

The EU Digital Operational Resilience Act (DORA)

How to achieve digital operational resilience in a changing risk landscape

- 5 key trends to consider for financial sector leaders
- In the spotlight: Third Party Risk Management

April 2024

Abstract

Being resilient has never been more important than today. Rapid technological developments, changing political and economic priorities of citizens, as well as geopolitical tensions put pressure on businesses and their leaders – but also create room for change and innovation.

The changing technological landscape creates opportunities for organisations, but also introduces new risks – especially when coupled with the ever-evolving threat landscape. Furthermore, the complex (digital) ecosystem in which most organisations are embedded nowadays, means an increase of dependencies between them, widening their risk landscape. Resilience means being prepared for and being able to sustain these pressures, and ideally to come out stronger.

In recent years the European Union (EU) has been introducing legislation to support organisations in strengthening their individual resilience – and thereby strengthen the resilience of the EU as a whole. This includes the Digital Operational Resilience Act (DORA).

DORA integrates with similar EU legislation (such as the Network and Information Security directive), and has been devised to strengthen the resilience of the EU's financial sector (FS) specifically. It is mandatory for all FS entities and FS ICT service providers, and has major implications for how these entities need to manage their digital operational resilience (beyond traditional, IT-focused continuity measures).

At the same time, DORA and its measures bring an opportunity for leaders to challenge their business to become more competitive – whether it is through better resilience practices, or the increase of customer trust that comes along with these better practices.

In this whitepaper, we put a spotlight on DORA, what it means for FS entities and their resilience strategies, whilst also putting particular focus on Third Party Risk Management as one of the more challenging DORA requirements.

We outline key trends and actions leaders of organisations should consider, and provide a practical approach to improve your organisation's digital operational resilience and get ready for DORA.

Contents

Introduction	04
The changing risk landscape: 5 key trends to consider	06
DORA deep dive	11
In the spotlight: Third Party Risk Management	17
Act now: 5 practical steps to improve your resilience and get ready for DORA	23



Introduction



The EU Digital Operational Resilience Act (DORA)

DORA is a crucial component of the EU Commission's digital financial package, aimed at enhancing the digital resilience of the European financial market.

Its primary objective is to ensure that financial market participants can maintain safe and reliable operations, even in the face of significant disruptions in Information and Communication Technology (ICT).

Companies affected by this regulation have been granted a transition period until January 2025 to achieve full compliance.

DORA will require entities to adopt a broader business view of resilience. It is designed to improve the operational resilience of the financial sector in Europe, reduce the risk of system-wide failures, and protect consumers and the broader economy. The regulation applies to the vast majority of entities operating in the EU financial sector, including banks, insurance companies, investment firms, payment and trading platforms, as well as ICT third party service providers. The regulation establishes binding rules for ICT risk management, ICT incident management, digital operational resilience testing, third party risk management and information sharing.

The implementation of DORA may pose challenges for financial sector firms. In order to comply with DORA's requirements, organisations must assess their strategic priorities, implement measures for resilience and ICT incident handling, manage third party risks, and test their operational resilience. However, while taking steps towards compliance is of importance, increasing overall resilience within the organisation is equally crucial to mitigate risks and avoid potential disruptions. To achieve compliance and strengthen resilience, businesses must take a proactive approach to managing risks.

This whitepaper highlights the changing risk landscape and key trends to consider for every entity that will be affected by the upcoming regulation. We will take a deep dive into the DORA regulation and highlight Third Party Risk Management, one of DORA's key components. Lastly, actionable recommendations for implementation are highlighted to improve resilience and get ready for DORA.

The changing risk landscape: 5 key trends to consider



Five key trends to consider

Achieving digital operational resilience has become ever more challenging in light of today’s continuously changing risk landscape.

While it is natural in this environment for financial sector players to prudently manage risk, at the same time it is important to recognise that we are living in an unprecedented transition period, in terms of geo-political, macroeconomic, technological and demographic factors. Leaders must be brave enough to invest significantly in the things needed to help both your business and your clients adapt.

The European Union’s complex regulatory landscape

1

Enhancing the resilience of critical industries within and across EU Member States has become a key agenda item for the EU. To protect the continuity of an efficient and effective economy and to safeguard public safety, security, and health, **the EU is enacting a range of legislation across cybersecurity, artificial intelligence, data, privacy, and digital platforms.** The overall intention of these upcoming legislative pieces is to create an environment where digital networks and services can prosper and promote digital as a driver for growth, whilst being secure.

The amount of cybersecurity and data protection legislation enacted or under consideration in Europe highlights that this is an issue of great concern and sensitivity for individuals, governments, and businesses. While each piece of legislation has its specific focus and objectives, they all share the common goal of protecting the security, privacy, and data assets of individuals and organisations. They aim to mitigate risks effectively and allow benefitting from emerging opportunities.

Existing and upcoming EU legislation related to resilience



Cyber Security Legislation

- Digital Operations Resilience Act (DORA)
- Network Information Security 2 Directive
- Cyber Resilience Act
- EU Cyber Solidarity Act



Artificial Intelligence

- AI Act
- Liability rules for AI



Data

- Data Governance Act
- Review of the Database Directive



Privacy & Platforms

- Digital Markets Act
- Digital Services Act

The legislation, including DORA, the Network Information Security Directive 2 (NIS2), Cyber Resilience Act (CRA), AI Act, and Digital Services Act (DSA), provides a structured framework for entities to adhere to strict cybersecurity and data protection standards. These regulations and directives mandate businesses to report cybersecurity risks and incidents. They also ensure that entities implement appropriate risk management, privacy, and data protection measures.

To comply, business leaders must stay knowledgeable of the current and evolving cybersecurity and data privacy landscape, recognise related threats and opportunities, and **ensure proper investment is in place in terms of governance, people, processes, and technology**. On the other hand, it is also important for leaders to guide and advise their businesses on the significance of the legislation to mitigate risks effectively and benefit from emerging opportunities.

