of digital transformation.

Use Case 2:
Designing a holistic approach for a Spanish bank through a dedicated tool

The challenge

The financial institution faced a dual challenge: aligning with DORA while maintaining smooth operations and controlling costs. Under DORA's strict requirements, the bank needed to assess its compliance across multiple regulatory chapters and articles, identifying gaps, strengths, and areas for improvement. Due to its small size, it had many aspects to audit and understand, without the necessary internal tools or expertise. The complexity and resource intensity of these tasks highlighted the need for external support, particularly as the bank wished to deploy a dedicated tool.

Approach and benefits

Sopra Steria provided a structured methodology to address these challenges. The consulting team conducted a detailed BIA, working closely with various departments to identify critical functions, assess risks, and align existing policies with DORA requirements. Leveraging the Global Suite tool selected by the bank, Sopra Steria delivered a centralised platform for risk management and compliance, streamlining the monitoring and assessment of critical services. This partnership enabled the bank to close its compliance gaps within the required timelines, strengthen its operational resilience, and meet regulatory expectations – while minimising risks and optimising resources.

Insurance

Unlike the banking sector, insurance companies have historically been subject to fewer sector-specific regulations, making compliance with DORA more complex and resource-intensive. One year after its entry into force, insurers still need to strengthen their ability to manage disruptions and recover quickly, combining technical solutions with strategic planning.

For international groups, these challenges are compounded by the diversity of regional risks: backup data localisation, local threat landscapes, and the integration of resilience into global operations. Resilience testing remains difficult due to the diversity of products, legacy systems, and the complexity of upgrading them. Third-party risk management — particularly for critical functions such as claims management — remains a central issue.

Smaller insurers and mutual organisations face a significant structural lag: many programmes and control frameworks still need to be deployed before full compliance can be achieved. These players, often constrained by limited resources and highly dependent on external service providers, are particularly exposed to operational and technical challenges.

Sopra Steria has supported insurers in their transformation and compliance journey, focusing on their key challenges:

Use Case 1:
Compliance in a cloud environment for a major international insurer

The challenge

An international insurance group faced a dual challenge: transforming its IT systems towards a modern, cloud-based environment while ensuring compliance with DORA. This transformation aimed to create a resilient infrastructure capable of minimising disruptions caused by incidents or disasters. However, meeting DORA's strict disaster recovery requirements represented a major challenge.

The group also had to account for diverse risks related to its international operations, such as geographical vulnerabilities and the proximity of backup environments.

Approach and benefits

The first step involved a detailed BIA to identify critical applications and components. Based on this analysis, targeted measures were developed to strengthen security and resilience.

These measures included extending backup retention periods, accelerating the implementation of immutable backups, and designing a multi-year disaster recovery testing plan. By addressing these priorities, the group ensured compliance with DORA while significantly improving its ability to anticipate, adapt to, and recover from potential disruptions.

This approach provided the group with a more robust and locally adapted disaster recovery framework, aligning global standards with regional needs. It not only strengthened operational resilience but also reinforced confidence in the group's ability to protect its operations and maintain customer trust.

Use Case 2: Streamlining processes and organisation to ensure DORA compliance for a major French insurer

The challenge

The insurer, a subsidiary of a major banking group, faced increasing regulatory requirements. With operations spanning EU and non-EU subsidiaries, as well as delegated entities and service providers, the organisation operated within a complex compliance landscape. Key challenges included defining the scope of regulatory responsibilities, preparing for reporting to multiple supervisory authorities such as ACPR, EIOPA, ENISA, and ANSSI, and establishing a cyber-resilient due diligence framework. In addition, the need for continuous monitoring, structured improvement plans, and rigorous documentation represented major obstacles, requiring a robust and forward-looking approach.

Approach and benefits

During the Build phase, standardised procedures, tools, and methodologies were developed to assess third-party due diligence and cybersecurity maturity. In the Run phase, maturity audits, security supervision, team training, and awareness programmes enabled effective implementation and long-term sustainability of the due diligence process within the relevant teams.

This approach ensured alignment with DORA (and other regulatory requirements), strengthened the client's cybersecurity posture, and provided a clear roadmap for continuous improvement.

Use Case 3:
Navigating DORA compliance for third-party risk management at a global insurer

The challenge

This Spanish insurer faced difficulties in defining and ensuring contractual compliance with its suppliers through effective due diligence. The organisation needed to tackle the complex task of aligning stakeholders, methodologies, and terminology with DORA articles, while meeting regulatory requirements related to resilience, continuity, and third-party oversight.

Approach and benefits

A multifaceted approach was deployed, starting with a three-week initial assessment using a DORA planning tool to align stakeholders with regulatory requirements and standardise methodologies and terminology.

The team introduced innovative solutions, including generative AI, to improve project efficiency, and developed a collaborative working model that fostered a shared understanding of objectives, risks, and required actions. Interconnections were mapped to ensure robust due diligence practices.

These efforts not only brought the client closer to full regulatory compliance, but also improved operational reliability, reduced risks, and positioned the organisation to address future challenges in an evolving regulatory environment.

Conclusion

One year after its entry into force, DORA shows that despite its uniform application across the financial sector, challenges vary significantly by segment. Insurers must manage complex third-party risks, ensure reliable reporting, and conduct appropriate resilience testing. Tier 1 banks face the alignment of their global operations with strict requirements, while smaller banks and neo-banks must implement advanced compliance mechanisms with limited resources These challenges are further compounded by national variations in regulatory frameworks, making country-specific adaptation essential.

