DORA

The 10 key challenges of a successful compliance journey

Bringing together all aspects of digital operational resilience

December 2023

pwc

Let’s Change the Way We See Risk

Acknowledgements

The messages mentioned in this document are those delivered at the conference “DORA Regulation: overview, main challenges and experience feedback” held on 24 November, 2022 by PwC France et Maghreb.

We would particularly like to thank the two main speakers during this conference:

Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management, AXA
Caroline Cerval, Chief Operating Officer, Head of Operations and Technology, LCH SA

This document was written with the contribution of PwC experts on the subject:

Romain Camus, Technology Risk Partner, Banking sector, PwC France et Maghreb
Karine Pariente, Technology Risk Partner, Insurance sector, PwC France et Maghreb
Jamal Basrire, Partner in charge of Cyber Intelligence activities, PwC France et Maghreb

We would also like to thank the Regulatory Centre of Excellence of PwC France et Maghreb:

Monique Tavares, Director, Banking sector
Olfa Ehrhard, Senior Manager, Insurance sector

Contents

What is DORA?

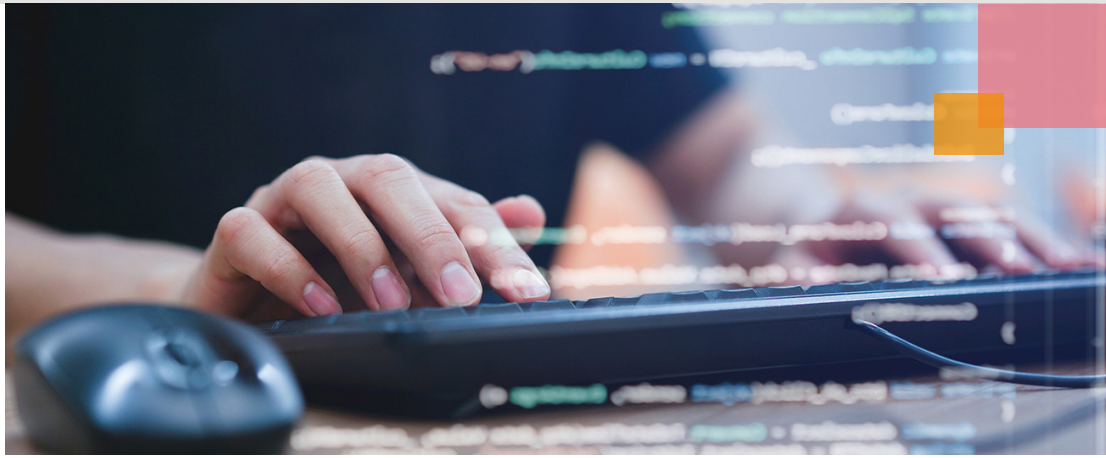
The “Digital Operational Resilience Act”, commonly known as “DORA”, is a European regulation[1] that aims to strengthen the digital operational resilience of the financial sector in a context of deep digital business transformation and an increased exposure to cyber and IT risks. It came into force on 16 January, 2023 and will be applicable from 17 January, 2025 across all EU member states.

Resilience is a challenge for financial service firms and the sector as a whole. Given an increase in cyber attacks and the interconnected nature of the financial system the profile of resilience has been elevated significantly. “Banks and insurance companies need access to an increasing volume of internal and external data.They have become increasingly reliant on information and communications technology third-parties. European regulators therefore want to take steps to establish the risk generated by these developments is managed effectively”, explains Karine Pariente, Partner, PwC France

“With the increasing use of digital technologies comes an increased cyber risk exposure which is a potential source of instability for the financial sector”, adds Jamal Basrire, Partner, PwC France.

Regulators and supervisors previously focused on strengthening their financial resilience. The DORA regulation creates a regulatory framework on digital operational resilience, whereby all financial entities need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats.

The concept of operational resilience thus emphasises the need to shift the approach to operational risk management from a focus on risk prevention and loss mitigation, to a broader and proactive approach. This assumes that incidents will occur and that we must be prepared to deal with them and ensure the continuity of critical and/or important core business activities and services.



Thus, the DORA regulation identifies and proposes requirements for five key pillars that financial entities will be required to comply with, specifically:

- ICT risk management framework,
- ICT incident management, including a more streamlined reporting to the relevant authorities,
- Digital operational resilience testing,
- ICT third-party risk management including an oversight framework of critical ICT third-party service providers operating at EU level,
- Information sharing on cyber threats.

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of December 14, 2022 on the digital operational resilience of the financial sector

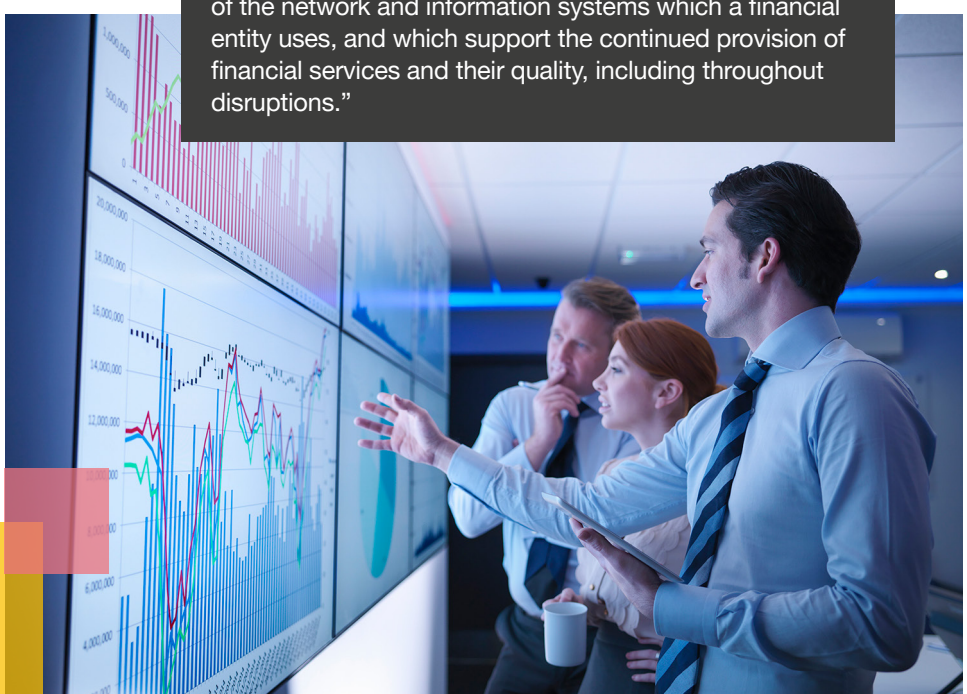
For the first time at EU level, the DORA regulation sets, in a single piece of legislation, a detailed and comprehensive framework on digital operational resilience for financial entities.