In summary, the significant regulatory focus on cybersecurity and data protection across Europe is a clear indication that organisations must take these issues seriously, as non-compliance carries intense penalties. Business leaders must provide guidance to their organisations, remain informed on future developments, and take necessary steps to comply with the requirements to ensure the long-term success of their business.

2 Geopolitical & societal shifts

During this period of worldwide economic and political changes, leaders in the banking industry encounter a myriad of challenges. Geopolitical concerns are causing a shift in the risks associated with company growth for financial sector entities. This is particularly due to political uncertainty and emerging technology risks. Geopolitical uncertainty and cybersecurity are increasingly entwined as both state and non-state actors attempt to disrupt democracies and their economies globally. Russia's war in Ukraine, the Israel-Gaza military conflict and the tensions between China and Taiwan are just a selection of key global events which threaten the

functioning of society and pose intense risks both to organisations individually and industries and economies as a whole. **Shifts in national strategies are changing the political and economic landscape (think: BRICS) and affect monetary and market risks arising from the new multi-polar world.**

In the summer of 2023, sophisticated hackers pulled off a cyberattack on the European investment bank, which coincided with Russian-led threats around undermining the Western financial system. The Russian-linked hacktivist group 'Killnet' claimed the attack on Telegram saying¹:



Hello Europe! How are things with the IBAN banking system? I feel like something is wrong with her. Perhaps the transfer system is affected by bad weather. And also the weather forecasters say that not only IBAN will be dead, but also SEPA, WISE, SWIFT."



This 'geo-politicisation' within cybersecurity has led the EU to developing its own cyber strategies, collaborating with other international bodies (e.g. NATO) and investing in cutting-edge technologies. **Intelligence sharing amongst allies is critical to keep pace with the ever-developing techniques of malicious actors.** However, shifts in political priorities and ideological differences can affect the willingness to share sensitive cyber intelligence and collaborate on capacity-building initiatives.

2024 is the year of elections with a combined global population of 49% of the people in the world able to head to the polls, more voters than ever in history. Russia held presidential election this year, where the Putin regime is likely to continue for the foreseeable future, as will the ongoing war with Ukraine. Moreover, the European Union itself is conducting the election for the European Parliament. **Those who take seats in the European Parliament will have direct impact on the digital policies affecting cybersecurity across the region.**

¹ [European Investment Bank attacked, hackers claiming to "impose sanctions on EU" | Cybernews](https://cybernews.com/news/european-investment-bank-cyberattack-russia/)
(<https://cybernews.com/news/european-investment-bank-cyberattack-russia/>)

These emerging geopolitical risks and cybersecurity threats pose significant challenges for business leaders. As state and non-state actors continue to target democracies and their economies, it is imperative to prioritise operational resilience, business continuity planning and cybersecurity measures in strategic planning. **Businesses and their leaders must assess the potential impact of geopolitical risks and cybersecurity threats on their business operations, supply chain, and customers.** The stability of the EU financial sector is heavily dependent on trust in the system. Political and economic uncertainty can undermine this trust, exacerbating the geopolitical risk.

3

Artificial Intelligence

Whilst some may still consider Artificial Intelligence (AI) to be a shiny new technology, it has very much become part of our daily lives both personally and within business. Whether we realise or not, most of us interact with AI every day, for example through the mobile applications we use on our smart phones and social networking sites.

2022 saw the beginning of a massive public integration and adoption of generative AI, particularly given the release of ChatGPT. More recently, 2023 will be remembered for the rapid diversification of AI. Since ChatGPT, the AI landscape witnessed countless breakthroughs and constant innovation.

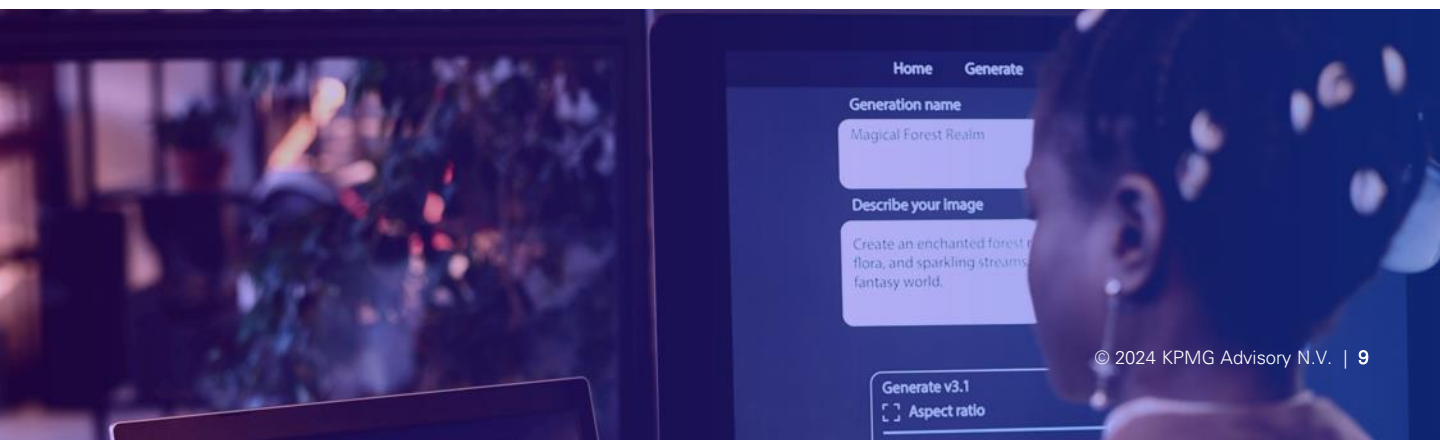
Some of the biggest companies in the world, Microsoft (inc. OpenAI), Google, Amazon, X and Meta, all released Generative AI models during 2023. This burst of AI has brought the topic to the fore across the global media and businesses.