Experience to date demonstrates that DORA compliance is resource-intensive and ongoing, but it also represents a strategic opportunity to strengthen operational resilience and customer trust. The next phase of our analysis will provide detailed strategies and best practices that enable institutions to address DORA's critical requirements effectively, while consolidating their position in an ever-evolving digital environment.

Part 2:

Best practices for ensuring sustained DORA compliance over time

In the following section, we take a deeper look at the most sensitive operational aspects of DORA, analysing its practical implications for financial institutions and providing concrete recommendations to help navigate the complex DORA framework and embed its principles into robust operational practices.

DORA's Pillars:

DORA Pillar 1: Ensuring strong governance in ICT crisis management

DORA significantly expands the concept of digital operational resilience by emphasising the need for financial institutions to embed resilience into day-to-day operations, not only in response to disruptions. Achieving DORA compliance requires financial entities to establish a comprehensive ICT crisis management framework covering the entire organisation, which represents a complex programme management challenge.

To address these challenges, we recommend that financial institutions adopt the **Three Lines of Defence (3LoD)** model as a practical governance approach, ensuring accountability, oversight, and operational efficiency. This model is the most widely used and aligns with DORA requirements. Four key aspects should be considered:

Apply the proportionality principle

The proportionality principle requires financial entities to tailor their ICT crisis management approach to the size of the organisation, its risk profile, and its operational complexity. To do so, organisations should conduct a maturity assessment to identify current gaps in ICT resilience. This assessment helps define clear objectives, roles, and key performance indicators (KPIs) aligned with DORA requirements.

Define roles and responsibilities using the Three Lines of Defence (3LoD) model

The 3LoD model provides a structured approach to clarifying responsibilities and improving coordination across teams:

- **First line (operational teams):** Responsible for identifying, reporting, and managing ICT incidents. A designated Crisis Manager coordinates incident response, ensures the activation of operational procedures, and drives rapid resolution of tactical issues.

- **Second line (control and oversight functions):** Oversees governance, risk, and compliance. It establishes policies, frameworks, and controls to guide first-line actions and challenges their risk assessments.

- **Third line (independent audit and assurance):** Led by internal audit, it conducts independent assessments of the ICT crisis management framework. Findings serve as a feedback loop, enabling the first and second lines to adjust and improve the system.

Evolution of roles across implementation phases

The responsibilities of the three lines evolve throughout the implementation lifecycle:

- **Initial phase (preparation and set-up):**
  The first line builds DORA compliance processes and tools; the second line defines policies and provides oversight; the third line performs readiness audits.

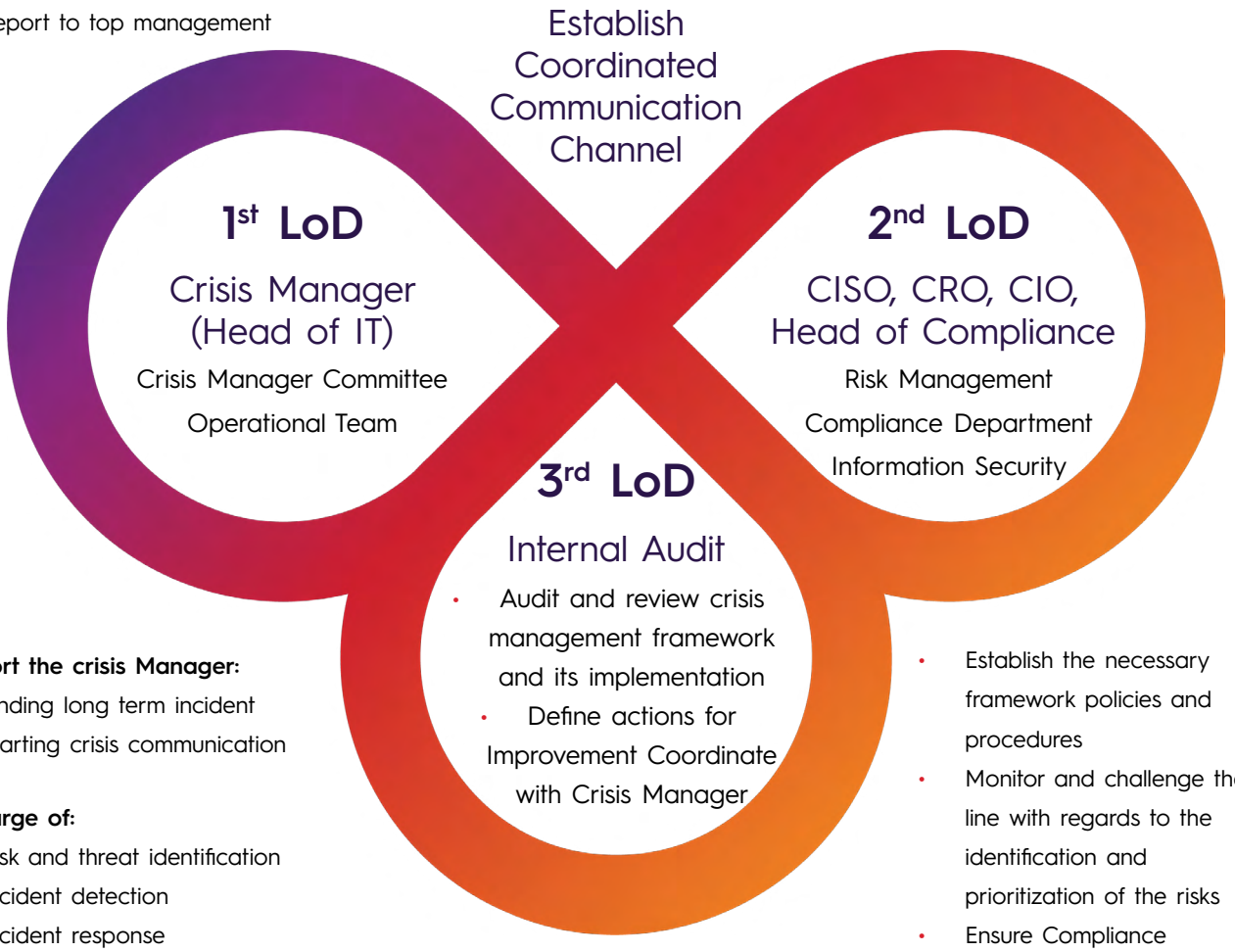
- **Intermediate phase (implementation and execution):**
  The first line implements risk management, reporting, and testing procedures; the second line monitors compliance; the third line conducts targeted audits to verify ongoing compliance.

