

DORA, A New Milestone for Financial Resilience

The importance of a unified,
pragmatic approach to compliance

DORA, A New Milestone for Financial Resilience

The importance a unified,
approach and pragmatic compliance

Contents

Preface [p.5](#)

The Rise of New Threats [p.7](#)

3 questions to Erwan Brouder,
Deputy Director of Cybersecurity,
Sopra Steria [p.11](#)

DORA, Evolving Compliance [p.13](#)

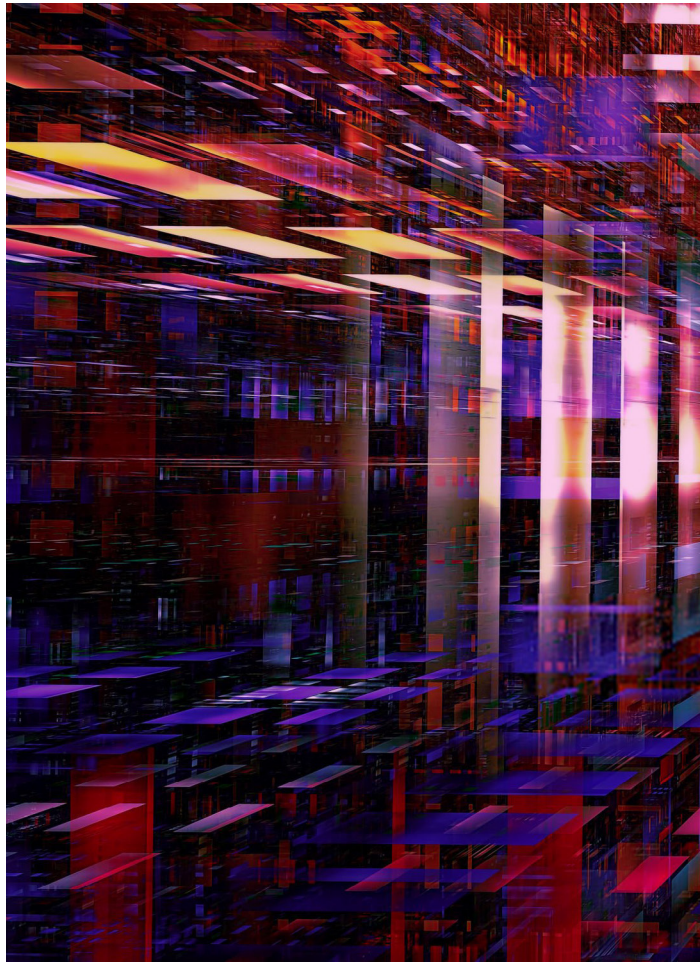
DORA, A Guide [p.19](#)

Interview with Wilfried Lauber,
Chief Information Security Officer,
Amundi Asset Management [p.25](#)

DORA, what's next? [p.27](#)

Acknowledgements [p.29](#)

Preface



In an increasingly digital world with complex interdependencies, companies in the financial sector must step up their requirements to maintain the trust of their ecosystem. While interoperability is a tremendous lever for innovation, it does expose companies to increased risks: an isolated failure can quickly spread, threatening the stability of the entire banking system. Risk management must be systematically integrated into organizational policies, ensuring adherence to established standards and fostering shared responsibility among all parties.

The **Digital Operational Resilience Act** (DORA) provides an unprecedented response to this new challenge. By harmonizing the sector's digital security standards at the European level for the first time, the regulation obliges banking institutions to adopt common risk management rules, to increase the supervision of their service providers and to strengthen their collaboration. The objective is to guarantee business continuity in the face of cyber threats while establishing a culture of digital resilience within the financial ecosystem.

However, **DORA** is only one piece of the European regulatory puzzle. It is part of a broader arsenal alongside texts such as the GDPR, the NIS 2 Directive, the Resilience of Critical Entities (RCE) and the future regulation on artificial intelligence (AI Act). In a digital world exposed to attacks of all kinds, these initiatives demonstrate a strong desire to strengthen cybersecurity and the protection of personal data and financial assets.

A cross-disciplinary approach is therefore necessary, both to ensure compliance and to control costs and possible redundancies. It also guarantees the ability of companies to anticipate future developments in the European regulatory framework.

In this white paper, we will detail the reasons why **DORA** represents an essential milestone in the digital resilience of the financial sector, while being part of a much broader regulatory landscape. We will also discuss how companies can combine compliance with opportunity in a complex and constantly changing digital environment. ●



CONTEXT

The Rise of New Threats

Interconnection with a growing number of financial and non-financial partners allows banks to enhance their offering to appeal to consumers who are increasingly keen on smooth and innovative processes. However, the opening up of IT systems has resulted in a multiplication of potential attack surfaces. As a result, in a global geopolitical environment that fosters the rise of cyber risks, the threats have become more numerous and sophisticated than ever before.