AI brings opportunities for businesses as a whole (e.g. fintech innovation), but also specifically within cybersecurity, which in turn strengthens the digital operational resilience of organisations. Leaders should continually look at what new technologies are becoming available that can help you serve your customers better or connect your business more seamlessly. This not only satisfies customer demand, but also helps cybersecurity departments to effectively identify intricate data patterns and deliver actionable guidance, as well as empower decision-making and incident response efforts.

Despite these positives, challenges, limitations and threats to and of AI exist. Adversaries may capitalise on weaknesses within AI systems, such as manipulating inputs to deceive or elude detection. Moreover, **malicious actors are increasingly using AI and machine learning as advanced attack techniques**, such as by adopting the technology to become more proficient in evading detection. These risks require continuous development and improvements in AI security practices to ensure that potential risks are managed effectively.

Safeguarding AI models from adversarial attacks requires strong defences and ongoing monitoring to counter potential vulnerabilities. As well as the potential of malicious actors tampering with AI systems, issues around data quality and accessibility, as well as transparency and comprehensibility (which upcoming EU legislation requires) lead to new challenges for businesses.

Integrating AI into cybersecurity necessitates expertise spanning both domains. Organisations encounter the hurdle of recruiting and retaining professionals possessing a profound grasp of AI and cybersecurity. These experts must possess interdisciplinary skills to proficiently construct, implement, and sustain AI-driven security systems.



4

Cyber skills gap

Not only with the complex addition of AI-specific skills, but cybersecurity in general – and with it digital operational resilience – has been facing a critical skills gap over the recent years. The skills gap can be considered just as challenging as the overall staff shortages within the field. This causes significant wage inflation as entities compete in a tight labour market to find and retain talent.

These skills are crucial to adapt to the current risk landscape that the financial sector faces. The growth of organised criminal underground networks and motivated nation states has increased the sophistication of attacks. The adoption of cloud and mass remote working triggered by the pandemic means that organisations have a larger attack surface to defend, which exacerbates the cybersecurity skills gap issue even further.

The reality is that organisations must drastically increase the headcount for employees working across cybersecurity, whilst also ensuring they are appropriately trained and qualified. Amid the current threat landscape, which is the most complex and sophisticated it has ever been, **the escalating challenges facing cybersecurity professionals underscore the urgency for organisations to invest in their teams**, both in terms of new talent and existing staff, equipping them with essential security skills – and preventing them from burning out in the face of an unparalleled amount of challenges.

5

Rising third party dependency

As a result of these key trends – such as increased legislative pressure, continued technical innovation, and the growing skills gap – businesses further lean on sourcing third party support. Additionally, **there is a tremendous demand from businesses to offer their customers digitally-enabled financial services solutions.**

This appetite has fuelled the convergence of technology businesses and traditional financial service companies. The companies that offer these services in a connected, secure, and reliable way, will come out as winners in this market.

The other side of the coin is that this adds complexity, as businesses are operating in an ever-growing digital ecosystem of fintech in which more and more connections are made between digital systems. Furthermore, beyond the risk of traditional IT vulnerabilities being introduced by third parties in the digital supply chain, operational dependencies on the risk and continuity measures of third party service providers and their technological solutions exacerbate the need for effective governance of the digital ecosystem.

Additionally, driven by legislation or sustainable ambitions, businesses are more likely to share data with their suppliers to create transparency across supply chains. It is becoming harder for CI(S)Os to oversee the complete digital landscape that the business is operating in. This creates known and unknown dependencies that pose new cyber risks to all parties involved in the ecosystem. Every organisation is responsible for its own security and every organisation is responsible for due diligence on its suppliers. This creates a business equivalent of playing chess on multiple boards instead of one. It is paramount – and inevitable in the light of these interdependencies – to collaborate and work collectively toward the improving the resilience of an entity's digital ecosystem as a whole.

A collective ecosystem approach, with a strategy and underlying policies and procedures in the form of a joint covenant – instead of a multitude of traditional service level agreements between parties – is required. Agreeing collectively on how cyber and operational continuity risks should be managed, sharing knowledge and resources, means the resilience of the ecosystem as a whole increases, and through that the resilience of its members.

DORA deep dive



DORA in perspective: the EU's effort to strengthen digital operational resilience

DORA is one of many upcoming pieces of legislation across the European Union.

As a result of the widespread digitisation in the European financial sector, the European Commission has implemented DORA to establish the foundation for digital resilience in financial institutions. Financial entities will need to enhance their digital resilience by improving processes related to IT risk management, incident handling, and the management of third party relationships.

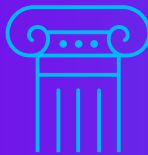
ENISA – The European Union Agency for Cybersecurity’s Mandate

In 2019 the European Parliament adopted the European Union Cybersecurity Act. This strengthened the EU’s cybersecurity agency, ENISA, by granting to the agency a permanent mandate, reinforcing its financial and human resources and overall enhancing its role in supporting EU to achieve a common and high level cybersecurity.

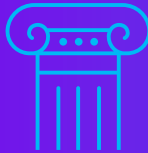
Furthermore, the act established the first EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products and services.

Digital Single Market Package

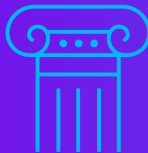
The European Commission has set out to create a Europe fit for the digital age, empowering people with a new generation of technologies. The commission aims for 80% of the EU population to have basic digital skills by 2030, with €43 billion of policy-driven investment until 2030. The digital single market strategy is one of the European Commission’s top 10 political priorities, and is made up of 3 pillars:



Improving access to digital goods and services



An environment where digital networks and services can prosper



Digital as a driver for growth

The EU regulatory outlook

DORA falls into a complex web of laws and regulations as it encompasses various principles and regulatory frameworks applicable to (financial) institutions. Below, selected upcoming legislation is highlighted.

Cybersecurity

European cyber strategy

- Protecting Europe from cyber attacks
- Integrated approach with all stakeholders
- Creation of European cyber security center
- Stimulation of research and development

- International cooperation and common standards and guidelines
- Integration of cybersecurity into all aspects of business
- Enforcement of regulatory frameworks and laws.