- **Ongoing phase (sustainable compliance and continuous improvement):**
  The first line maintains operational resilience; the second line focuses on monitoring regulatory developments and improving processes; the third line performs periodic audits to ensure alignment with continuously evolving DORA standards.

Management Body (CEO, Group CISO etc.)

- Oversees the operational team and ensure that response procedures are activated
- Define the crisis ccommunication strategy
- Acts as the primary point of contact for reporting crisis-related information
- Report to top management

- Supervision role
- Communicate and coordinate with crisis manager
- Report to top management



Support the crisis Manager:

- Finding long term incident
- Starting crisis communication

In charge of:

- Risk and threat identification
- Incident detection
- Incident response

- Establish the necessary framework policies and procedures
- Monitor and challenge the first line with regards to the identification and prioritization of the risks
- Ensure Compliance

Nevertheless, implementing DORA adds an additional layer of complexity to an already complex operating model between second- and third-line functions, as illustrated by the following examples:

- The ICT risk control function has responsibilities that are similar — or even identical — to those of the operational risk function with regard to ICT risks (as part of operational risk). To properly identify, measure, mitigate, and report ICT risks, alignment between these two functions must be established.

- In its assessment report of the ICT risk framework, as required under DORA, the ICT risk control function must include relevant conclusions from the compliance and internal audit functions. As a result, a reporting line must be established between these second- and third-line functions and the ICT risk control function.

Consequently, clear governance between second- and third-line functions — with clearly defined and distinct roles and responsibilities—must be established in the context of DORA, to avoid overlaps, gaps in interdependencies, and unnecessary complexity between these functions.

Establish robust communication protocols

Communication is the cornerstone of DORA's ICT crisis management requirements.

Crisis communication plans must clearly define roles and responsibilities to avoid ambiguity in reporting structures. The Crisis Manager acts as the central coordinator, relaying critical information to the CISO and senior management to ensure smooth and timely responses.

DORA emphasises management accountability for ICT resilience, making active involvement and informed decision making, supported by regular updates and structured reporting—essential for effective crisis management.

Strengthen awareness and implement training programmes

DORA compliance requires a clear understanding of roles and effective training for ICT crisis management. Role-based training aligned with the **Three Lines of Defence (3LoD)** model ensures that teams develop relevant capabilities, particularly in IT compliance and information security. This is especially important as compliance functions often lack the technical expertise required to effectively oversee IT functions.

Crisis simulations and resilience testing further enhance preparedness, enabling organisations to assess their response capabilities, identify weaknesses, and improve coordination – even across geographically dispersed teams.

By establishing strong ICT crisis management frameworks from the outset, organisations can reduce disruptions, strengthen customer trust, and ensure business continuity. The Three Lines of Defence (3LoD) model, when well designed and consistently applied, promotes accountability and responsiveness.

Conducting an effective Business Impact Analysis (BIA)

Financial institutions often operate within a vast ecosystem of digital solutions and information systems. Many of these can affect one or more critical banking services if they are impacted by an incident.