By authorizing the sharing of data between banking and non-banking players, open finance has radically transformed the ecosystem of the financial sector. Constantly striving for greater innovation and personalization, consumers are among the primary beneficiaries. However, this drive for innovation comes with a downside: heightened risks related to data security and confidentiality. Banks now depend on increasingly complex and interconnected information systems, expanding both the range of services and the number of partners or suppliers. As a result, there is a significant rise in the number of access points available to attackers, particularly in the absence of adequate supervision.

INCREASING DIGITALIZATION IN THE WORKPLACE

At the same time, digital technology has made it possible to increase the sector's productivity tenfold. Today, at the heart of banking, it is accompanied

by a explosion in cyberthreats, linked among other things to the widespread use of teleworking. For many years, virtual private networks (VPNs) have regularly been exposed to serious security flaws known as *Zero Day*, i.e. potentially exploitable by hackers even before a fix can be developed.

Added to this is the rapid adoption of new applications and technologies such as artificial intelligence, blockchain and the cloud, often provided by non-sovereign third parties. Financial institutions and their critical third parties are indeed engaged in a real innovation race to remain efficient and offer their customers the most advanced services. Many of them have thus transferred some of their IT infrastructures, applications or services to cloud computing services (IaaS, SaaS, PaaS) such as AWS, Microsoft Azure or Google to manage sensitive data, carry out online transactions or improve the accessibility of their services. This outsourcing to big tech, which can go as far as a strategic partnership in some cases, ———>

creates just as many new dependencies and new sources of vulnerability.

STRENGTHENED INTERDEPENDENCIES

The massive spread of IT outsourcing is expected to continue to increase: according to Statista, the European market could experience a compounded annual growth rate of 8.2% from 2024 to 2029, reaching a volume of 262 billion dollars by that time.

By increasing interdependencies, this rapidly growing externalization increases the risks to companies, starting with those in the banking sector. In the summer of 2024, an update from CrowdStrike, one of Microsoft's subcontractors, affected 8.5 million Windows computers. As a result, several banks saw their activity totally paralyzed for several hours, until the patch was deployed. This incident illustrates the need for stronger third-party controls to optimize the security of the entire value chain.

SOPHISTICATED CYBERATTACKS

Ransomware, phishing, data breaches... Cybercriminals have no limits other than those of their imagination. Due to the proliferation of tools at

their disposal and compromised infrastructures make their attack patterns increasingly difficult to detect. One in two companies suffered a cyber attack in 2023, a figure that is rising steadily every year. Among them, banks are prime targets: in 2023, 66% of DDoS attacks in the EMEA region targeted financial institutions. Cybercriminals also exploit artificial intelligence (AI) to analyze user habits and develop more targeted attacks. Not to mention the use of legitimate libraries, i.e. authentic files or software components that are hijacked and repurposed to infiltrate information systems without being detected.

THE CYBERSPACE, THEATER OF INTERNATIONAL CONFLICTS

Cyber risks are greatly amplified by global geopolitical instability. This is evidenced by the massive cyberattacks by hacktivists and state-backed cybercriminals during the invasion of Ukraine. Groups such as pro-Russian KillNet and NoName057 have increased the number of denial of service (DDoS) campaigns against banking infrastructures to disrupt the functioning of their services. The countries of the European Union therefore have every interest in harmonizing their defense strategy around common standards to guarantee transnational operational resilience. ●

92%

companies outsource their
IT tasks

77%

of European
companies use
cloud solutions

+182%

increase in zettabytes of data volume
between 2020 and 2025

3rd

sector most impacted by
cyber threats in 2024**, finance
is particularly targeted

33%

of employees work
remotely at least once
a week.

*Source : Sopra Steria

**"Threat Landscape" report by the European Union Agency for Cybersecurity (ENISA)



3 QUESTIONS TO

Erwan Brouder \

Deputy Director, Cybersecurity,
Sopra Steria



With DORA, we are moving from cyber risk management to digital operational resilience. What does this involve?

**Erwan Brouder ** Digital Operational resilience means the ability to ensure the continuity of an essential business process despite an incident. Under the DORA regulation, this continuity remains at the discretion of each player in the financial sector, based on several criteria including the availability of the service and the integrity of customer data. It is up to each individual to define their risks internally, but also to identify their critical third-party service providers and to set up continuous monitoring mechanisms and regular audits to verify their compliance. There is no such thing as absolute resilience. It is inevitably linked to an objective.

Can we say that there is a certain degree of flexibility within this regulatory framework?

**E.B. ** Yes, the regulations do not state that the services must be operational 24 hours a day, 7 days a week, nor that the loss of any data is a horizon to be reached tomorrow. To put it simply, DORA says: "Analyze yourself, identify the actions necessary to maintain your activity, implement them, formalize them in a contract, monitor your subcontractors to make sure

they are in the same dynamic and test them." Ultimately, it is truly part of a risk response strategy.

Is this a radical new approach?