Regulation

DORA

Operational resilience within the financial sector

Cyber Resilience Act

Cybersecurity requirements for products with digital elements

Cybersecurity Act

Mandating ENISA and further allocation of resources and powers

Cyber Solidarity Act

Establish European cybersecurity shield

Directive

NIS2

Network and information security requirements

Critical Entities Resilience Directive

Physical security (including IT-related physical security)

Further policies and initiatives

Cyber Diplomacy Toolbox

Harmonisation and unified approach to cyber policy issues

European Cyber Defence Policy

Strengthen collaboration military/civilian cyber communities

Data & Privacy

Regulation

GDPR

Rules for processing personal data

Data Act

Measures for a fair and innovative data economy

Digital Services Act

Legal framework on e-commerce to be updated

ePrivacy Regulation

Protection of personal data in electronic communications

Directive

Digital Markets Act

Regulation of online platforms

Data Governance

Facilitate data sharing across sectors

Further policies and initiatives

Data Spaces

Initiative to facilitate data exchange within EU

Other

AI Act

Rules regarding products with AI

EU Strategic Compass

Plan to strengthen the EU's security and defence policy

CER Directive

Strengthening the resilience of critical infrastructure

European Chips Act

Improve competitiveness and resilience with regard to chips

DORA

As a result of the widespread digitisation in the European financial sector, the European Commission has implemented DORA to establish the foundation for digital resilience in financial institutions. Financial entities will need to enhance their digital resilience by improving processes related to IT risk management, incident handling, and the management of third party relationships. Additionally, they are expected to share information on cyber-related issues and their experiences with other peer entities, contributing to the overall strengthening of the sector. Notably, DORA extends its regulatory oversight to encompass new financial segments, placing them under the supervision of the European Commission.

The goal of DORA

DORA is a component of the broader Digital Finance package introduced by the European Commission. Its objective is that entities can withstand, respond to and recover from all types of ICT-related disruptions and threats. This goal needs to be balanced to facilitate innovation and competition within the digital finance domain while managing the associated information and communication technology (ICT) risks. The exponential use of ICT within the financial sector is undeniable, reaching a point where ICT risks

cannot be treated merely as a subset of business processes. This integration extends across various financial services, spanning payments, clearing and settlement, and algorithmic trading. Moreover, ICT risks consistently pose a significant challenge to the operational resilience and stability of the European financial system.

DORA and BCM

The implementation of DORA highlights the importance of resilience and business continuity management (BCM) in the financial sector. As stated in DORA: "Financial entities need to have an effective Business Continuity Management in place that ensures they are able to maintain and quickly restore their critical business processes even in the event of disruptions to ensure the continuity of their business operations. This includes identifying backup systems and services, as well as conducting regular emergency drills". Financial institutions must recognise the critical role that digital systems play in their business operations and prioritise the establishment of robust BCM processes. In this context, by focusing on improving your resilience and BCM practices, your organisation is moving towards becoming DORA compliant.

Why DORA?

- Create a harmonised digital finance strategy.
- Broaden the scope of financial markets by including new markets such as crypto and Distributed Ledger Technology.
- Fostering technological development by encouraging innovation and supporting competition.
- Ensuring financial stability and consumer protection by increasing infrastructure resilience.



Entities in the DORA scope: expanding the regulatory perimeter

Building upon existing regulation within the financial market, DORA expands that scope to include new markets to capture a wider range of financial entities. Additionally, DORA will enhance its focus on third party risk management by including third parties in its scope.

Europeans are becoming heavily dependent on the digital assets and systems of the financial entities. As more financial services are provided through digital channels, there is a greater risk of cyber attacks and operational failures that could disrupt critical services and damage financial institutions and their customers. The consequences of failing to deliver these essential services can be consequential, and due to the integrated nature of the European Union can be felt all across Europe.

Besides the increased integration, the financial market is in quick development and new forms of financial entities are emerging. DORA aims to encompass not only encompass traditional financial entities such as banks and credit institutions, but also emerging entities such as crowdfunding service providers and crypto-asset services. These entities operate in a largely unregulated space and pose potential threats to the financial system due to their decentralised nature, lack of transparency, and high volatility.

Both these developments are reason enough for the European Commission to expand the regulatory perimeter to secure the market. By expanding the regulatory perimeter, the regulation covers a wider range of financial institutions and enables more effective coordination, communication, and cooperation among all relevant stakeholders in managing digital risks and ensuring the stability of the financial sector. By bringing all of these institutions under one regulatory umbrella, DORA seeks to protect investors, institutions, and European citizens and ensure the stability of the financial system by creating a more comprehensive regulatory framework that covers all types of financial entities, regardless of their digital or traditional nature.

Entities in scope

Annex I

- Credit institutions
- Management companies
- Payment institutions
- Data reporting service providers
- Electronic money institutions
- Insurance and reinsurance undertakings
- Investment firms
- Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
- Crypto-asset service providers, issuers of crypto-assets, issuers of asset referenced tokens and issuers of significant asset-referenced tokens
- Institutions for occupational retirement pensions
- Central securities depositories,
- Credit rating agencies
- Central counterparties
- Trading venues Administrators of critical benchmarks
- Trade repositories
- Crowdfunding service providers
- Management companies of alternative investment funds
- Securitisation repositories
- ICT third party service providers

**Organisational impact in 5 pillars:
what do they mean?**

In light of the 5 pillars of DORA, leaders of the entities in scope of DORA should ask in how far their businesses are meeting the relevant requirements.

ICT risk management requirements

Financial entities need agile processes and systems to minimise the impact of ICT risks. Continuous identification and mitigation from various sources, along with internal controls and recovery plans, are vital to safeguard the integrity, safety, and resilience of ICT systems and supporting physical infrastructure. This means strengthening your ICT and cyber risk management (e.g. framework, strategy, target operating model, policies, metrics) and maturing your Identification; Protection; Detection; Response & Recovery; Learning & Evolving processes.