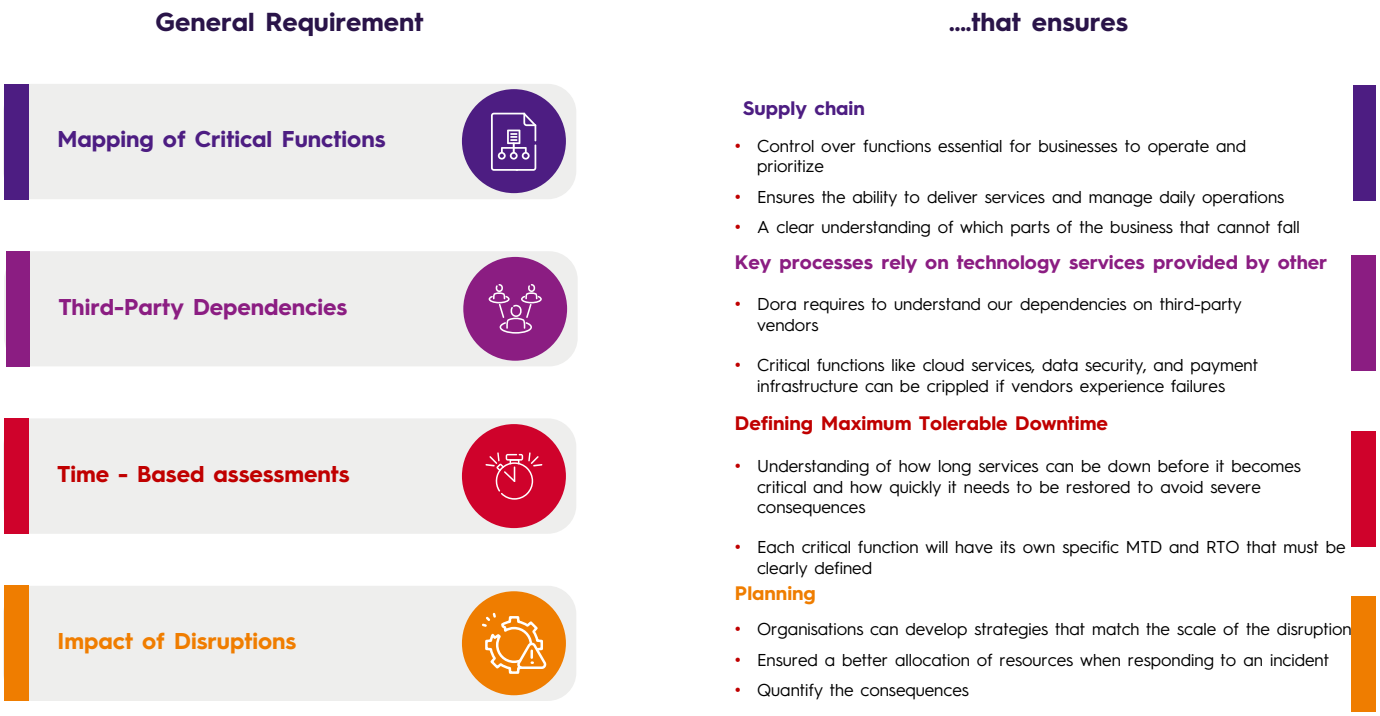
In this context, the first pillar of DORA provides entities with the tools needed to prepare for threats to their resilience: the **BIA,** which DORA requires financial institutions to perform in order to assess their exposure to severe disruptions.

The BIA provides financial institutions with critical insights to respond to disruptions, accelerate recovery, and minimise financial and reputational damage. It applies not only to operations, but also to IT, compliance, risk management, and senior management. A disruption in one area can trigger cascading effects across the entire organisation. The BIA helps institutions understand both the short- and long-term impacts of such events.

DORA mandates a **structured BIA approach** within financial institutions to ensure operational resilience. Organisations must identify their critical functions in order to prioritise them, assess dependencies on third parties, and define key metrics such as **Recovery Time Objectives (RTO) and Maximum Tolerable Disruption (MTD).**

DORA also requires ICT assets and services to be aligned with the BIA, particularly with regard to the redundancy of critical components. A comprehensive understanding of dependencies and recovery requirements enables institutions to develop robust business continuity strategies, reducing the risk of operational failure and ensuring financial stability and regulatory compliance.

DORA mandates a comprehensive approach to BIA



A well-executed BIA provides senior management with clear insights that guide future decisions and priorities. The process typically includes mapping critical systems, assessing the potential impacts of disruptions, and identifying third-party dependencies. The outcome is a prioritised list of functions and systems essential to the institution's operations, enabling rapid recovery and limiting financial instability.

At Sopra Steria, our approach is built around five key recommendations:

- **A continuous process:**
  The BIA must be regularly reviewed to reflect evolving technologies, regulations, and customer expectations, ensuring long-term resilience and sustained DORA compliance.
  It should not be a one-off exercise performed only at the time of DORA implementation, but rather embedded as a recurring process within the organisation.

- **A structured framework:**
  Leveraging standards such as ISO 22301 and ISO 22317 enables a systematic and repeatable approach, tailored to the institution's specific business continuity needs.

- **Business-driven governance:**
  Senior management must identify and prioritise critical functions, ensuring that the BIA accurately reflects real operational priorities.

- **IT–business collaboration:**
  IT and business teams must work closely together to understand system and process dependencies, avoid misunderstandings, and ensure effective implementation of critical priorities.

- **Mapping and strengthening dependencies:**
  Identify existing and potential dependencies, plan for redundancies, approval mechanisms, and monitoring capabilities to ensure comprehensive preparedness for disruptions.

DORA – Pillar 2: Establishing a robust incident management framework

DORA requires financial institutions in the banking and insurance sectors to establish and maintain comprehensive incident management and reporting frameworks — many of which institutions have already partially implemented. The regulation aims to strengthen incident identification, classification, and reporting processes by requiring clear criteria based on severity and impact.

The **BIA** described above, and **incident management** are closely linked and together form the backbone of an effective resilience strategy. The BIA identifies critical systems and assesses the potential impact of disruptions, while incident management ensures their rapid restoration in the event of an incident.

Effective incident management is essential to minimise economic and reputational damage and to ensure a swift return to normal operations. Financial entities must establish clear processes to monitor and handle incidents, assess their impacts, and implement measures to prevent recurrence.

We recommend an end-to-end approach based on three phases:

- **Assessment phase:** review existing processes to strengthen and refine incident classification procedures.
- **Data management phase:**

  1. Identify the data required to produce incident reports, and

  2. Perform gap analysis and data mapping to identify missing information.
- **Modelling and reporting phase:** analyse and develop new rules to industrialise reporting, ensure data accuracy, and enable appropriate communication to all stakeholders.

One year after DORA's entry into force, short notification timelines and the complexity of triggering criteria remain sensitive issues for institutions. It is therefore advisable to regularly simulate incidents to:

- Verify that escalation procedures correctly identify decision-makers and enable rapid execution of critical actions, including notification to competent authorities.
- Provide teams with concise, actionable information to support decision-making, such as triggering criteria, relevant business stakeholders, critical functions, and associated systems.