**E.B. ** For banks and financial services operators, the implementation of resilience tests is nothing new. But this is the first time that there has been a desire to harmonize the regulation of the European financial sector, since nearly 22,000 establishments are affected by DORA. For international groups, this has the advantage of finally establishing a unified compliance framework. DORA also introduces the obligation to test the entire functional chain and the liability of company directors in the event of non-compliance. ●

« There is no resilience in absolute terms. »

Erwan Brouder
Deputy Director, Cybersecurity,
Sopra Steria

DORA: Evolving Compliance

13

\ GDPR, Cybersecurity Act (CSA), Network and Information Security (NIS) directives or Resilience of Critical Entities (RCE) Since 1995, regulations related to digital assets have multiplied and been strengthened to harmonize the rules of the European digital market. To ensure compliance while capitalizing on the transformations already undertaken, a transversal vision is therefore essential.

With the rapid expansion of the digital landscape and online transactions, new regulations have been introduced to strengthen existing laws.

The objective is to prevent the "Wild West" of the digital world, where the absence of common standards can leave data and digital transactions vulnerable to a wide range of attacks.

The effective implementation of these new technical and organizational requirements defined by RTS or regulations is no longer an option: in the event of non-compliance, companies now risk fines or increased financial penalties, most often proportional to the consolidated turnover. In this area, the General Data Protection Regulation (**GDPR**), which entered into force in all member states in May 2018, has paved the way with fines that can reach 4% of consolidated turnover. This text applies to any entity in the sector of online financial transactions, the

payment information of a natural person falls within the scope of personal data. The confidentiality, integrity, availability and traceability of this data must be guaranteed by technical and organizational means.

The **NIS1** directive, the cyber equivalent of the **GDPR**, also came into force in the same year. In view of the proliferation and severity of new threats, it has continued to evolve since 2018, giving rise to **NIS 2** in 2024. This revised version, the first act of which has been applicable to all Member States since November 5th, 2024 advocates the implementation of a zero trust guarantee, the only reasonable alternative for the protection of corporate data, infrastructure and digital services. According to this security concept, any user, device or service must potentially be considered suspicious, whether it is located inside or outside the organization's network. **NIS 2** also broadens the concept of control and management of the supply chain. It particularly targets credit institutions, which are now considered essential entities, any disruption of those services could have a major impact on public safety, security or health, or even cause a systemic risk. Failure to comply **NIS 2** is penalized by fines of up to 2% of consolidated turnover —→



« In a constantly evolving digital world, security is not optional: it is essential to the trust and sustainability of financial services. »

Marine Lecomte

Head of Offers and Innovations,
Group Financial Services Vertical

« Regulations are multiplying to keep pace with developments in the cyber environment, creating a major challenge for financial institutions : they must manage the impact of each text. »

Marine Lecomte
Head of Offers and Innovations,
Group Financial Services Vertical

October 17th, 2024 also marks the final date for the transposition and entry into force of the **RCE** Directive for the resilience of critical entities. In France, it specifically targets operators of vital importance (OVI), which include certain banks considered critical for the continuity of economic activity and national security. These will therefore have to meet the additional requirements of the new directive, which complements the requirements of **NIS 2** and allows for closer supervision by national authorities. The level of fines for violating the principles of **RCE** will be defined by each Member State.

Finally, the Cybersecurity Act (CSA), which establishes a legislative framework and unique cybersecu-

ity standards for the European area since 2019, has expanded its scope in December 2024 to include more digital products and services. Its revised version also strengthens the obligations to notify incidents to ENISA to ensure a rapid and coordinated response to cyber threats. While the **CSA** certification schemes are currently voluntary, the European Commission may be required to revise this clause for specific sectors (such as financial services) or essential products (such as connected objects).

By introducing obligations to report incidents in real time, aligning practices for incident response and the need to deploy common protocols, the **CSA** is echoing the requirements of **DORA** in terms of sharing information on cyber incidents.

Thus, DORA is coming into force in a context of continuous strengthening of cyber requirements for several years. Its deployment requires capitalizing on what has already been implemented under past regulations, but also taking into account the requirements of NIS 2 or RCE not covered by DORA or other already announced cross-cutting regulatory frameworks (AI Act, etc.). The aim will be to optimize governance and introduce new processes and tools to ensure the harmonized and consistent implementation of these various texts, with a view to ongoing and progressive compliance. —>

DORA, GDPR, NIS 2: Who is affected?

	GDPR	DORA	NIS 2
Recipients	All economic players processing personal data in the EU or concerning EU citizens	Financial and insurance institutions and their critical technology service providers	All entities medium or large considered to be major and large enterprises in the critical sectors: health, transport, energy, finance, water, telecoms and digital service providers.
Date of implementation	May 25, 2018	January 17, 2025	From October 17, 2024
Main objective	Protecting of the personal data of EU residents	Protecting of all digital assets in the financial sector	Strengthening the resilience of critical infrastructures against cyberthreats, improve cooperation between EU member states
Key requirements	Transparency, consent, security of so-called sensitive data, breach notifications	Risk management, business continuity, continuous surveillance of third parties, responses to cyber incidents	Adopting of risk management policy and technical and organizational measures to secure networks and systems
Supervisors	National data protection authorities of each member state (CNIL in France)	European Banking Authority (EBA) European Securities and Markets Authority (ESMA)	Competent national authorities of each member state
Penalties	Fines of up to 20 million euros or 4% of the annual worldwide turnover	Fines of up to 10 million euros or 5% of the annual worldwide turnover	Fines of up to 10 million euros or 2% of the annual worldwide turnover

DORA, POSSIBLE CAPITALIZATION ON GDPR REQUIREMENTS

A unified approach to compliance requires identifying the areas where there is overlap between the main regulations. Since 2018, four provisions of the GDPR have led to the development of work that could be taken up as part of the deployment of DORA, which broadens its scope.