1 Do we have effective governance and risk management processes in place to identify, monitor and manage key ICT risks?

ICT-related incident reporting

DORA mandates establishing effective processes for consistent monitoring, handling, and follow-up of ICT incidents, including identifying and eliminating root causes to prevent their recurrence – and timely reporting to oversight bodies. This means that your cyber incident management will have to use specific EU criteria (e.g. geographic spread of incidents, reporting of ‘significant cyber threats’ to regulators). It also means expanding transparency and awareness of oversight for cyber risks and ICT incidents, and tightening up reporting structures (internal and external).

2 Is our ICT incident management effective in identifying and managing incidents across all priorities, and can we report efficiently and effectively to regulators about how things are going?

Digital operational resilience testing

Financial entities need a comprehensive digital operational resilience testing (DORT) program to assess resilience against incidents and attacks. The goal of this DORT program is to assess and improve preventive, detective and responsive measures. Additionally, every three years an external red team performs a mandatory "Threat-Led Pen Test" (TLPT) that assesses the entity’s resilience during an advanced attack simulation.

3 What is our testing strategy, and how effective are our (in-house or external) testing-service providers in their approach?

ICT third party risk

Financial entities must manage ICT third party providers throughout the entire lifecycle, adhering to the minimum requirements outlined in DORA, due to the growing reliance on ICT third party services. This requirement of DORA is perhaps one of the biggest challenges for most entities, which is why we dedicate a whole chapter in this whitepaper to the subject.

4 Do we have a clear view on who are critical ICT service providers are, and do we have agreements in place that reflect industry good practices with regard to cybersecurity and business continuity?

Information sharing agreements

To foster awareness and growth, the regulation encourages financial entities to share cyber threat information and intelligence. This means that your organisation should exchange cyber threat information and intelligence. Information sharing itself is not mandatory, but it is mandatory to send notifications and inform regulators about how your organisation participates in information sharing.

5 Are we participating in information sharing schemes (e.g. ISACs), and are effectively processing threat information which is shared with us?

In the spotlight: Third Party Risk Management



Introduction to DORA's ICT Third Party Domain

In the fast-paced world of finance, the integration of Information and Communication Technology (ICT) services has become indispensable. However, with this integration comes a host of challenges, particularly concerning third party ICT service providers.

In this section, we delve into the key aspects of DORA's ICT third party domain and its implications for financial entities.

DORA emerges as a response to the lack of harmonisation and regulatory clarity surrounding ICT third party risk monitoring across Member States. By addressing gaps and standardising terminology, DORA aims to enhance regulatory consistency and promote fair competition among financial entities operating within the European Union.

Widespread ICT service usage in finance leads to complex contracts with third parties, often lacking adequate subcontracting monitoring, hindering risk assessment. DORA aims to remedy this with targeted rules for ICT third party risk monitoring. Despite existing outsourcing rules, DORA highlights the absence of specific standards for ICT contracts, leaving critical risks unaddressed. It underscores the necessity of core contractual rights for effective risk management, especially for critical functions.

In spite of the existence of guidelines such as the *EBA Guidelines on outsourcing (2019)* and the *ESMA Guidelines on outsourcing to cloud service providers (2021)*, there remains a noticeable lack of uniformity in monitoring ICT third party risk. Union law falls short in fully addressing the systemic risks arising from the financial sector's reliance on a few critical ICT providers.

DORA aims to fill this gap by introducing an Oversight Framework for continuous monitoring of critical ICT third party service providers. The financial entity is responsible for ensuring detailed management of ICT risks related to third parties based on defined minimum criteria, thereby retaining liability and responsibility for compliance with this law.

Managing ICT Third Party Risks in Financial Entities

Financial entities must prioritise their third party ICT risk management, adopting a proportionate approach to monitoring ICT third party provider risks. This approach involves considering various factors such as the nature, scale, complexity, and importance of ICT dependencies. Assessing potential impacts on service continuity and quality at both individual and group levels is essential for effective ICT risk management (and DORA compliance).

Organisations should adopt a strategic approach to ICT third party risk management, approved by their management body. This approach involves continuous screening of all ICT dependencies and maintaining a register of contractual arrangements with ICT service providers. Supervisors may request access to this register to gain insights into entities' ICT dependencies and provide support for the Oversight Framework.

Before finalising contracts, financial entities must conduct thorough analyses of critical aspects. These aspects include service importance, supervisory approvals, concentration risk, and due diligence on ICT third party service providers. Adherence to high information security standards for critical functions is paramount. Financial entities must also recognise potential contract termination triggers and address them proactively.

The regulation adopts a flexible and gradual approach to managing the systemic impact of ICT third party concentration risk. It avoids rigid caps to preserve business conduct and contractual freedom while requiring financial entities to assess risks, particularly with subcontractors from third countries.

To ensure the secure offering of services by ICT third party service providers, key contractual elements must be harmonised. This harmonisation enables thorough risk monitoring, focusing on areas critical to maintaining the stability, functionality, availability, and security of the ICT services provided by third parties.

When renegotiating contracts to comply with the regulation, financial entities and ICT third party service providers must include key contractual provisions mandated by the regulation. These provisions ensure transparency, accountability, and effective risk management throughout the duration of the contract.

ICT service contracts should outline functions, locations, service levels, accessibility, security, and data protection. They must include termination terms, assistance in incidents, and cooperation with authorities. For critical functions, detailed service levels, notice periods, and testing cooperation are crucial. Financially vital ICT services contracts should allow access, inspection, and auditing rights for continuous monitoring and confidentiality, with provider cooperation and regulatory oversight.



Contractual arrangements for ICT services must include dedicated exit strategies with mandatory transition periods to minimise disruption risks. For entities under Directive 2014/59/EU, contracts must be robust and enforceable in resolution scenarios, containing clauses against termination, suspension, or modification due to restructuring or resolution, provided payment obligations are met.