It may also be beneficial to conduct these simulations in a confidential setting, to protect discussions and conclusions from any subsequent disclosure.

DORA – Pillar 3: Implementing a comprehensive digital operational resilience testing programme

DORA requires financial entities to establish a comprehensive digital operational resilience testing programme as part of their ICT risk management framework. This programme must assess the organisation's ability to respond to incidents, identify vulnerabilities, and address gaps.

Testing covers disaster recovery, business continuity, security, and third-party resilience. These tests ensure that critical functions can be rapidly restored and that essential services remain operational.

A key element is the introduction of **TLPT,** which simulates real-world cyberattacks to strengthen cyber-security, in line with the Threat Intelligence-Based Ethical Red Teaming (TIBER-EU**)** framework. Test results must be documented and integrated into overall risk management strategies to support continuous improvement.

One year on, the implementation of these tests remains a sensitive topic, and many institutions have not yet fully deployed all required tests, particularly TLPT. At Sopra Steria, we recommend a structured approach:

- **Assess the current state:** analyse DORA requirements and existing testing processes, identify gaps, and assess training needs for teams.
- **Prioritise critical systems:** map essential functions through the BIA and integrate different types of tests into a coherent testing programme.
- **Tracking and documentation:** centralise results, responsibilities, timelines, and corrective actions, with a particular focus on highly critical systems to ensure robust and compliant resilience.

Financial institutions may use existing test management tools or develop customised solutions tailored to their needs. These tools should enable the integration of multiple test types within a single framework, facilitating planning, execution, and monitoring. They should also support result documentation and the implementation of corrective actions to ensure continuous improvement and sustained DORA compliance.

To achieve this objective, we focus on the key factors that make a testing programme effective in ensuring resilience, in line with the approach outlined below:

Feature	Action	Benefit
Centralised test repository	Store all test cases, scenarios, and results in a single repository.	Ensures consistency and easy access to testing information.
Automated planning and execution	Use tools to automate test scheduling and execution.	Reduces manual effort and ensures tests are performed regularly.
Real-time monitoring and reporting	Leverage continuous monitoring tools to gain real-time insights.	Enables rapid detection and immediate response to issues.
Comprehensive documentation	Document test results, assessments, time-lines, and accountability details.	Promotes transparency and clear ownership.
Prioritisation of critical systems	Focus on testing efforts first on the most critical systems.	Ensures essential components are thoroughly tested.
Integration with risk management	Feed test results into the enterprise risk management framework.	Strengthens the organisation's ability to manage and mitigate risks.

Ensuring Long-Term Compliance

For long-term compliance, it is essential to go beyond a one-off approach and implement continuous monitoring and audit processes. This includes:

- Regularly updating the compliance framework to reflect regulatory developments.,
- Integrating compliance processes into the overall risk management framework.,
- Involving key stakeholders across the organisation (executive management, IT, business units, risk, and compliance).,
- Maintaining comprehensive and up-to-date documentation.,
- Promoting a culture of continuous improvement and operational resilience at all levels.

Overview – DORA testing requirements

DORA specifies testing requirements by introducing a variety of methods, which can be categorised as follows:

Disaster Recovery Tests
Simulations of emergency situations to evaluate the effectiveness of recovery plans and test backup and restoration procedures. These tests ensure that institutions can quickly recover and resume normal operations during a crisis.

Business Continuity Tests
Verifying that critical functions can be maintained even during disruptions. This involves testing operational continuity to confirm that essential services remain functional under adverse conditions.

Security Tests
Including penetration testing to identify IT infrastructure vulnerabilities, security analyses, and access control reviews. These tests detect weaknesses that could be exploited by malicious actors.

Third-Party and Supplier Resilience
Assessing risks associated with critical suppliers and verifying their ability to provide support in case of disruption. This includes reviewing service level agreements (SLAs) and ensuring compliance.

Regular Security Reviews
Audits and assessments conducted regularly to continuously enhance security measures. These reviews are essential for maintaining a high level of security over time.

Training and Awareness
Creating test scenarios to evaluate employee knowledge of security policies and emergency procedures. This includes simulated phishing exercises to assess employee vigilance against social engineering attacks.

Data Integrity Tests
Ensuring the integrity and availability of data under various conditions, which is crucial for maintaining trust in the accuracy and reliability of the institution's data.

Compliance Tests
Targeted reviews and testing to ensure full adherence to DORA regulatory requirements, helping to avoid legal or regulatory sanctions and ensuring the institution operates within the required legal framework.

DORA – Pillar 4: Streamlining third-party risk management through technology

One year after DORA's implementation, Pillar 4 remains the most complex for financial institutions to deploy. Few have completed a full review of their third-party suppliers. While prioritising critical functions was a first step, operational implementation remains resource intensive. Additionally, DORA's requirements for exit strategy testing remain challenging, as institutions must ensure that all critical suppliers can support a smooth disengagement in the event of contract termination or service disruption.

Despite these challenges, Pillar 4 represents a major strategic opportunity, strengthening operational resilience, control over critical suppliers, and digital sovereignty.

Successful implementation relies on two complementary pillars: organisation and technology.