- **Data mapping:** DORA and the GDPR both put the emphasis on the protection of personal data, its confidentiality, its integrity and its availability. Within the framework of the GDPR, the aim is to map the data and its use. DORA goes even further by requiring a comprehensive mapping of data flows and ICT assets (software, hardware, processes, etc.);
- **Knowledge of subcontracting:** The GDPR mandated that third-party service providers adhere to personal data protection standards. DORA strengthens this requirement through its fourth pillar, which expands the scope of systematic information collection by instituting a register of details on these service providers. These providers will be obligated to furnish comprehensive information about themselves, as well as their own suppliers.
- **Continuous monitoring of the compliance of subcontractors:** The GDPR requires companies to regularly test their compliance via a follow-up audit, so as to identify any shortcomings in the management of personal data and

to propose corrective measures. Similarly, pillar 4 of DORA requires continuous compliance monitoring, but extends its scope to all ICT service providers, who will have to undergo new advanced resilience tests, adapted to the threat: *Threat-Led Penetration Testing* or TLPT. Subcontracting agreements will also have to guarantee the performance of these audits and provide for regular tests of exist strategies.

- **The internal unification of the risk management system:** The GDPR requires organizations to assess the risks associated with personal data and apply appropriate technical and organizational measures to protect it. These include Data Protection Impact Assessments (DPIAs). For its part, pillar 1 of DORA (management of ICT-related risks) requires financial institutions to establish a structured framework for identifying, assessing, managing, and monitoring the risks associated with their IT infrastructures. These requirements include in particular the implementation of security controls (intrusion detection, encryption protocols, etc.), resilience tests and a business continuity and disaster recovery plan.

DORA, LEX SPECIALIS DE NIS 2

DORA and NIS 2 both aim to strengthen the resilience and security of information systems in Europe, in particular through regular risk assessments and cooperation and information sharing between the entities concerned and the authorities.

However, DORA only applies entities in the financial sector and focuses strongly on subcontractors, while NIS 2 targets the overall cybersecurity level of so-called essential and important entities (covering 18 sectors of activity) in the European Union. Another special feature is that NIS 2 is a directive – transposable by local authorities – and not a regulation.

According to the *lex specialis principle* – a specific law takes precedence over all or part of a general law – entities in the financial sector will apply the provisions contained in DORA as a priority. In the case of requirements not covered by the regulation, they will have to comply with NIS 2. From an operational point of view, the directive provides additional technical elements on subjects such as multi-factor authentication (MFA), which is explicitly required in NIS 2 but not in DORA, or data encryption: NIS 2 requires the use of advanced encryption tools to protect sensitive data, which is not explicitly covered by DORA.

Furthermore, the governance structure to be implemented will vary depending on the regulations: European Supervisory Authorities (ESAs) under DORA, compared to national authorities (such as ANSSI in France) for the additional NIS 2 requirements targeting the financial sector. ●



« The diversity of regulations requires unified compliance in order to meet the digital challenges with efficiency. »

Marine Lecomte

Head of Offers and Innovations,
Group Financial Services Vertical



869357256

DEVELOPMENT

DORA: A Guide

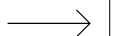
The implementation of DORA requires a coherent approach, based on a holistic regulatory vision. Driven by the general management, it will then be deployed uniformly across all business lines and entities. The time and effort required to achieve compliance may however vary depending on the pillars considered.

- Optimization of third-party management, greatly reinforced by the **DORA** regulation. The new contractual requirements and the implementation of the subcontractor information register are among the most time-consuming projects
- The integration of DORA by design project methodologies in all new projects to guarantee their success without compromising the overall compliance of the financial institution.

A FEDERAL STRATEGY GUIDED BY THE GENERAL DIRECTORATE

One of the major new features of **DORA** is the involvement of management bodies in ensuring compliance, with the possibility of administrative and criminal sanctions in the event of non-compliance. The objective is to make managers accountable and to guarantee the dissemination of a culture of resilience throughout the organization via a top-down approach.

This paradigm shift will require the implementation of cybersecurity awareness programs and training in digital operational resilience for members of the Executive Committee and Executive Board. This is an essential step to enable managers to set priorities, allocate the necessary resources and ensure that compliance obligations are met at the level of each entity. To carry out these tasks successfully, they will need to equip themselves with comprehensive governance tools to improve their risk vision and monitoring of the implementation of the required actions.



