DORA Regulation - Frequently Asked Questions

Osborne Clarke

July 2025

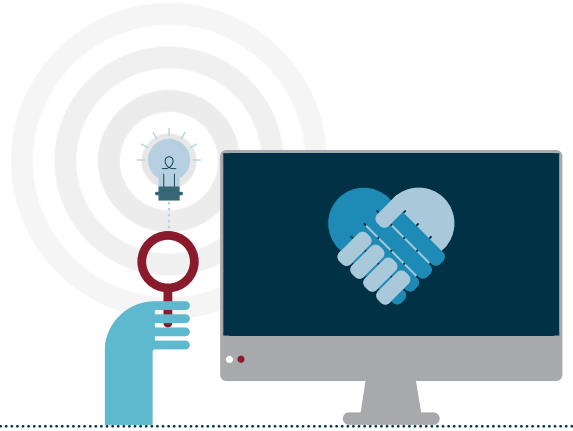
Start

Introduction

Welcome to Osborne Clarke's frequently asked questions (FAQ) on the Digital Operational Resilience Act (DORA). As an international law firm committed to providing comprehensive legal guidance, we understand the importance of staying informed about regulatory changes that have an impact on the financial sector.

DORA aims to strengthen the IT security and operational resilience of financial entities within the EU, ensuring they can withstand and recover from all types of disruptions.

In this FAQ, we address common questions regarding DORA, its implications, and how it affects your organisation. Whether you are seeking clarity on compliance requirements, timelines or specific provisions, our goal is to provide you with the information you need to navigate this regulation effectively.



Contents

01 Scope | Who is subject to DORA?

02 Scope | What are the exemptions from DORA?

03 Requirements | What are the main requirements of DORA?

04 Third-party risk | How should financial entities treat ICT services that they receive from other financial entities in scope of DORA?

05 Third-party risk | How does DORA apply to outsourcing agreements?

06 Third-party risk | What practical problems arise when negotiating contracts with potential ICT third-party service providers?

07 Third-party risk | What risks must financial entities assess before contracting with ICT third party service providers?

08 Third-party risk | Is due diligence required before contracting with ICT third party service providers?

09 Overlaps | Do entities subject to NIS 2 Directive also need to comply with DORA?

10 Overlaps | What is the interplay between DORA and AI Act?

11 Overlaps | Does DORA impact the way personal data is protected under GDPR?

12 Overlaps | Do companies with ISO 27001 certification also need to implement DORA?

13 Contacts

1. Scope | Who is subject to DORA?

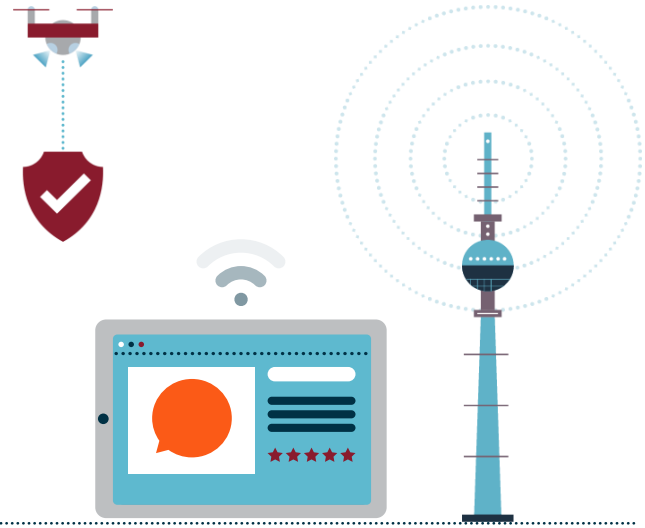
DORA applies to a wide range of financial entities such banks, insurance companies and investment firms.

DORA's article 2 lists the specific entities falling under its scope: credit institutions, payment institutions, account information service providers, electronic money institutions, investment firms, crypto-asset service providers, central securities depositories, central counterparties, trading venues, trade repositories, managers of alternative investment funds, management companies, data-reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, institutions for occupational retirement provision, credit rating agencies, administrators of critical benchmarks, crowdfunding service providers, securitisation repositories and information communication technology (ICT) third-party service providers (when supporting the digital operations of financial entities, such as software development, IT infrastructure and technical support).

2. Scope | What are the exemptions from DORA?

DORA regulation does not apply to certain entities indicated in its article 2: managers of alternative investment funds, insurance and reinsurance undertakings, institutions for occupational retirement provision that operates pension schemes which together do not have more than 15 members in total, natural or legal persons under the directive on markets in financial instruments, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries that are microenterprises or small or medium-sized enterprises, and post office "giro" institutions.

Some financial entities are subject to lighter requirements or exemptions for reasons associated with their size or the services they provide, such as small and non-interconnected investment firms, or some small institutions for occupational retirement provision. These entities will need to comply with a simplified ICT risk management framework.