Organisation

- **Governance and Contracts:** Clarify DORA-related obligations within contracts, including rapid incident notification, continuity of critical functions, and participation in resilience testing. Contracts must also explicitly address testing requirements related to exit strategies.
- **Business Oversight and Prioritisation:** Clearly define critical functions, assign responsibilities, and hold decision-makers accountable to accelerate decision-making during crisis situations. Ensure regular oversight through harmonised audits at both group and entity levels.
- **Centralised Register:** Maintain a single, standardised register of suppliers, including contracts, exit strategies, and critical functions, to ensure visibility and operational consistency.

Technology

- **Automation and Reporting:** Leverage tools to automatically collect and update supplier information, reduce manual workload, and ensure continuous oversight.
- **AI-enabled Support:** Use contract analysis and regulatory monitoring tools powered by AI to identify gaps, simplify compliance, and support operational decision-making.
- **Continuous Supplier Monitoring:** Deploy technical solutions to monitor in real time the performance, resilience, and compliance with DORA obligations of critical service providers.

By combining a robust organisational framework with strong technological enablement, institutions can not only reduce operational burden but, above all, ensure sustainable control over critical third-party providers, thereby strengthening long-term resilience and digital sovereignty.

Ensuring harmonisation of practices across the organisation

DORA applies uniformly across the financial sector, requiring multi-entity banking groups to adopt a consistent and coordinated approach, regardless of the national or European scope of their subsidiaries. While each entity remains responsible for its own compliance, the central level must ensure a harmonised application to safeguard overall group compliance.

This challenge is particularly pronounced for large European banking groups operating across multiple jurisdictions, such as BNP Paribas, HSBC, Santander, Deutsche Bank, or UniCredit. These institutions are largely supervised by the European Central Bank, which directly oversees 113 significant institutions and expects a high level of maturity in operational resilience, including DORA compliance.

In this context, several DORA requirements increase operational complexity: synchronisation of ICT resilience tests across entities, coordination of their execution, consistent implementation of remediation plans, and incident reporting subject to strict timelines and formats. Without an appropriate organisational model, these obligations expose groups to compliance risks and duplicated efforts.

Our key recommendation is therefore to adopt a **federated approach to DORA compliance.**

This approach combines strong central governance with controlled local autonomy and is based on:

- A centralised and shared interpretation of DORA, disseminated through regular communication.;
- Harmonised gap analyses to identify and prioritise compliance actions.;
- Cross-functional collaboration between business, IT, risk, and legal teams;.
- Consistent training programs across the group to ensure team alignment.;
- Centralised audit, reporting, and monitoring tools enabling effective supervision and consistent risk management, particularly for third-party risks.

This federated organisation strengthens compliance, reduces redundancy, and fosters a shared culture of operational resilience, while preserving the flexibility needed to address local specificities.

Conclusion

One year after its entry into force, DORA remains a major and structural challenge for banks, and the path toward fully operational compliance is still long. While some institutions are now approaching a satisfactory level of maturity, others are only beginning— or still consolidating— their efforts on key pillars, revealing significant disparities in preparedness across the sector.

In this context, the recommendations outlined above are intended to support institutions in translating DORA into operational reality, beyond mere regulatory compliance. The challenge is now to build sustainable compliance, capable of evolving over time alongside risks, technologies, and outsourcing models. More than a regulatory obligation, operational resilience is increasingly becoming a strategic lever, central to the robustness of banks in an increasingly uncertain digital and geopolitical environment.

Part 3:

What are the consequences in the post-DORA landscape?

DORA marks a turning point in European financial regulation, but it is only one step within an ever-evolving regulatory landscape. As cyber threats grow in sophistication, new initiatives will complement this framework, such as the AI Act governing the use of artificial intelligence and the Cyber Resilience Act aimed at strengthening the security of digital products.

1. A strategic lever toward more sovereign and independent financial institutions

Beyond its strictly regulatory dimension, DORA serves as a foundation for more sovereign and independent organisations in the management of critical digital activities. By mandating the maintenance of an exhaustive ICT supplier register, covering not only direct subcontractors but, progressively, cascading subcontracting chains — DORA enables financial institutions to precisely map their technological dependencies.

This visibility, long lacking, sheds light on risk concentrations, excessive geographic or technological dependencies, and structural vulnerabilities often hidden within complex outsourcing models.

Furthermore, the requirement to identify critical or important service providers and to implement enhanced oversight mechanisms represents a major shift. It pushes organisations away from purely contractual management toward an active dependency management approach, supported by monitoring, control, and risk anticipation mechanisms. This enables institutions to identify the most structurally significant dependencies particularly on dominant cloud or digital service providers, and to define proportionate responses, whether through diversification, strengthened contractual clauses, or credible exit strategies.

Finally, by reinforcing requirements around business continuity and disaster recovery planning, DORA forces institutions to consider major external shock scenarios: systemic cyberattacks, failures of critical providers, geopolitical crises, or infrastructure disruptions. This reflection, too often theoretical in the past, becomes operational and structuring. It fosters a stronger crisis management culture, clarifies decision-making chains, and enhances the ability of organisations to maintain essential functions even under degraded conditions.

In this respect, DORA goes beyond compliance: it acts as a catalyst for transformation toward greater sovereignty, stronger control, and resilience more closely aligned with the long-term strategic challenges facing the financial sector.