At the entry into force of **DORA**, the financial institutions display varying degrees of maturity. The only certainty is that compliance can only be achieved gradually, and the challenges that remain after the deadline of January 17 are numerous. By 2025, it should already be possible to get to grips with four major issues:

- The effective deployment of a system of federated governance, driven from the general management, to harmonize internal practices;
- The implementation of the new resilience tests, particularly the TLPT, the first campaigns of which will mainly be conducted in 2025, is expected to be complex due to the large number of teams involved.

In terms of professions, the implementation of **DORA** involves a resolutely cross-disciplinary approach involving different teams: compliance for regulatory aspects, risk management, legal affairs, purchasing, as well as information systems security (CISO), but also different entities to guarantee the pooling of practices. This coordination, which is essential to avoid any fragmentation in the risk management strategy, will require upstream clarification of the responsibilities of each department.

For large establishments with numerous entities, a federated organization, i.e. coordinated by a central body and shared with the entities, will ensure a homogeneous compliance. It will be supplemented by the appointment of correspondents in each entity. The main benefits of such an approach are:

- **Improved surveillance and control** through unified risk management and the establishment of standardized operational resilience protocols;
- **The effectiveness of the response to cyber incidents**, thanks to more prompt escalation of incidents and centralization of major ICT incident reports;
- **Consistent monitoring of compliance** and the optimized allocation of resources, guaranteeing greater efficiency in the event of regulatory control;
- **Optimization of third-party management**, with the obligation to review the clauses of all subcontracting contracts according to Group models.

NEW RESILIENCE TESTS TO BE DEPLOYED

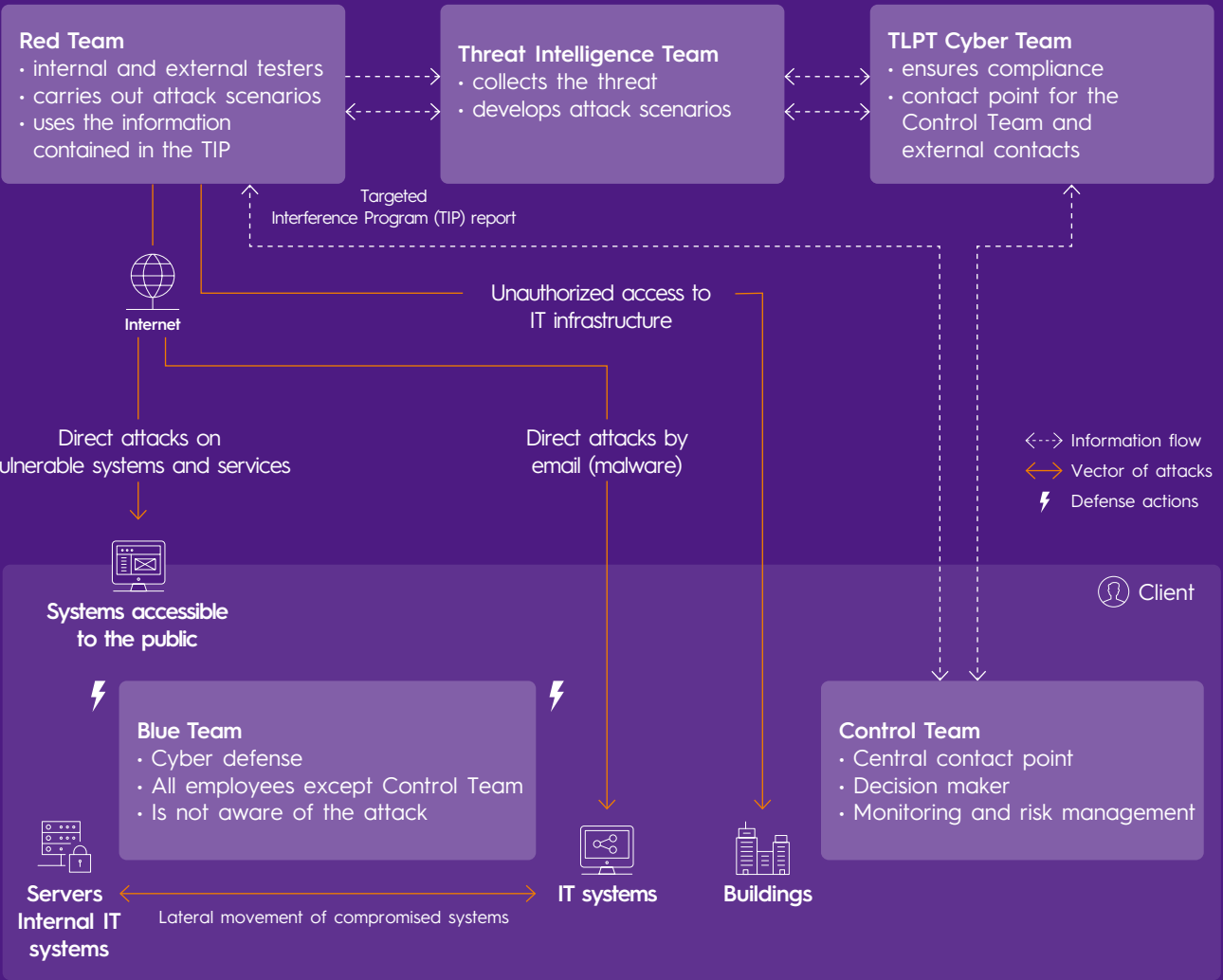
Faced with a threat that is constantly evolving and strengthening, DORA introduces the concept of Threat Led Penetration Testing (TLPT), to be carried out in part by an independent external team. These tests are a key tool for assessing resilience to cyber threats and identifying potential vulnerabilities in critical infrastructure. DORA requires them to be carried out at least every three years on banks' own information systems and on those of the most critical subcontractors.