The 5 pillars of digital operational resilience

1. ICT risk management framework
2. ICT-related incident management, classification and reporting
3. Digital operational resilience testing
4. ICT third-party risk management and oversight framework
5. Information sharing on cyber threats

What does digital operational resilience mean? According to DORA:

"The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions."



What is the scope of DORA?

The DORA Regulation applies to a wide range of financial institutions as well as to service providers providing ICT services to financial entities within the EU.

Financial entities

- Credit institutions
- Payment institutions
- Electronic money institutions
- Investment firms
- Management companies and AIF managers
- Account Information Service Providers or “bank account aggregators”
- Crypto-asset service providers as authorised under MiCA regulation

- Insurance and reinsurance companies
- Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
- Institutions for occupational retirement provision

Note: Regulatory requirements are scaled based on size criteria

- Central counterparties
- Central securities depositories
- Trading venues and repositories
- Data reporting service providers
- Credit rating agencies, administrators of critical benchmarks
- Crowdfunding service providers

ICT third-party service providers

Firms that provide digital and data services through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.

ICT third-party risk management framework

The following are considered to be ICT service providers:

- ICT intra-group service providers that provide predominantly ICT services to their parent undertakings, or to subsidiaries or branches of their parent company
- Financial entities that provide ICT services to other financial entities
- Participants in the payment services ecosystem

Oversight framework

ICT service providers designated as “critical” with the exception of:

- Financial entities that provide ICT services to other financial entities
- ICT intra-group service providers
- ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks of the European banking system

Challenge #1 Understand the regulatory approach

Although DORA is aligned with the principle of previous guidelines provided by the regulators, the new regulation is a game changer. The level of expectation has increased even more. This has to be acknowledged before getting to understand the specific requirements of DORA.

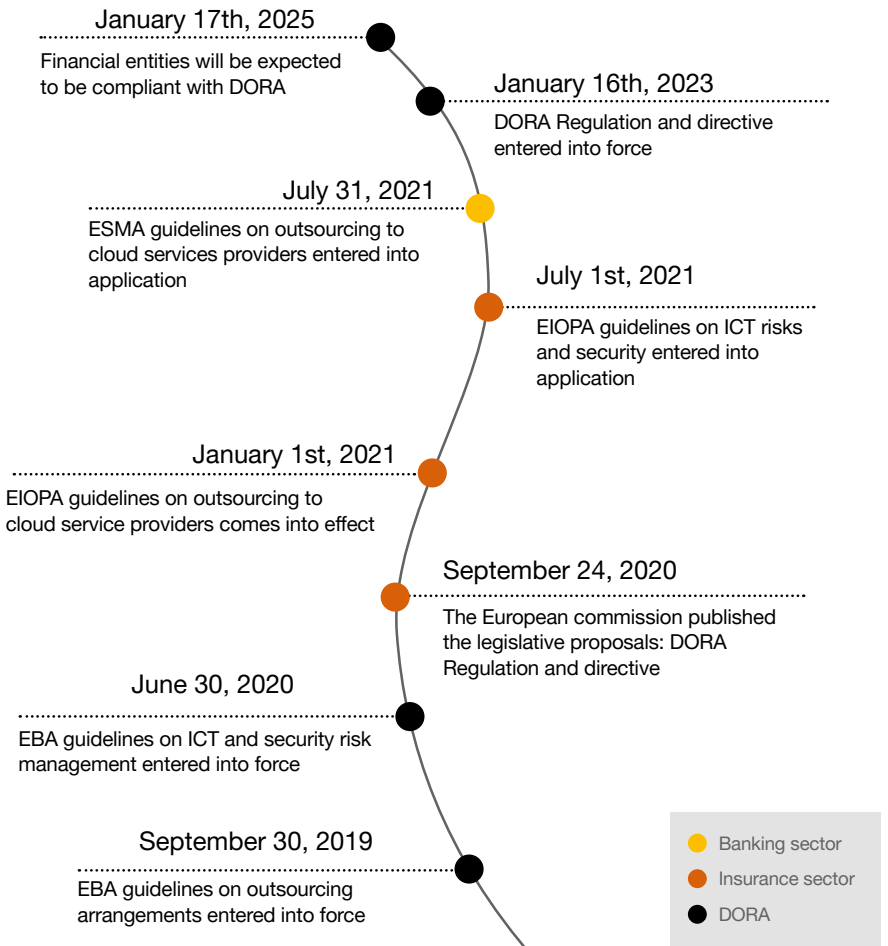
The existing regulatory environment for banks includes requirements such as the European Banking Authority guidelines on outsourcing, ICT and security risk management. Additionally the European Securities and Markets Authority guidelines on outsourcing to cloud service providers. As far as insurance companies are concerned, several texts mirror those impacting banks, with, for example, the European Insurance and Occupational Pensions Authority guidelines on outsourcing to cloud service providers.

So many topics related to risk management and digital operational resilience will now be under one umbrella: DORA. "*Until now, the current regulatory framework was fragmented and heterogeneous.*

There were various sectoral regulations, but they were of different levels and more or less restrictive. This has led to overlaps, different interpretations in different European countries and, ultimately, to very high compliance costs.