Competent authorities play a vital role in verifying financial entities' compliance with the Lead Overseer's recommendations. As part of their prudential supervision duties, they may require entities to take extra measures based on these recommendations.

Achieving compliance through best-practice third party risk management

Incorporating third party ICT Risks into Overall Framework

Integration of management of third party ICT risks into overarching ICT risk framework is now a best practice since it ensures that entities remain responsible for regulatory compliance and proportionately address risks based on their significance and potential impact on financial services.

Development of Strategy and Policies

Financial entities are mandated to develop and periodically update a strategy for managing third party ICT risks. This strategy should include policies for using ICT services for critical functions, tailored to the entity's risk profile and business complexity. These policies should be applicable across all organisational levels, ensuring consistency and alignment with overarching risk management objectives.

Maintenance of Detailed Register and Reporting Requirements

It is required to maintain a detailed register of all ICT service contracts. Additionally, entities must report annually on new arrangements to regulatory bodies and inform these authorities about contracts for critical functions or when a function becomes

critical. This ensures transparency and accountability in the management of third party ICT risks, facilitating regulatory oversight and intervention when necessary.

Pre-Contract Evaluation and Due Diligence

Before engaging in ICT service contracts, financial entities must conduct comprehensive evaluations. This evaluation includes assessing the contract's relevance to critical functions, compliance with supervisory conditions, potential risks such as concentration risk, and the presence of any conflicts of interest.

Adherence to Information Security Standards

Financial entities are only permitted to contract with ICT third party service providers that meet specific information security standards.

This requirement is particularly stringent for services related to critical or important functions, where the highest and most current standards must be considered before finalising arrangements.



Planning Audits and Inspections

It is no longer sufficient to only contract the option for audits if and when necessary. Now planning audits and inspections of ICT third party providers based on risk assessments is a must. Entities must adhere to established audit standards and ensure that auditors possess the necessary skills, especially for arrangements involving high technical complexity. Regular audits and inspections help verify compliance with contractual obligations and identify potential areas of improvement or risk.

Provisions for Contract Termination and Exit Strategies

Financial entities must have provisions to terminate ICT service contracts under various circumstances, including;

- Significant breaches,
- Changes affecting service performance,
- Or weaknesses in the provider's ICT risk management.

Additionally, entities must develop exit strategies for critical ICT services to mitigate risks from provider failure and ensure smooth termination. These exit strategies should include identifying alternatives and regular testing transition plans to maintain business continuity without compromising regulatory compliance or service quality.

Assessment of ICT Service Contracts Risks

Financial entities must assess risks in ICT service contracts, considering the substitutability of providers and the concentration of contracts with one or closely connected providers, while evaluating alternatives based on their digital resilience strategy.

Evaluation for the benefits and risks of subcontracting ICT services for critical functions need to be embedded, including legal and regulatory implications, data recovery, and monitoring challenges, especially with third-country providers.

Contracting facts

The contract between a financial entity and an ICT third party service provider must clearly define and document in writing all rights and obligations, including service level agreements, in a format that is accessible and durable for both parties. Comprehensive provisions are essential for thorough coverage across all aspects as follows:

1. Service descriptions (Art.30-2a)
2. Location of services and data processing (Art.30-2b)
3. Data protection measures (Art.30-2c)
4. Recovery and access provisions (Art.30-2d)
5. Service level details (Art.30-2e)
6. Support obligations (Art.30-2f)
7. Cooperation with authorities (Art.30-2g)
8. Termination rights and notice period (Art.30-2h)
9. Conditions for security/resilience training (Art.30-2i)

Contracts for the use of ICT services in critical or important functions must include additional provisions to address the heightened importance of these functions. This includes:

1. Detailed service level descriptions and corrective actions to be taken (Art.30-3a)
2. Notification and reporting requirements (Art.30-3b)
3. Business contingency provisions and ICT security measures, tools and policies (Art.30-3c)
4. Cooperation in testing and oversight (Art.30-3d)
5. Rights for ongoing monitoring and audits (Art.30-3e)
6. Exit strategies with an adequate transition (Art.30-3f)

Furthermore, provisions should be included for microenterprises to delegate audit rights to an independent third party to ensure effective oversight.

Follow-Up with Competent Authorities and Lead Overseers

If a competent authority detects inadequate management of ICT third party risk within a financial entity, it is obligated to notify the entity accordingly.

The notification stipulates that unless the entity amends its contracts within 60 days to effectively address these identified risks, a decision may be taken.

Competent authorities are mandated to grant financial entities sufficient time to adjust and modify agreements with critical ICT third party providers. This allowance is crucial for ensuring digital operational resilience and facilitating the seamless implementation of exit strategies and transition plans.

Act now: 5 practical steps to improve your resilience and get ready for DORA



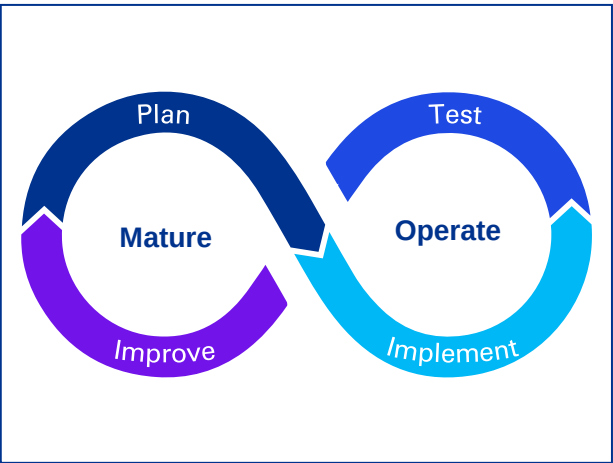
Getting DORA-ready

What does DORA readiness mean for you? Financial sector entities have been focused on ICT risk management and compliance and their respect to resilience for a number of years.