Unlike traditional penetration tests, which follow a standardized approach, TLPT tests the resilience of critical infrastructure based on plausible attack scenarios. It thus prepares companies for the real threats that could compromise their operations.

To guarantee the realism of the tests and thus optimize the preparation for attacks, the dedicated external team will combine an approach based on both Red Team and *Cyber Threat Intelligence* (CTI) skills. The latter provides a *Targeted Threat Intelligence Report* (TTIR), which aims to transform threat analysis into actionable scenarios for use in directed intrusion tests. A well-structured TTIR thus allows defensive efforts to be contextualized and prioritized against the most probable and most impactful threats.

The first Threat Led Penetration Testing campaigns (TLPT) began in 2024 and will continue well into 2025. The implementation of a methodology

TIBER-EU: A framework dedicated to the conduct of TLPT



Driving a public transportation vehicle

This relies on the coordination of several teams:

- | | | | |
|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The Threat Intelligence Team,
which provides actionable information on current and emerging threats</p> | <p>The Red Team,
which simulates the role of an external or internal attacker based on plausible scenarios</p> | <p>The Blue Team,
responsible for defending the information systems of the organization as if it were a real attack</p> | <p>The Control Team,
which objectively evaluates the actions of the Red Team and the Blue Team and ensures that the test is conducted without compromising the organization's real operations or violating laws and regulations</p> |
|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

will be essential to guarantee its success and ensure that these tests effectively contribute to greater resilience in the banking sector.

THIRD-PARTY MANAGEMENT TO BE OPTIMIZED

In a context marked by the constant growth of outsourcing, the use of third-party solutions and the rise of interdependence between financial institutions, the management of subcontractors is one of the fundamental pillars of DORA. For financial institutions, it is also one of the most complex aspects to implement, as it requires close coordination between numerous actors – internal teams, critical subcontractors, regulatory authorities – as well as the meticulous execution of tasks that are often time-consuming. It is therefore easy to understand that this pillar is the one in which the banks are the most behind.

To meet the new requirements, the financial players will have to create a complete register of their service providers including information on their criticality level, the expected services, the respective responsibilities and the documentation of incidents. The next step will be to adjust the contractual clauses, particularly those relating to the reversibility of contracts and business continuity. These will be delicate discussions with the largest service providers, who are likely to oppose DORA with their own contractual standards.

In addition to this upgrade, DORA provides for specific clauses allowing institutions

to carry out regular audits and checks to verify the service provider's ability to meet digital resilience obligations.

These controls are not limited to a simple cyber vision: they must take into account the hyper-systemic nature of the risk. In the context of resilience tests and crisis simulations, Article 18 requires banking organizations to notify the competent authority of any significant cybersecurity incident within four hours of its detection, as well as the incident management measures in place. As these incidents can be caused by the subcontractors themselves, it is therefore imperative to strengthen the means of control.

While compliance – and its maintenance over time – suggests a high consumption of resources, this could be offset by the judicious use of new technologies, in addition to effective human intervention. One example is the contribution of artificial intelligence, which will enable it to identify contractual deviations more quickly and suggest corrective measures. AI could also help to establish and carry out control plans.

DORA BY DESIGN IN A NEW CLOUD PROJECT

The selection of a cloud provider must now be inline with DORA requirements:

- **more demanding contractualization**, to be anticipated from the provider selection phase, particularly with regard to exit clauses;
- **more refined governance** with systematic training teams using the cloud;
- **better census of the active population** and more systematic reporting of incidents, ensuring access to data on performance and service continuity;
- **plans that ensure** resilience and continuity

Imposing a DORA *by design* framework on major cloud providers can be complex. On the plus side, cloud solutions natively address most requirements for business continuity and disaster recovery, particularly through resilience testing.

The main providers (e.g. AWS) also make it possible to define environments, including backup spaces, according to geographical criteria that comply with regulations. Finally, they provide evidence of compliance: technical reports, third-party certification, and control methodologies.

However, these provisions are insufficient in view of the new

regulatory requirements. Customers remain responsible for the management of critical requirements, which involves, for example, the revision of standard clauses. In addition, cloud providers offer multiple service ranges, each of which requires specific measures.