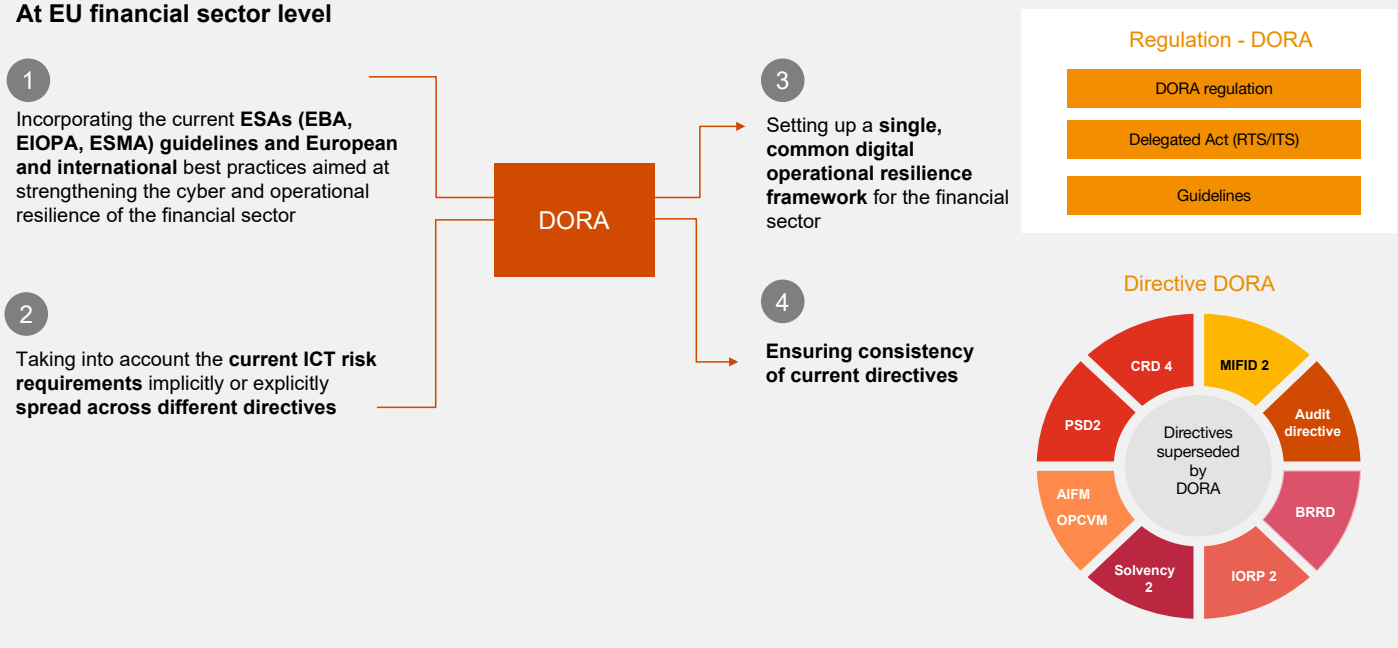
DORA sets a single regulatory framework, incorporating all the previous guidelines issued by the European supervisory authorities as well as the european and international best practices in cyber resilience and ICT risk management. The new regulation will, in a way, make all existing texts consistent in terms of IT risk, cybersecurity, third-party management and business continuity", explains Karine Pariente, Partner, PwC France.

Progressive strengthening and harmonisation of sectoral requirements on ICT risk management



In addition to the DORA regulation, the related directive[2] will also amend the current directives in order to bring them into line with the provisions of the regulation. For example, credit institutions will be required to report operational or payment security incidents - previously reported under the Payment Service Directive 2- under DORA. DORA came into force on 16 January, 2023 and must be transposed by the Member States by 17 January, 2025.

Building a harmonised and consistent regulatory framework



2 Directive (EU) 2022/2556 of the European Parliament and of the Council of December 14, 2022

Overall, the regulatory approach is based on three main principles:

1. Convergence

For the first time in Europe, regulators are getting together to address the risks related to information and communication technology (ICT) and to define the core principles and main elements to overcome these operational and IT challenges.

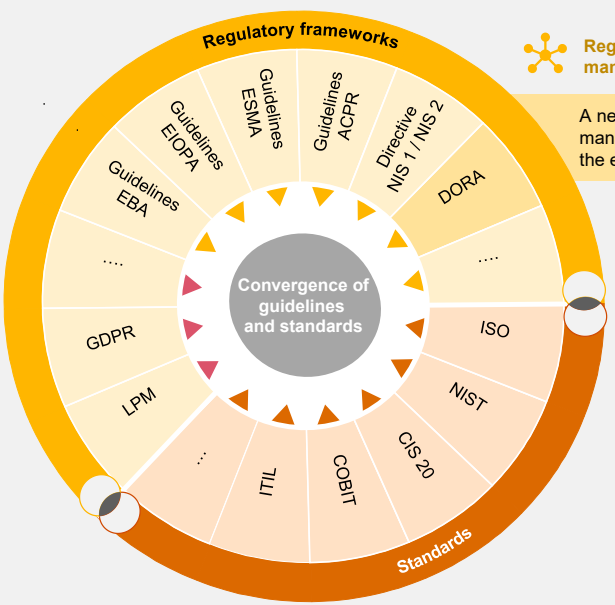
"*We are counting on DORA to provide a common language and an aligned timeline, as opposed to the many divergent requirements today in the countries where we operate*", explains Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA.

However, financial entities still need to be able to rely on all the work already done in the framework of the various regulations, whether in the areas of third-party risk management, business continuity or cybersecurity, and not start from scratch...

"*For example, our cybersecurity strategy has been ambitious for several years, with waves of major investments and the implementation of controls to strengthen the security of our operations. Recently, we have updated this strategy to ensure a better coverage of the attack surface*", states Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA.

This will also require a convergence of the organisation and risk management approaches: "*The convergence principle will most likely lead organizations to consolidate their risk management approach to address silos we can sometimes observe in organizations between IT, Cyber, Business Continuity, Third-Party Risk Management*", explains Jamal Basrire, Partner, PwC France.

Capitalise on the convergence of texts and on the efforts already undertaken



Regulatory trends: converge and harmonise the regulatory frameworks for ICT and security risk management.

A new regulatory framework converging EBA, EIOPA and ESMA guidance on ICT and security risk management, with new requirements to strengthen and harmonise ICT and security risk management for the entire financial sector.

Key objectives of convergence

- **Simplify compliance** by consolidating applicable regulatory requirements in a single framework
- **Build a robust, comprehenzive and compliant** transformation program to optimize compliance process efforts
- **Facilitate reporting** to regulators and management bodies
- Identify synergies with new regulatory frameworks and **anticipate compliance** with additional new requirements

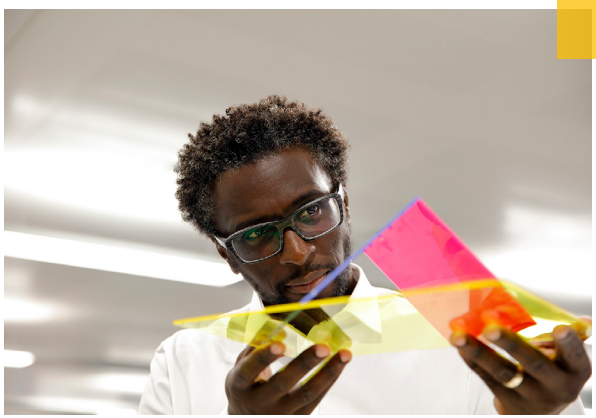
It is by capitalising on their recent and previous works that financial entities can manage to improve their resilience without complexifying the organisation. "*We can even hope that, in the end, the text will simplify compliance for financial entities*", says Romain Camus, Partner, PwC France.