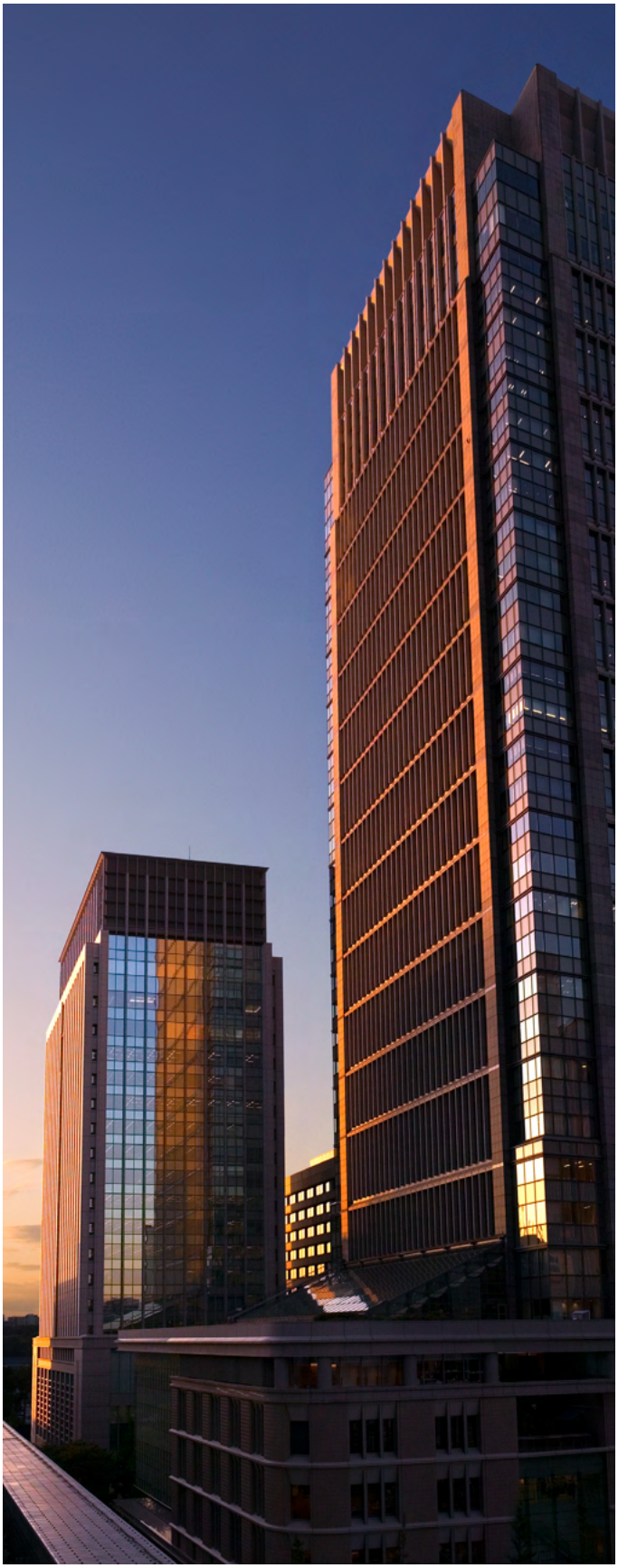
2. Toward a consolidation of ICT service providers?

The implementation of DORA highlights in a very tangible way the structural dependence of financial institutions on ICT service providers, particularly large international vendors. Requirements for transparency across the entire subcontracting chain, strengthened contractual clauses, audit rights, and resilience obligations shift the focus from simple vendor management to active operational risk control.

These requirements are gradually reshaping market dynamics. Large technology providers must align with more stringent European standards, sometimes at odds with their global operating models: acceptance of extended audit rights, continuity and exit plan requirements, and constraints related to data localisation and service reversibility. For financial institutions, this leads to more structured renegotiation of supplier relationships and more selective sourcing of critical partners.

For smaller technology players, DORA acts as a catalyst for transformation. The expected level of compliance requires significant investments in governance, security, and business continuity. Some providers are rapidly increasing their maturity, while others pursue strategies of consolidation, specialisation, or integration with more robust players. These dynamics foster both market consolidation and the emergence of specialised providers better aligned with regulatory expectations.

Ultimately, DORA helps structure a more selective ICT services market, where compliance, control capabilities, and resilience become decisive criteria alongside cost and innovation. This evolution strengthens financial institutions' ability to secure critical dependencies and anchor their technology choices in a more sustainable and controlled framework.