3. Requirements | What are the main requirements of DORA?

DORA aims to strengthen the overall digital operational resilience and IT security of financial entities by ensuring that they are well prepared to face ICT-related challenges and threats.

To this end, DORA sets out a range of main requirements for ICT risk management.

- **ICT risk management framework**. Entities concerned must establish and maintain a comprehensive ICT risk management framework, which should be reviewed regularly. This will involve implementing measures that may already be in place (or that will need to be put in place if this is not the case), such as policies, risk mapping and identification of systems considered critical, implementation of an IT security policy, or disaster recovery plan.
- **ICT incident reporting**. Entities concerned are required to implement mechanisms for detecting and reporting ICT-related incidents. They must report significant ICT incidents to their national competent authorities within strict time limits.
- **Testing**. Entities should implement digital operational resilience testing programmes. This includes conducting vulnerability assessments, penetration testing and scenario-based testing to ensure preparedness for ICT disruptions. All essential IT systems and applications should be at tested at least once a year.
- **ICT third-party risk management**. DORA sets out several requirements for financial entities when contracting with ICT third-party service providers. This includes conducting due diligence, establishing contractual arrangements, and monitoring the performance and security of ICT third-party providers.
- **Information sharing**: DORA intends to facilitate information sharing regarding incidents and entities are encouraged to participate in information sharing arrangements to exchange knowledge and best practices related to ICT risk management and cyber threats (such as tactics, techniques, procedures, etc).

4. Third-party risk | How should financial entities treat ICT services that they receive from other financial entities in scope of DORA?

DORA's broad scope and wide definitions

The general issue is the broad scope and wide definitions of DORA:

ICT services are "digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis (including hardware as a service and hardware services such as the provision of technical support via software or firmware updates by the hardware provider, and excluding traditional analogue telephone services)."

DORA's recitals, for example Recital 35, emphasise the intention to address all risks arising from all types of ICT services. The definition of ICT services in the context of DORA shall be interpreted broadly to include digital services and data services provided on an ongoing basis to one or more internal or external users via ICT systems.

The risk management rules for financial entities subject to DORA who receive ICT services from third-parties are not limited to a certain group of technology service providers (for example, cloud computing providers or data centre operators) and may also encompass banks, insurance companies and other financial entities if they provide ICT services to other financial entities. The non-tech nature of a service provider does not release financial entities from DORA's ICT risk management requirements.

4. Third-party risk | How should financial entities treat ICT services that they receive from other financial entities in scope of DORA?

Categorisation issues

Many financial institutions are still having trouble categorising various of the services that either have been or are delivered using ICT.

A tricky scenario, for example, arises when a financial entity that is regulated under the Markets in Financial Instruments Directive (MiFID) II or the Markets in Crypto-Assets Regulation (MiCAR) and provides regulated services to another financial entity to which it makes the financial service available on an ongoing and digital basis.

The problem in this type of scenario is that the service provider – as a MiFID II investment firm or a MiCAR crypto-asset service provider – is already subject to financial regulatory requirements.

It is, therefore, important for the service provider to know whether it must meet third-party risk management requirements of DORA in addition to the existing compliance requirements for its regulated services.

The core question is, will any service with an ICT element provided by a financial entity to another financial entity necessarily trigger DORA's ICT third-party risk management requirements?

4. Third-party risk | How should financial entities treat ICT services that they receive from other financial entities in scope of DORA?

Supervisory and regulatory developments

In mid-2024, the joint European supervisory authorities (ESAs) - the European Banking Authority, European Insurance and Occupational Pensions Authority and European Securities and Markets Authority – published FAQs as part of their “DORA 2024 Dry Run Exercise on Reporting of Registers of Information”.

The ESAs concluded in the FAQs that if a financial entity requires authorisation, licensing or registration as a financial entity to provide a service, then that service is a regulated financial service and not an ICT service for the purpose of DORA.

In October 2024, a joint statement was made by trade and interest associations Futures Industry Association, Association of Financial Markets in Europe, the European Association of Central Counterparty Clearing Houses, European Central Securities Depositories Association and Federation of European Securities Exchanges, in which they called on ESAs to adhere to their view from their "dry run" exercise and to determine as quickly as possible that financial services should not be treated as ICT services.

The statement called for a clarification that regulated financial services should include all services and activities subject to supervision of a financial services regulator, including any ancillary or delegated services.

Just before DORA became applicable on 17 January 2025, the European Commission commented that, if a financial entity (within the meaning of DORA) receives service from a regulated financial institution, the receiving financial entity must conduct a two-part assessment to evaluate the service it receives.