2. Proportionality

Under the principle of proportionality, financial entities must implement the requirements whilst taking into account their size and overall risk profile as well as the nature, scope and complexity of their services, activities and operations. Indeed: "*Given the large spectrum of DORA, it is essential to calibrate its efforts and the level of depth of its actions to the business context and the risks to which it is exposed*", explains Jamal Basrire Partner, PwC France.

3. Promotion of the *"security by design"* principle

Finally, the approach integrates the general principle of "security by design", i.e. the idea that security must be thought from the design of products and services, right through to its distribution to customers and throughout the entire life cycle and by imposing this issue at the heart of Institutional governance. This also implies developing an overall vision of the ICT supply chain and assessing its resilience.



Challenge #2 Start as soon as possible

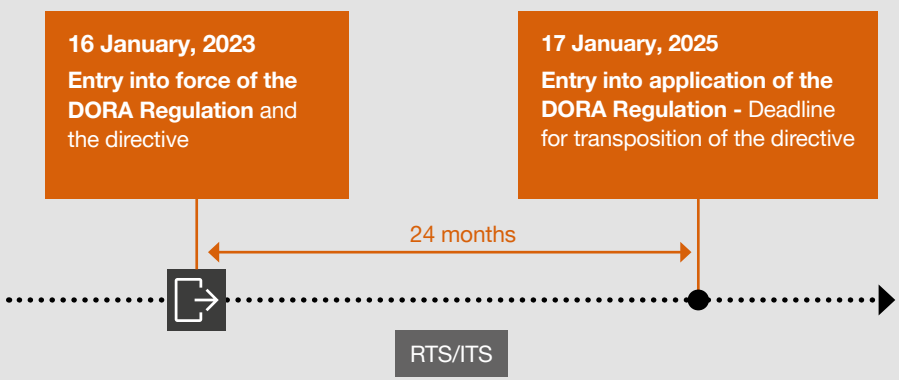
Financial entities were given two years to prepare for the new European regulation. A period that might seem sufficient... But, in reality, the financial entities that have already started to work on the subject have already realised that it will require a lot of work.

"*We started working on DORA in early 2022. First, we had to identify and classify the profiles of risks of the third parties we work with. Then work on the interdependencies between information systems, processes, data, etc. Risk management is at the heart of our business, but in the cyber domain, it requires change management and the appropriation of cyber risks by the business lines and by all levels of management*", explains Caroline Cerval, Chief Operating Officer, Head of Operations and Technology - LCH SA.

Planning for compliance with DORA by the 17 January 2025 deadline must take into account the regulatory technical standards (RTSs) which are yet to be finalized. These standards further specify the DORA requirements and introduce additional details. The RTSs are prepared in two batches and must be submitted for adoption by the EU commission at the latest 17 January 2024 and 17 July 2024 respectively. At the time of this report, the draft of the first batch of RTSs have been released for public consultation. The release of the second batch is expected for November or December 2023. "*When the detailed texts are published (RTS/ITS), there will be less than a year left to implement them: that's a very short time in terms of technological risk*", says Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA.

Application from 17 January, 2025

Key dates



The ESAs will have to submit RTS/ITS to the European Commission by the following deadlines and in particular on the subjects listed below:

- **By 17 January, 2024:** ICT risk management tools, methodologies, processes and policies; Simplified framework; Incident and cyber threat classification; Risk strategy for ICT third party service providers; Standard templates for the ICT service provider information registry including information common to all contractual arrangements for the use of ICT services
- **By 17 July, 2024**: Content and templates for notification reports; Advanced testing; Outsourcing of ICT services; Oversight of critical ICT service providers

The fact remains that, even without having the finalised versions of the level 2 texts, it is necessary to move forward with the work... "*This can be destabilising, but many elements of the future texts are known and the current rules can already be a source of inspiration*", says Karine Pariente, Partner, PwC France.

The major steps of the roadmap are already known. "*It is possible to work now on the gap analysis between the system implemented by the company and the expectations described in the DORA regulation. It is also necessary to define the action plan in the light of an analysis of the company's context (evolution of the business model, particularly in the context of digitalisation, geographical presence, interconnections with third-party partners/suppliers/customers, etc.) and its risks. The principle of proportionality then allows to adapt the system in place to the company's context",* explains Jamal Basrire, Partner, PwC France.

Implementing this work means confirming that strong governance is in place.

Challenge #3 Adapt governance and raise management awareness

Governance is a central challenge in the new regulation: the objective is to develop a holistic risk governance to ensure digital operational resilience, a new paradigm brought about by DORA. "*We will have to break silos that sometimes exist between IT, cyber, third-party and business continuity risk management. A revolution, or almost, for many financial entities: until recently, the "BCP" (Business Continuity Plans) were the only way to manage risks. Many institutions' business continuity plans did not take into account cyber risk, even though ransomware attacks will be one of the main threats in 2022 that could lead to a major information system disruption*", explains Jamal Basrire, Partner, PwC France.

In practice, financial entities need to put in place or continue to put in place governance rules that enable them to evaluate effective and prudent management of ICT-related risks and achieve a "high level" of digital operational resilience.

The Regulator entrusts the management body with the responsibility of implementing the ICT risk management and monitoring system. In particular, it is responsible for :

- Defining the digital business resiliency strategy, including determining the level of risk tolerance for ICT,
- Approval, oversight and periodic review of the ICT business continuity policy and ICT response and recovery plans,
- Approval and review of audit plans and ICT audits,
- Review of at least the major ICT incidents, their impact and the response, recovery and remediation measures implemented
- Approval and review of the policy for the use of ICT services provided by third parties and review of new contracts or amendments to existing contracts,
- The allocation of the necessary recourses

As a result, risk management governance will need to be revisited to incorporate the digital operational resilience paradigm while preserving the three-line model of defence, allowing in particular to challenge the systems in place. Indeed, financial entities will have to ensure an adequate separation of IT management functions, control functions and internal audit functions.

The ICT risk management framework must be documented and reviewed at least once a year.