In any case, it will be important to ensure the commitment of suppliers to meeting deadlines for reporting incidents and to verify the control of their own subcontracting. In France, ANSSI has published a list of recommendations for cloud hosting and may request that essential entities comply (or even require it for operators of vital importance).

NEW PROJECTS DORA BY DESIGN

To guarantee long-term compliance and avoid costly adjustments after the fact, the systematization of a DORA *by design* methodology must be imposed as of today in all new development projects, following the example of the principles adopted during the implementation of the **GDPR**. In concrete terms, each stage of the project, from the choice of service providers to the definition of data flows, will have to include strict security and resilience criteria, based in particular on monitoring and audit procedures as well as operational tests.

In this context, it is recommended that project managers and technical teams be trained in the specifics of DORA and that they be provided with the necessary tools and resources to assess the impact of each new project on digital security and operational resilience. DORA by design therefore represents a new culture of compliance and security, geared towards operational sustainability and proactive protection against digital risks. It thus helps to strengthen the confidence of stakeholders and the stability of financial institutions.



INTERVIEW

Wilfried Lauber

\ Chief Information Security
Officer, Amundi Asset Management

« The advantage of DORA is that it allows for a certain degree of flexibility. »

When and how did you start the industrialization of third-party management? Which business divisions were involved?

Wilfried Lauber \ At Amundi, we have prepared from 2022 to compliance, with the completion of our gap analysis. This first step was followed in 2023 by the updating of the risk mapping and the actions to be taken. We then structured our approach by coordinating the various functions concerned: IT of course, but also risk, compliance, legal and purchasing. Once the governance structures had been defined, we were able to operate in project mode throughout 2024, with regular reporting to the general management, the project sponsor.

Beyond the necessary work of reviewing subcontractors, what tools have you put in place to assess their cyber risk from onboarding and throughout the life of the contract?

W.L. \ We were fortunate to have an internal tool developed by Amundi Technology dedicated to monitoring all contracts. We simply updated it to be able to collect all the information required under DORA and to be able to carry out the reporting expected by the regulator. What makes us special is that we wear two hats as both a management company and a provider of technological solutions: we offer our own portfolio management platform, ALTO Investment, to other asset managers. Compliance with DORA has enabled us to integrate the expected requirements quite naturally, this time as a third-party service provider. We can thus guarantee to our clients that we apply internally on ALTO the level of security required by our clients from their service providers.

The industrialization of third-party management does not prevent human intervention, particularly on sensitive clauses such as reversibility. What is your feedback on this subject?

W.L. \ We are currently looking into ways of implementing this clause. Identifying the publisher to whom one could switch services in the event of an incident requires testing procedures, which in turn require retrieving one's data in order to transfer it to a potential competitor. This seems difficult to achieve during the term of the contract. Ideally, these tests should be carried out before signing, so that data can be transferred quickly if necessary. We are therefore in the process of reviewing our

selection process to integrate the reversibility phase from the start of the contract. The advantage of DORA is that it allows for a certain amount of flexibility: each company remains free to define its own action plan.

With just a few weeks to go before DORA* comes into force, how would you rate your progress?

W.L. \ The management of third parties is the only project that will not be finalized by January 17th, 2025 as the duration of contractual renegotiations is unpredictable by nature. Several service providers have already rejected our proposals, which means that the discussions will take some time. The aim is to prioritize the review of clauses with our critical service providers, i.e. those whose failure could have serious impacts on our activity.

To conclude, would you say that DORA is more of a constraint or an opportunity for the banking industry?

W.L. This text will force the management of every company to address the issue of cybersecurity and operational resilience. In this sense, I think it is a real opportunity to highlight the issues related to these new risks and to reconsider them at the highest level. In addition, the supervision that will be carried out by regulators on systemic critical service providers will benefit the entire European market because the overall level of operational resilience will be strengthened. DORA is not just a tech topic, far from it! Moreover, the text bridges the gap between two worlds that are not used to communicating with each other, namely the legal world and the world of cybersecurity. A wide gap that should also generate positive spin-offs.