With the upcoming DORA regulation, entities must move from preparation to implementation and take steps towards demonstrating how their practices comply with DORA.

Financial entities will need to demonstrate appropriate security and resilience of critical ICT systems and applications to comply with DORA. The level of compliance efforts will vary depending on the size and complexity of your entity. A risk-based approach and appropriate security and resilience testing are necessary to address potential vulnerabilities and to prove compliance in meeting evidence requirements of the European Supervisory Authorities. By focusing on long-term resilience, entities can establish a resilient foundation, which will aid them in their steps towards DORA compliance.

Resilience means learning from the past, to improve the present, and to prepare for the future.



Our 5 key actions towards DORA readiness

In order to make entities ready for DORA, we have identified 5 key actions to assist those that are in the preparation phase. These actions will enable entities to effectively manage their digital operational resilience be ready for DORA:

1. Determine strategic priorities and set up a DORA implementation program
2. Implement resilience and incident management measures to effectively manage continuity risks
3. Manage third party risks
4. Test digital operational resilience
5. Implement (additional) measures for resilience & ICT incident handling

Action

Determine strategic priorities and set up a DORA implementation program



The approach

Key stakeholders

CIO, CISO, COO, Head of (IT) Risk, CRO, Legal & Compliance Officer, BCM/Resilience coordinator

What does my business need?

- ✓ An integrated digital operational resilience strategy that is carried throughout the organisation.
- ✓ A long-term resilience program.

Objective

To enhance your daily business practices, aim to achieve a transformation towards a resilient end-to-end IT & operations environment. In order to ensure strong risk management, be focused on achieving a broad agile transformation that takes into account risks associated with your ICT/technology suppliers and continuity measures. Additionally, it is necessary to aim to increase your agility in serving digital channels by implementing strong BCM measures.

Key success factors

- Managerial support and vision for the long term.
- Good communication for awareness of affected stakeholders.



How do I ensure that in the long-term my digital operations are resilient and in line

with good practices and requirements?

What is my (end-state) vision for our digital environment taking to heart the objectives of DORA?

Relevant DORA pillars:

ICT Risk Management



Action

Implement resilience and incident management measures to effectively manage continuity risks



What are my key risks that threaten my digital operational resilience – and what

can I do to manage them effectively?

Relevant DORA pillars:

ICT Risk Management

Information Sharing

The approach

Key stakeholders

BCM/Resilience coordinator, CISO, COO, IT & Security Management, First-line management functions

What does my business need?

- ✓ Mapping of current gaps with good practices and DORA requirements
- ✓ Defines measures and implementation roadmap, including effective follow-up measures on chosen activities

Objective

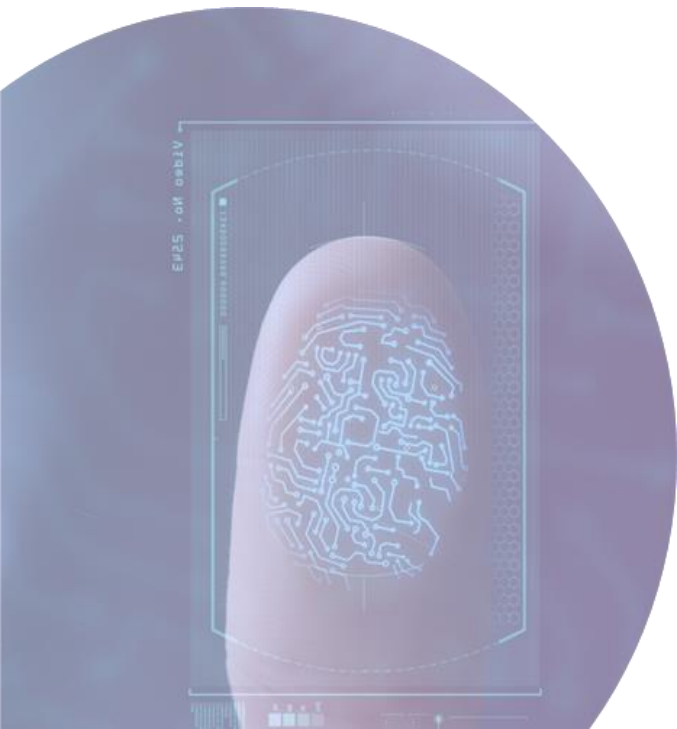
To ensure effective implementation of your program, it is crucial to ensure leadership support, as well as translation of strategic and regulatory requirements into operational measures.

It is essential to enable control owners and line management to manage compliance requirements in a risk-based way, including the automation of controls related to digital resilience, in order to manage the complexity of (compliance) requirements effectively.

Think big and start small – for example by organising a workshop with relevant middle-management players to align and agree on the implementation strategy of your DORA program.

Key success factors

- Focus on actualising long-term resilience, not just on compliance.
- Leadership support and involvement.



Action

Manage third party risks



The approach

Key stakeholders

CIO, CISO, COO, Legal & Procurement officer

What does my business need?

- ✓ A strong and transparent TPRM management structure, with extensive policies, procedures and monitoring force.

Objective

To ensure effective management of ICT risk related to third party providers, it is essential to conduct complete monitoring of all ICT-related third party risks throughout all relationship phases.

This involves the classification and analysis of providers and their management bodies, record-keeping of relevant information, managing proportionality, managing compliance, and creating a TPRM risk strategy. By undertaking these steps, comprehensive management of ICT risk in relation to third party providers can be ensured.

Key success factors

- Active TPRM throughout the whole third party lifecycle (strategy – governance – pre-contract – contracting – contract management & business as usual).
- Avoiding ICT concentration risk at entity level.



How well is my understanding of my ICT supply chain?

To what extent does my business have a central contract management administration for supporting the third party life cycle?

Has my business prepared exit strategies for their current ICT third parties to ensure smooth continuation of their business and ICT processes in case service delivery is discontinued by an ICT third party?

Relevant DORA pillars:

Third Party Risk Management



Action

Test digital operational resilience

Test

4

The approach

Key stakeholders

CISO, IT Management, CRO

What does my business need?