The management body must have relevant skills

To achieve this, awareness and training efforts will also have to be undertaken: "*IT risk governance is part of the mandate of our CIOs, and, more broadly, topics such as knowledge of the IT assets or obsolescence management are discussed during Risk Committees or the Management Committee*", explains Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA. However, due to the rapid evolution of threats, it will be necessary to reinforce the skills of the members of the management body in order to fulfil their responsibilities: expectations on maintaining an up-to-date knowledge on cyber and IT risks

Challenge #4 Involve the right stakeholders

Point of attention: DORA is not just about cybersecurity! It is true that the text deals with cyber risk and the security of networks and information systems; However, it concerns many other areas: third-party risks, business continuity, IT risks, etc. "*Operational resilience touches on much broader challenges than just IT security. IT should not be seen as the owner of DORA compliance which is a more broader Risk challenge*", says Jamal Basrire, Partner, PwC France.

In fact, this is a strategic subject, which must be treated as such: at a strategic level, at the executive level, with the support of the company's top management. In addition to IT and cyber managers, many other functions must be made aware of the subject and involved in the project. First and foremost, top management.

"*The main challenge will be to coordinate actions with the main stakeholders involved. This requires strengthening governance and can only be achieved by involving top management*", emphasises Karine Pariente, Partner, PwC France

As this is an operational risk challenge, most market players have generally positioned the subject at the level of the Risk or Compliance Department, with strong contributions expected from the IT Department, security managers, business continuity teams, purchasing and legal departments (for service contracts with third parties).

DORA compliance must involve all stakeholders: business, risk, IT operations and cybersecurity

Challenge #5 Identify the interlinks with current and upcoming regulations

As previously mentioned, the deadlines are short and work must begin now to comply with the regulation and to monitor future drafts of Regulatory Technical Standards and Implementing Technical Standards . "*It is also essential to consider DORA in the overall regulatory landscape, especially with the new NIS 2 directive*[3]", says Jamal Basrire, Partner, PwC France.

Indeed, the DORA regulation is linked to the new NIS 2 directive (the revised version of the NIS directive that was adopted by the EU on 28th November 2022), which came into force on 16 January, 2023, and which defines the horizontal framework of minimummeasures to ensure a common high level of cybersecurity throughout the EU. The DORA regulation is the "lex specialis" for the financial sector with regard to cybersecurity risk management measures and incident reporting requirements.

It will be all the more necessary to have an overall reading of the two texts as the scope of application of the NIS 2 directive is extended to all medium and large entities in the sectors of activity covered by the directive ("essential and significant entities"), and no longer only to entities designated as operators of essential services (OES). The NIS 2 directive must be transposed by Member States by 17 October, 2024.

In addition to this initiative, it will also be necessary to make the link with other current or ongoing legislative initiatives on cybersecurity. First of all with the cybersecurity regulation effective since 2019: for certain categories of critical and important entities that will be required under the NIS 2 directive to certify certain ICT products, services or processes developed by entities or acquired from third parties in accordance with this regulation. Also to be followed is the proposed Cyber Resilience Act, published on September 15, 2022, which did specify cybersecurity requirements applicable when developing or distributing products and services with digital elements.

The objectives of all of these initiatives are to strengthen the security of ICT assets but also of the entire ICT supply chain.

3 Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022

Challenge #6 Leverage on current initiatives with a resilience perspective

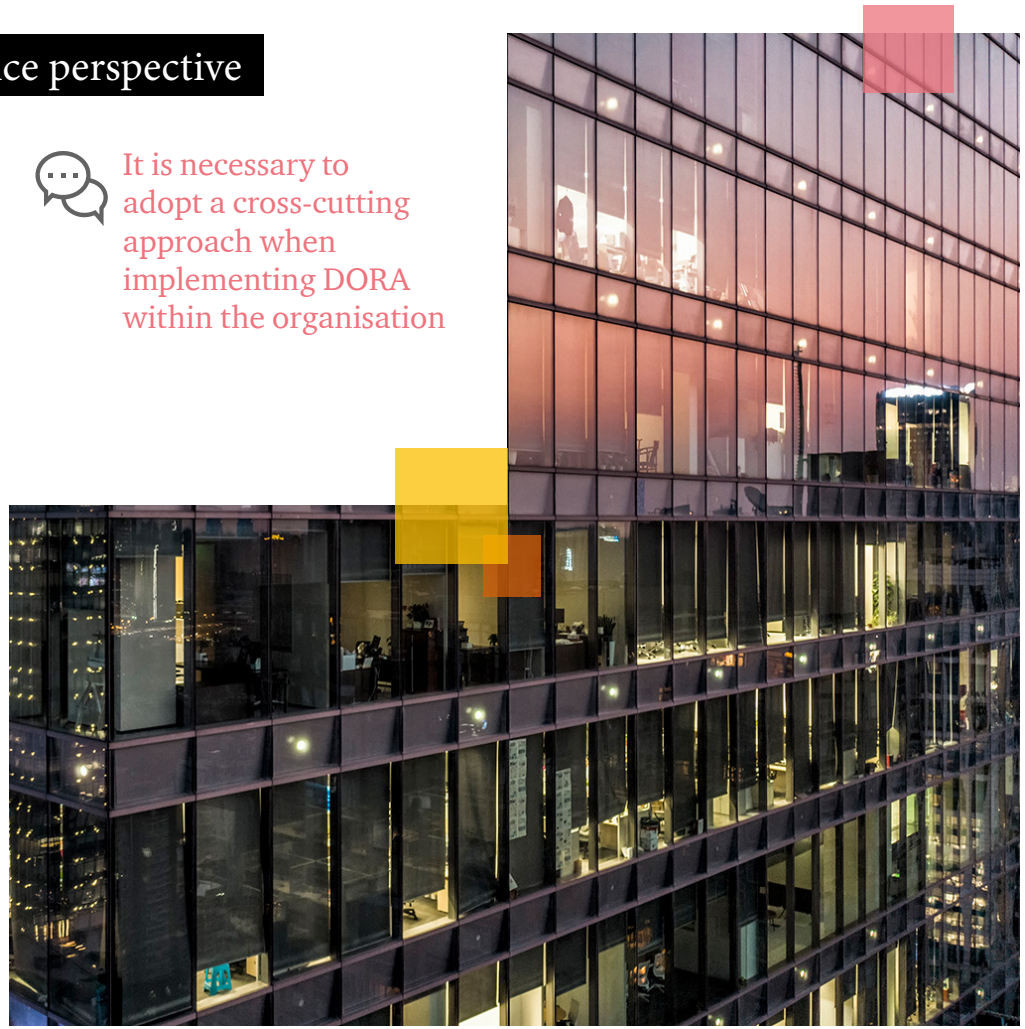
For the more mature financial entities, which have already worked hard on the current rules around IT risk management, cybersecurity or Third Party Management there could be less uplift.