** Interview conducted in December 2024*



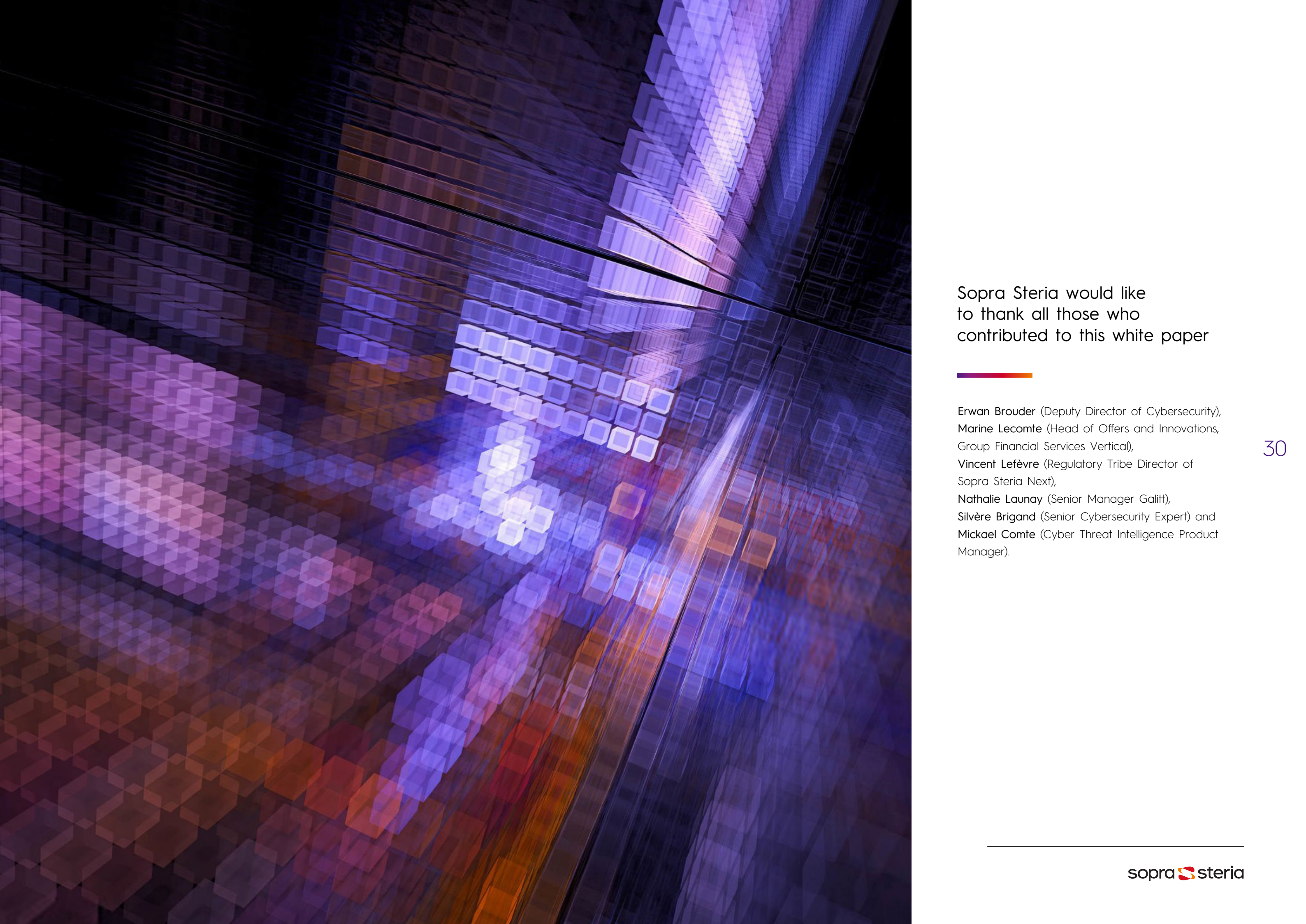
DORA, what's next?

The digital operational resilience advocated by **DORA** goes far beyond the mere issue of asset protection. The aim is to build a more secure digital Europe by guaranteeing the availability and integrity of financial services, including in the event of a major incident. For banks, the time has come to transform this new constraint into a real strategic lever, with a dual objective: to build a more resilient future and anticipate the next standards.

The **Cyber Resilience Act** (CRA), which came into force on November 12, 2024 and is applicable from December 11th, 2027 is already on their agenda. This European regulation establishes common cybersecurity standards for products with digital elements (connected hardware and software, for example). Financial entities using these products will not only have to comply with **DORA** requirements for operational resilience but also with **CRA** requirements for cybersecurity.

For its part, the AI Act, the first measures of which will be applicable from February 2025, will complement this system by regulating the use of AI through new standards of security and transparency. It targets companies developing or using artificial intelligence systems in so-called "high-risk" sectors such as finance, healthcare or recruitment, with requirements that partially overlap those of DORA. Any breach of the AI Act can lead to fines of up to 7% of consolidated turnover.

In this increasingly dense regulatory landscape, a global, coherent and agile compliance strategy is essential. Far from being an end in itself, DORA symbolizes a crucial new stage in strengthening the resilience of the financial sector. By embracing its requirements, all stakeholders - institutions, clients and partners - will benefit from a financial ecosystem that is safer, more robust and better prepared for the challenges of tomorrow. ●



Sopra Steria would like
to thank all those who
contributed to this white paper

Erwan Brouder (Deputy Director of Cybersecurity),
Marine Lecomte (Head of Offers and Innovations,
Group Financial Services Vertical),
Vincent Lefèvre (Regulatory Tribe Director of
Sopra Steria Next),
Nathalie Launay (Senior Manager Galitt),
Silvère Brigand (Senior Cybersecurity Expert) and
Mickael Comte (Cyber Threat Intelligence Product
Manager).