First, the financial entity must assess whether the received service match elements for an ICT service within the meaning of DORA. The second step is a verification that both the service provider is regulated as a financial institution and the relevant service is a regulated financial service under EU law, national legislation of an EU member state or legislation of any third country. This means that the services must be regulated “anywhere in the world”.

If the answer to both questions is "yes", the service should be treated as predominantly a financial service and not an ICT service under DORA.

If a service provided by a regulated financial institution is unrelated or independent from its regulated financial services, it would constitute an ICT service under DORA.

4. Third-party risk | How should financial entities treat ICT services that they receive from other financial entities in scope of DORA?

Next steps and practical implications

The guidance by the Commission is an important step in clarifying DORA's scope and application, and it serves as a framework for financial entities to classify services received from other regulated providers.

Financial entities will have to adapt their approach to classification to consider both the nature of service and the regulatory status of the service provider. They will also likely need to review previous classifications to the extent that they may not be in line with the Commission's guidance. They should revise the DORA-mandated register of information to include or exclude some third-party arrangements.

The new guidance is no "one for all" solution. A case-by-case assessment will remain necessary, especially since the Commission's comment neither defines the terms "financial service" nor "being regulated". This brings up the question on how to treat a scenario in which the provided services *generally* require a licence and, however, an exemption applies.

5. Third-party risk | How does DORA apply to outsourcing agreements?

General principles and minimum contractual requirements when engaging third-party ICT providers in outsourcing

As a rule, DORA follows two major general principles when it comes to third-party ICT risk management and outsourcing.

The first principle is that the responsibility to comply with DORA and financial regulations remains with the regulated entities receiving ICT services by a third-party ICT provider. This is a similar principle as applied in non-DORA-related outsourcing by regulated entities.

The second principle is the principle of proportionality. It is explicitly mentioned in article 4 DORA, stating that: “Financial entities shall implement the [ICT risk management rules] in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.”

This second principle ensures that financial entities apply the regulatory requirements in a proportionate manner, taking into account the increased or reduced elements of complexity or the overall risk profile. It aims to prevent undue burdens on smaller firms, while maintaining robust operational resilience across the sector. The principle allows for flexibility in implementing measures, ensuring they are appropriate and effective for each specific entity.

Where, for example, financial entities might not have adjusted all outsourcing agreements with third-party ICT providers to DORA yet, national competent authorities might ask for a realistic and reasonable timetable for the planned adjustments instead of directly sanctioning those entities.

The German Federal Financial Supervisory Authority (BaFin), for example, has explicitly stated this as their general approach.

With this in mind, financial entities will be looking to ensure that they take a number of specific approaches when engaging third-party ICT providers.

5. Third-party risk | How does DORA apply to outsourcing agreements?

Enhanced due diligence

Performance of enhanced due diligence on third-party ICT providers will help financial entities ensure they meet DORA's operational resilience standard. An example would be assessing third-party ICT provider's cybersecurity measures, data protection protocols and business continuity plans – and documenting these assessments.

Contractual clauses in outsourcing agreements

These include specific clauses that address DORA requirements, such as risk management, incident reporting, audit rights and termination rights. For example, the agreement should include regular security assessments, immediate notification of incidents and the right to terminate the agreement if third-party ICT provider fails to comply with DORA. The clauses should be reviewed and updated regularly to reflect any changes in regulatory requirements.

Concentration risk management

The management of concentration risks involves avoiding over reliance on a single ICT third-party service provider. For example, services can be distributed across multiple ICT third-party service providers to mitigate concentration risk. This strategy should be documented in the financial entity's compliance handbooks and form part of the entity's risk management framework.

5. Third-party risk | How does DORA apply to outsourcing agreements?

Resilience testing

Provisions for regular resilience testing, such as "penetration" testing and disaster recovery exercises, can help ensure ICT third-party service provider's systems are robust and secure. For example, annual penetration testing and bi-annual disaster recovery exercises can help assess ICT third-party service provider's resilience. The financial entity's compliance handbooks should provide for the results of these tests to be reviewed and for any identified weaknesses to be addressed promptly.

Implementing DORA into existing outsourcing agreements

According to DORA, the specific minimum requirements for outsourcing agreements with ICT third-party service providers must be laid down in one, single document.

Outsourcing agreements that already existed before DORA often have a regulatory annex. Where DORA fully replaces any existing national regulatory provisions, the regulatory annex could be fully replaced with a DORA annex. Where existing national regulatory provisions remain applicable next to DORA, financial entities can follow two alternative approaches:

- They could have two separate annexes: the existing regulatory annex and a new DORA annex. This is clear and easy to implement. However, it might bring up issues with the priority of overlapping provision.
- An alternative is to have one combined annex, consisting of existing regulatory provisions as well as DORA-specific provisions. In this case, there is less risk of double regulation or issues with the priority of provisions. However, creating such combined annex is certainly more complicated from a legal technical perspective.