The evolution will focus on the development of a holistic vision of the subject through the digital operational resilience strategy and the consideration of the depth of the requirements. The evolution will be more or less important depending on the extent to which risk management is considered through the prism of resilience and integrated resilience in governance bodies. "*The fragmented and siloed approaches to risk management have allowed us to grow in maturity on these different subjects, but this does not allow us to address the new paradigm that DORA brings*", underlines Jamal Basrire, Partner, PwC France

Thus, if the convergence of the texts makes it possible to capitalise on the efforts already achieved, "*it is necessary to rationalise, homogenise and adopt a cross-cutting approach when implementing DORA*", says Jamal Basrire, Partner, PwC France.

For less mature financial entities, however, the new regulation may be a real challenge. "*Strengthening our IT risk management will require an evolution of our governance and the strengthening of our lines of defense. We will also have to equip ourselves to follow the risks in a holistic way, to be able to monitor them and to establish a reporting system, both strategically and managerially*", explains Caroline Cerval, Chief Operating Officer, Head of Operations and Technology - LCH SA, which defines itself as a player of "measured size".

It is necessary to adopt a cross-cutting approach when implementing DORA within the organisation



Challenge #7 Promote cyber-threats information sharing

"*The number of incident reporting requests is increasing*", says Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA. "*If we really want to achieve the objectives of incident reporting, i.e. a rapid reaction in the case of a systemic event and then a good understanding afterwards to adapt to the threats, reporting must be harmonised*", adds Céline Samain.

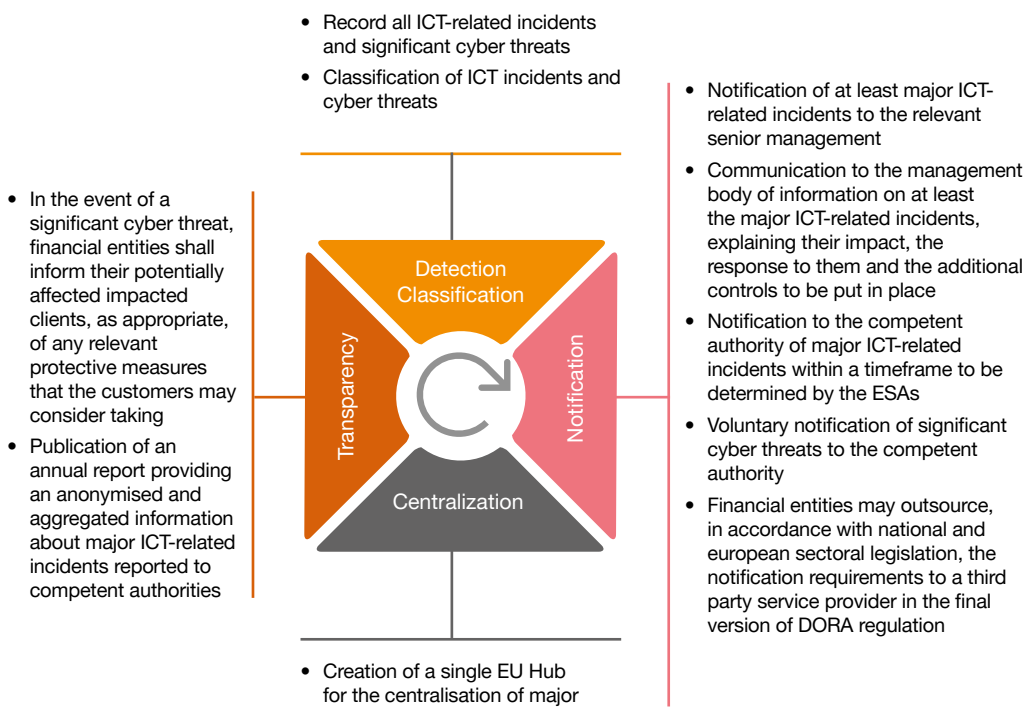
This is one of the objectives of the DORA regulation, which aims to harmonise and simplify the mandatory reporting process of major ICT incidents and to introduce voluntary reporting of significant cyber threats. The level 2 texts will specify the threshold for considering an incident as major as well as the deadlines for reporting incidents to the competent authorities.

The DORA regulation also sets out a certain number of rules to promote information sharing among financial entities.

"*For the benefits of all stakeholders and in order to improve the resilience of all, we will need to share significant threats.*"
"*Of course, this is sensitive data and it will be necessary to create a secure, trusted framework for these exchanges and to inform the authorities of the information exchange agreements concluded between financial entities, third parties, authorities, etc.*", adds Romain Camus.

DORA requires financial entities to maintain operations to a certain standard to allow for the sharing of information between them, in addition to this it requires each of the relevant competent authorities who regulate the entities to be organised to a certain level to facilitate this reporting centrally. This centralisation could result in a single EU Hub for major ICT-related incidents.

ICT-related incident management, classification and reporting



Challenge #8 Take the opportunity to review relationships with ICT service providers

It is clear that, in recent years, financial entities have increasingly outsourced IT services. With sometimes an imbalance in the contractual relationship: "small banks" or small financial entities face very large players, which leave them little room for negotiation. This could all change thanks to DORA: "*The text establishes a legal framework for the supervision of critical ICT service providers that is very clear and very reassuring for financial entities*", says Romain Camus, Partner, PwC France.

The implementation of standard contractual clauses, including termination clauses and exit strategies, should eventually lead to the standardisation of contracts with ICT service providers. "*DORA will help us to have a homogeneous framework for the management of third parties, on which we are very dependent*", explains Caroline Cerval, Chief Operating Officer, Head of Operations and Technology - LCH SA. "*DORA will give greater legitimacy to the requests we make to our service providers*," adds Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA. Indeed: "f*or resilience to be effective, it must be achieved on both sides of the relationship and the entire value chain must be strengthened*" adds Céline Samain