- ✓ All critical ICT systems & applications are tested at least once per year by an independent party.
- ✓ The testing program is risk-based.

Objective

To ensure operational resilience, it is crucial to test critical and important functions more frequently than non-critical or unimportant functions, at least once a year.

The program for testing digital operational resilience must be based on relevant threat scenarios. A best practice is to implement an appropriate test set-up for each threat, in order to test the resilience effectively. Moreover, every three years, entities are required to perform Threat-Led Penetration Testing (TLPT) that simulates a realistic and advanced cyber attack. This simulation helps organisations prepare and train for real cyber attacks.

Key success factors

- Active follow-up on testing results..



Does my business perform digital resilience testing on a regular basis, to stay resilient in light of cyber threats?

Does my business have processes in place to prioritise penetration testing through risk- and threat assessments?

Relevant DORA pillars:

Digital Operational Resilience Testing



Action

Implement
(additional) measures
for resilience & ICT
incident handling

5

Improve



How strong is my
business's ICT
incident handling?

If my business
experiences a major IT incident,
are you able to continue operations
in the meantime and recover
swiftly?

How does my business report
major security incidents to the
national authorities?

Does my business exchange
cyber-threat information with other
(peer-)entities?

How do I do effective cyber threat
management?

Relevant DORA pillars:

ICT Incident Management

Digital Operational Resilience
Testing

The approach

Key stakeholders

CIO, CISO, COO, SOC & IT Managers

What does my business need?

- ✓ A strong incident reporting structure.
- ✓ Cross-organisational awareness for resilience.

Objective

To establish strong operational resilience measures and incident management, it is essential to accomplish resilience testing from a wider perspective, which – beyond technical security testing – includes regular crisis simulations.

It is important to improve business continuity plans and ICT crisis scenarios to ensure that uncontrolled disruptions are avoided due to slow and ineffective incident management.

Moreover, accomplishing mature threat intelligence and assessing top continuity risk scenarios is crucial to enhance resilience and preparedness in critical situations.

By undertaking these measures, strong operational resilience can be established, ensuring smooth and uninterrupted operations.

Key success factors

- Have clear communication lines and reporting processes.
- A security-aware culture that encourages early reporting of incidents.



Your cyber capabilities vs DORA

DORA builds upon many of your entity’s existing capabilities. If you focus your efforts on strengthening your cyber resilience, your organisation will be well positioned to meet the requirements set by DORA. To achieve the objectives listed above, it is relevant to adhere to the following actions regarding the specific DORA pillars.

DORA pillar	DORA actions	Organisational capabilities
ICT Risk Management	• Scope all ICT assets (incl. supporting applications and tooling). • Evaluate your ICT risk framework. • Review your response and recovery processes. • Strengthen your awareness and cyber risk hygiene plans.	• Cyber governance • Security risk management framework • Important business services • Network and Infrastructure security • Third party security • Information security policies and standards • User access management • Change management • Incident Response/SIEM • BCP/DR/Crisis Management • Security Awareness • Vulnerability Management • DevSecOps • Crisis Communications
ICT Incident Management	• Update your incident classifications according to DORA requirements. • Update your incident reporting processes to the AFM for major incidents. • Review your crisis communication strategies.	• Incident Management • Incident Response • Crisis management
Digital Operational Resilience Testing	• Perform a ‘Stress-Test’. • Perform the required level of threat-led penetration testing. • Align testing procedures with DORA testing requirements.	• Vulnerability management • DevSecOps • Penetration Testing • Source code reviews • Network security • Secure configuration • SAST/DAST • Cyber scenario testing
Third Party Risk Management	• Map third parties. • Evaluate vendor exit strategies. • Review contract contents. • Map the concentration of risk including third party dependencies.	• Third party risk management • Critical ICT third party service providers • Multi-vendor strategy
Information Sharing	• Create a trusted community/ecosystem of financial entities to share cyber threat information and intelligence.	• Incident Response • Threat Intelligence • Cyber Governance • Guaranteed data security

What we do

	Digital strategy and operational risk management	- Digital strategy development and implementation incl. DORA requirements - Target operating model development for a business-driven and cost-effective digital environment - Operational resilience maturity assessments and improvement planning - third party/outsourcing risk assessments and mitigation	Expert Secondment	Solution Partnerships (ServiceNow, Microsoft, Vectral, Clarity,...)	Advisory, Audit & Assurance Services
	DORA program implementation	- Development and implementation of business continuity programs - Incident management process design and implementation - Design and implementation of DORA-based control frameworks - Digital sourcing support for technology service providers			
	Cyber resilience testing and improvement	- Threat Intelligence Based Ethical Red Teaming (TIBER) assessments - Threat led (advanced) penetration testing - Red Teaming and (operational) resilience testing - Phishing and awareness testing - Purple Teaming / SOC readiness assessment - Attack Surface Management Assessment			
	Quality assurance and compliance	- Assurance on DORA controls reporting under ISAE3000A standard - Internal Audit support in conducting DORA audits - Compliance Assessments (overall or specific DORA chapters) - Quality assurance on DORA Implementation Projects			

Aligned with client business priorities and needs

Your contacts



Bert Koelewijn
Partner
koelewijn.bert@kpmg.nl
+31 (0) 206 567635



Augustinus Mohn
Senior Manager
mohn.augustinus@kpmg.nl
+31 (0) 206 562981



Ali Alam
Senior Manager
alam.ali@kpmg.nl
+31 (0) 206 568773

Credits

This document has been created through the collaborative efforts of the following individuals: Hamish Wishart, Mert Şölen, Marijn Pronk, Carlien Groenewegen, Simon Plasmeijer, Jordi van den Breekel, and Justin Black.



home.kpmg/socialmedia

For more information on KPMG and DORA visit:

t.ly/9Rizd

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. The KPMG name and logo are trademarks used under licence by the independent member firms of the KPMG global organisation. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.