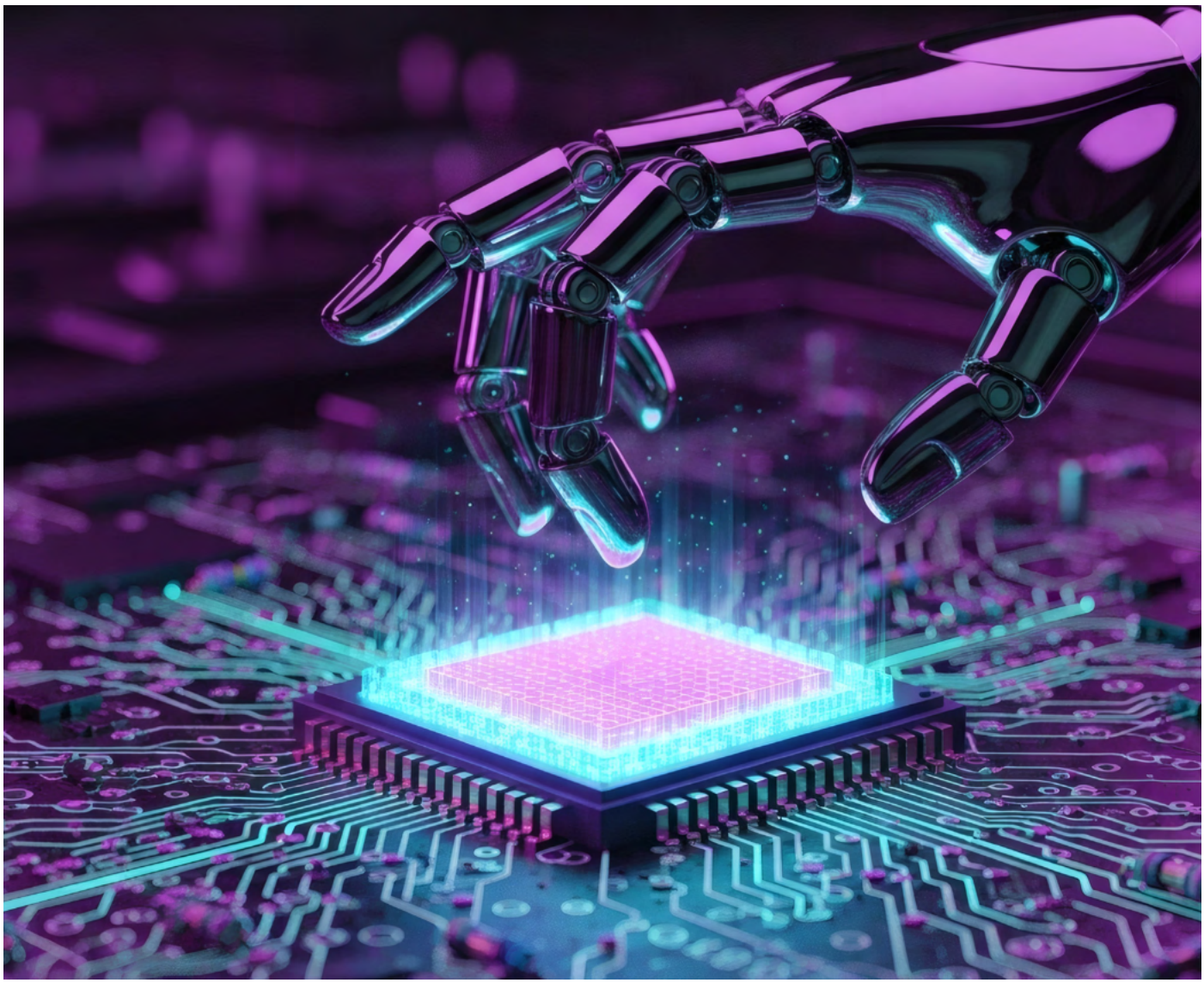


3. DORA as an accelerator of innovation and transformation

One year after DORA's entry into force, it clarifies that compliance can no longer rely solely on manual or ad hoc processes. To meet growing requirements around operational resilience and oversight of ICT providers, financial institutions must leverage advanced technological solutions capable of turning regulatory constraints into strategic enablers.

AI and RegTech solutions play a central role in this transformation: automating data collection, simplifying regulatory reporting, enabling continuous monitoring of third-party risks, and anticipating critical vulnerabilities. By embedding these tools directly into business processes, organisations do more than just reduced operational burden, they establish proactive governance that is more agile and capable to adapt to regulatory changes and external shocks.

In this sense, DORA emerges as a true accelerator of innovation and transformation, encouraging financial institutions to rethink how they manage resilience, strengthen digital sovereignty, and place compliance at the heart of operational strategy.



4. Toward increased executive accountability and a stronger resilience culture

One year after DORA's implementation, executive committee involvement in digital resilience remains at an early stage. The regulation strengthens direct accountability of senior management, with supervisory obligations and potential sanctions in case of non-compliance, underscoring that DORA compliance is not optional but a strategic imperative.

For financial institutions, this means embedding executive engagement as an ongoing governance process rather than a one-off project. Senior leaders must rely on robust monitoring, reporting, and testing systems while fostering a resilience culture across the organisation. This approach not only reduces risk and secures operations but also frees executives from day-to-day operational constraints, allowing them to focus on strategic direction and transformation.

DORA thus turns executive accountability into a strategic lever, driving the continuous and proactive integration of resilience and compliance into overall organisational governance.

Conclusion

DORA confirms its strategic importance for the European financial sector. It imposes a holistic and coordinated vision of operational resilience, encompassing not only institutions' internal systems but also the entire ICT supply chain. This collective approach reinforced by information sharing among market participants helps contain systemic risks in an increasingly interconnected financial ecosystem.

DORA also acts as a lever for digital sovereignty: by identifying critical providers, supervising dependencies, and strengthening continuity mechanisms, it enables institutions to regain greater control over essential infrastructures and services. Harmonised European standards promote a culture of shared responsibility and drive the consolidation of best practices across the sector.

However, this is only the beginning. DORA compliance is a long-term endeavour, not a one-off exercise. It must be continuously reviewed, updated, and adjusted over time to remain effective. Getting compliance right from the outset is therefore essential to avoid additional costs and risks later. Large banks already accustomed to strict supervision and complex regulatory requirements are often better prepared to meet this challenge than insurers or Tier 2 and Tier 3 banks, which will need to progressively deploy their resilience and control frameworks.

DORA redefines operational resilience, strengthens control over critical risks and digital sovereignty, and reinforces the principle that compliance is a continuous, structuring, and strategic process for the entire European financial sector.

To stay ahead, financial institutions must remain agile and proactive. This is where the support of experts such as Sopra Steria becomes crucial. With our deep understanding of regulatory developments and emerging risks, we help financial organisations not only comply with DORA requirements, but also leverage the regulation as a springboard toward a stronger, more secure future.