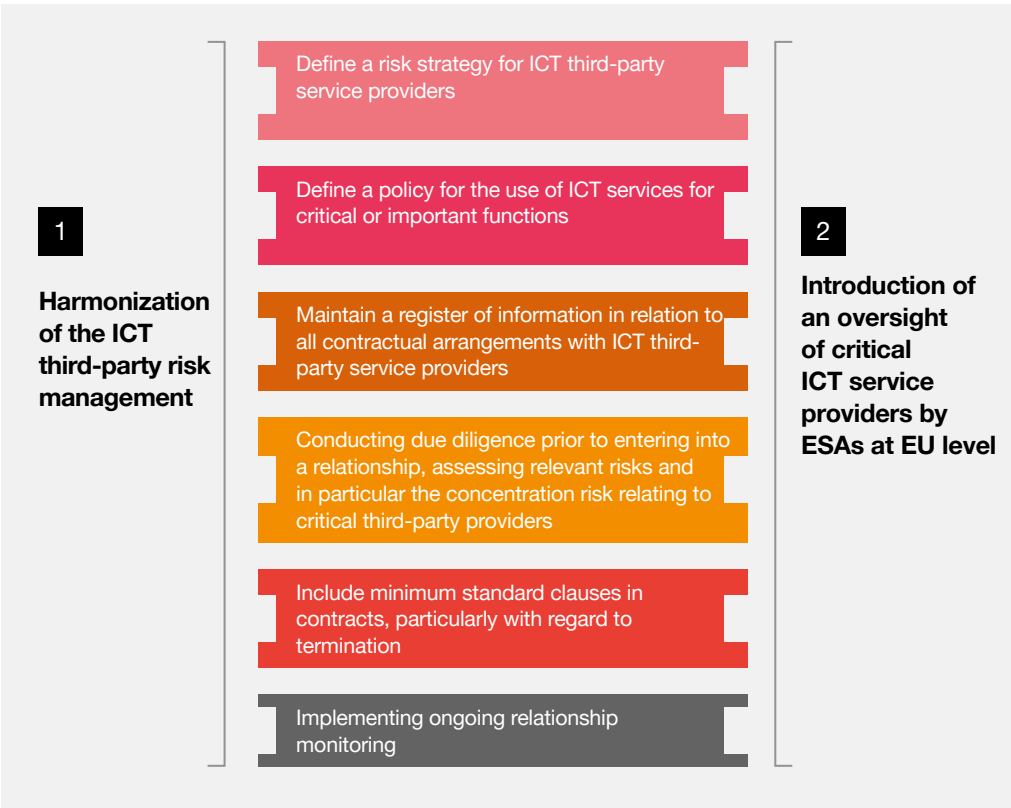
This will strengthen the entire value chain and thus improve the overall resilience of the financial sector. "*The new requirements on third party risk will force providers to provide information to their clients. With also a right of follow-through for the supervisor: if providers do not live up to expectations, clients will have to change them. There will therefore be a competitive advantage to compliance, which should lead to an overall improvement in relations with all of the players in the market*", says Romain Camus.

And, finally, we can hope for a better consideration of the specificities of the financial sector by ICT service providers, more adapted services and potentially more reactivity.

The principle of proportionality is also important in managing third parties: "*We will have to determine the efforts to be made for each service provider, based on various criteria. For instance we have control frameworks for our providers that are organised around a decision tree, which depending on the data, connections, depth of relationship, etc. will potentially evolve, strengthen or even lighten up...*", explains Céline Samain.

An oversight mechanism of critical ICT providers more secure for financial institutions

Managing risks related to ICT third-party service providers

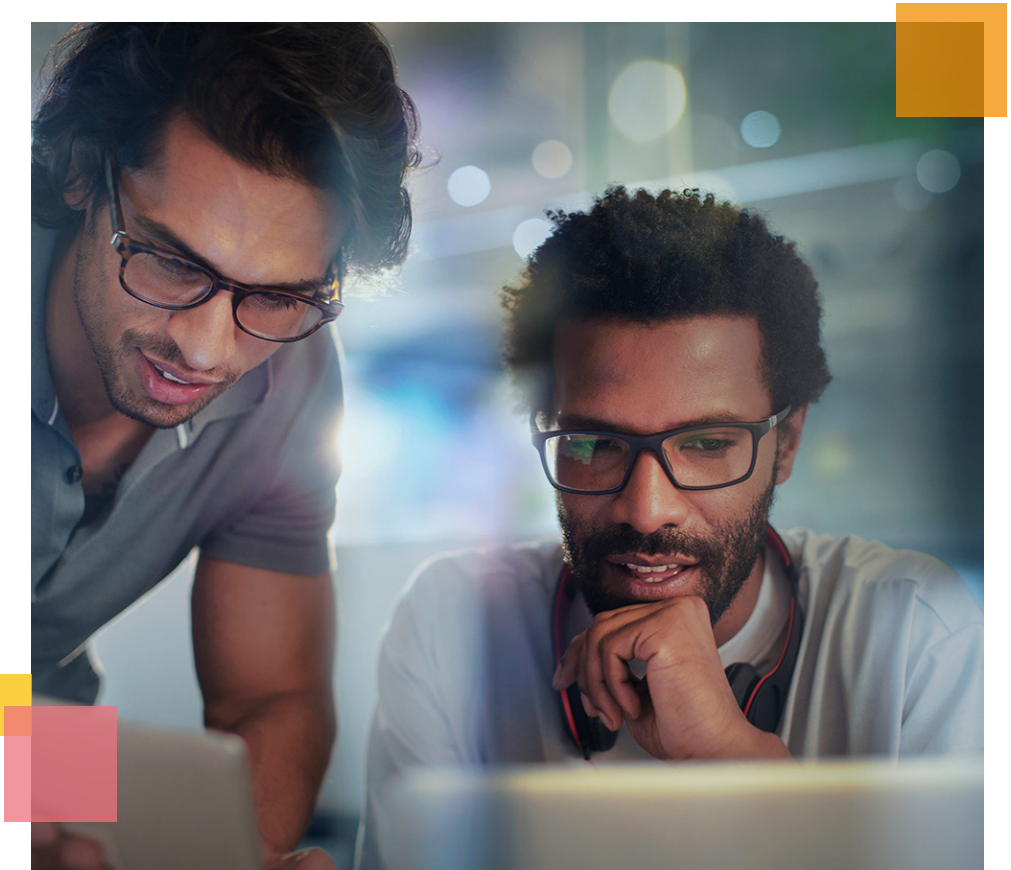


Challenge #9 Test resilience capabilities on a regular basis

Digital operational resilience capabilities must be tested in real conditions in order to identify gaps and potential failures. "*DORA places a strong emphasis on testing programmes and the need to prepare operationally, beyond what is already being done today. We will have to set up solid crisis simulation exercises*", explains Karine Pariente, Partner, PwC France.

Indeed, financial entities, apart from microenterprises, should define, maintain and review a robust and comprehensive digital operational resilience testing programme. As an essential component of the overall digital operational resilience strategy and as part of the ICT risk management framework, it should regularly assess ICT capabilities and security in the event of incidents or cyber attacks.

The DORA regulation requires a proportionate application of the requirements for conducting resilience tests based on the size, activity and risk profile of financial entities. Thus, if all financial entities, including microenterprises must test their ICT tools and systems, only those designated by the competent authorities as significant and cyber-mature, will be required to conduct advanced testing (Threat-Led Penetration Testing or TLPT). The designation of 'significant and cyber-mature' is based on the criteria set forth in the regulation and clarified by future level 2 texts. "*This concerns entities that pose a potential systemic risk at the European Union or national level. They will have to test their critical or important functions every three years, relying on independent internal or external testers*", explains Jamal Basrire, Partner, PwC France. The testing programme should be developed based on a risk-based approach.

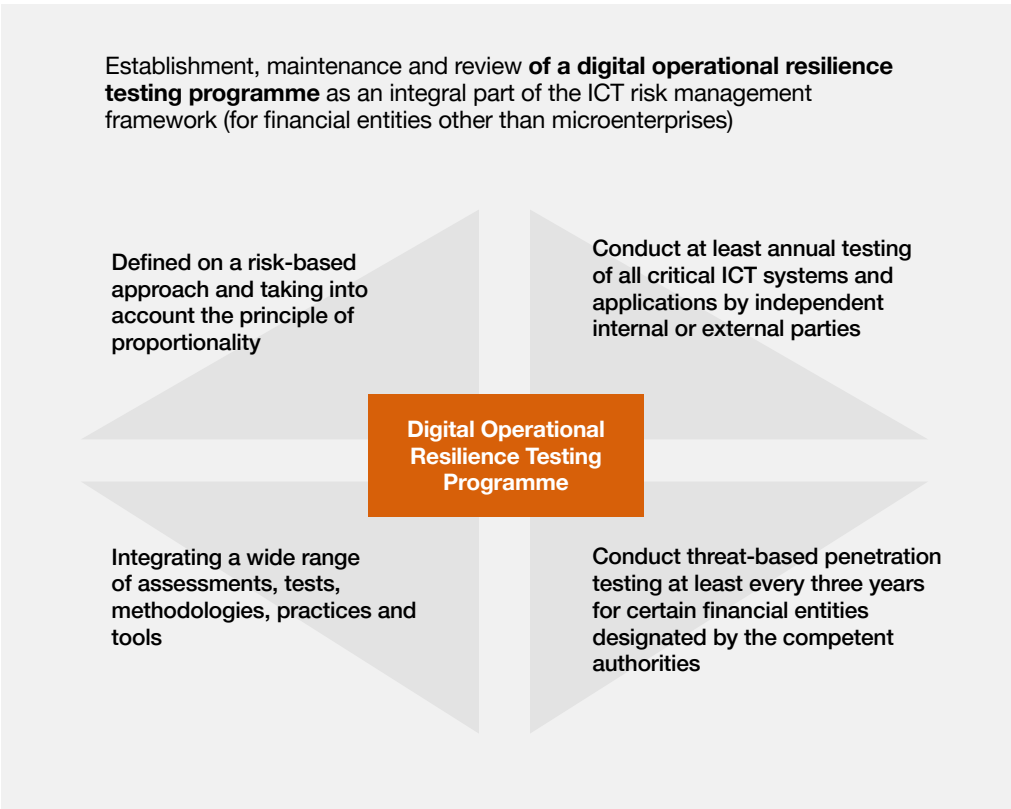


The new framework for conducting advanced tests will bring a significant advantage: these tests will benefit from mutual recognition at EU level. However, the conduct of these tests will require greater efforts in terms of preparation and coordination.

It should be noted that financial entities will need to include ICT service providers involved in critical or important functions to a greater extent and incorporate these enhanced testing obligations into their contractual agreements.

Finally, regular testing as part of a dynamic programme promotes a strong culture focused on operational resilience.

Digital operational resilience testing



Challenge #10 Develop a true culture of digital operational resilience

Beyond the details, the principle of digital operational resilience is truly the guiding principle of DORA: to ensure the robustness of the financial system, institutions need to be able to deal with all types of ICT-related incidents. "*Many companies have improved their cyber risk management. This is a very positive starting point, but it is not enough to address DORA's new paradigm: digital operational resilience. Today, we need to homogenise and work cross-functionally to truly understand the entire subject and develop a culture of operational resilience*", insists Jamal Basrire, Partner, PwC France. The challenge of implementing DORA lies in the transition to this new culture of resilience. Drawing on the lessons learned from their recent crisis management experiences during the COVID-19 pandemic or cyber incidents, some financial entities have evolved their culture in response to their clients expectations.

"*The culture of operational resilience is very important to our clients. We have set up a specific organisation to strengthen it, through an analysis of critical resources, crisis governance and business continuity plans that are regularly tested but have also been proven by numerous events in recent years: social unrest, pandemics, or war...*", illustrates Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA. For other financial entities, the challenge remains important.

A culture of digital operational resilience must be established

Glossary

EBA: European Banking Authority

EIOPA: European Insurance and Occupational Pensions Authority

ESA: European Supervisory Authorities

ESMA: European Securities and Markets Authority

AIF: Alternative Investment Fund

MiCA: Proposed European regulation on crypto-assets known as the “MiCA” (Markets in Crypto-Assets) regulation.

NIS: “NIS” directive for “Network and Information Security” relating to the security of networks and information systems

BCP: Business Continuity Plan

OES: Operators of essential services

ICT: Information and Communication Technologies

TLPT: Threat-Led Penetration Testing

Conclusion

In an uncertain geopolitical context, with an increase in cyberattacks and a clear focus on the digitalisation of the financial sector, the DORA regulation sets a single and common framework on digital operational resilience for financial entities and service providers providing ICT services to financial entities at EU level.

The strategic and operational challenges raised are complex and require the involvement of several internal functions such as the Risk and Compliance Department, the IT Department, the Security Department, the Purchasing Department, and more particularly the strong sponsorship of Management in the establishment of an appropriate governance.

The “key challenges” that we have identified here are guidelines to help prepare for compliance as soon as possible. They constitute benchmarks that will obviously have to be adapted to each environment in order to make DORA not an additional regulatory constraint but an opportunity for financial entities to differentiate themselves on the market by strengthening their operational resilience to IT, cybersecurity, business continuity and risks related to third parties.

Contacts

Rami Feghali

Partner, Head of Risk Services,
EMEA and PwC France

rami.feghali@pwc.com

Philipp Schulz

Director,
DORA Lead at PwC Germany

philipp.schulz@pwc.com

Grant Waterfall

Partner, Cyber Security Leader
EMEA and PwC Germany

grant.w.waterfall@pwc.com

Samantha Trama

Director,
DORA Lead at PwC Italy

samantha.trama@pwc.com

RITM13989654