6. Third-party risk | What practical problems arise when negotiating contracts with potential ICT third-party service providers?

When negotiating outsourcing agreements with ICT third-party service providers, the principle of proportionality is often interpreted incorrectly by both parties.

ICT third-party service providers have very complex and highly standardised agreements in place and maintain a very defensive and sometimes non-compliant position. Further, "hyper-scalers" among ICT third-party service providers are in a strong position to negotiate agreements.

Financial entities subject to DORA are often overshooting the target by imposing requirements on ICT third-party service providers that go above and beyond the regulatory requirements.

When negotiating with ICT third-party service providers, financial entities will be looking to maintain a realistic position in the discussions, understand the implications of what they are asking, request additional requirements to the extent that there is a real objective need for it, and, of course, avoid presenting something as a DORA or regulatory requirement if it is not the case, to dial down on “advisory” tone.

7. Third-party risk | What risks must financial entities assess before contracting with ICT third-party service providers?

Under DORA, financial entities must conduct a comprehensive ex ante risk assessment before concluding contractual agreements with ICT service providers, especially those supporting critical or important functions.

This assessment will need to consider:

- Operational risks, including potential service disruptions, performance degradation, procedural errors and operational dependencies.
- Legal risks, covering contractual aspects, regulatory compliance, legal liabilities and jurisdictional implications.
- ICT risks, including cybersecurity threats, system vulnerabilities and infrastructure resilience.
- Reputational risks, considering impacts on customer trust, market perception and brand image.
- Risks related to confidential or personal data protection, assessing General Data Protection Regulation (GDPR) compliance and data protection mechanisms.
- Data availability risks, including accessibility, recovery capabilities, and data service continuity.
- Risks related to data processing and storage locations, considering data sovereignty aspects and cross-border transfers.
- Risks related to the location of the ICT service provider, evaluating geopolitical implications and host country stability.
- ICT concentration risks at the entity level, analysing dependencies on single providers and technologies together with risk diversification.

The assessment must be conducted at the financial-entity level and, where applicable, at consolidated and sub-consolidated level and completed before finalising any contractual agreement to ensure a comprehensive understanding of all risks associated with the ICT product or service provision.

8. Third-party risk | Is due diligence required before contracting with ICT third party service providers?

DORA explicitly requires financial entities to perform due diligence before contracting with ICT third-party service providers. When conducting due diligence under DORA, financial entities must evaluate providers proportionally to the scope of the service and its impact on business risks, particularly when the service supports critical or important functions.

When evaluating potential ICT third-party service providers, financial entities must assess whether the provider:

- Has a good commercial reputation, sufficient capabilities and expertise; adequate financial, human and technical resources; appropriate information security standards; proper organisational structure, risk management processes and internal controls; and necessary authorisations or registrations.
- Demonstrates capacity to monitor relevant technological developments, identifies best practices in ICT security and implement them to maintain an effective digital operational resilience framework.
- Uses or intends to use ICT subcontractors for performing critical or important functions or significant parts thereof.
- Is located in a third country or processes or stores data in a third country, and whether this affects operational or reputational risks or creates exposure to restrictive measures that could impact service delivery.
- Allows for effective audits by the financial entity, designated third parties, and competent authorities, including on-site audits.
- Acts ethically and responsibly, respects human and children's rights (including prohibition of child labour), follows environmental protection principles, and ensures adequate working conditions.
- Financial entities must also define the due diligence procedure, determining which of the following elements to consider in order to ensure an appropriate level of assurance regarding the effectiveness of the ICT third-party service provider's risk management framework: audits or independent assessments performed by the financial entity or on its behalf; independent audit reports made on request by the ICT third-party service provider; internal audit reports from the ICT third-party service provider; appropriate third-party certifications; and other relevant information available to the financial entity or provided by the ICT third-party service provider.

9. Overlaps | Do entities subject to NIS 2 Directive also need to comply with DORA?

The key difference between DORA and the Network and Information Security Directive 2 (NIS2) lies in the scope of application of these legal acts.

While DORA applies to selected categories of entities in the financial sector, NIS2 has a much broader scope and covers entities from various diverse sectors of the economy.

The only entities that are obligatorily subject to both DORA and NIS2 are credit institutions (primarily banks). This means that entities such as payment institutions, investment firms, insurers or insurance intermediaries, unless they operate in a hybrid manner as other entities required to comply with NIS2 provisions, generally do not fall under NIS2 and must comply solely with DORA.

In the case of credit institutions, the way DORA and NIS2 are applied together may vary depending on the country in which the institution operates. This is because, unlike DORA, NIS2 is a directive that requires the adoption of national legislative measures to be fully effective. Therefore, it is the local legislator in each EU member state who decides what specific security obligations credit institutions must meet, in addition to those arising from DORA.

In the event of any irreconcilable discrepancies, DORA, as an EU regulation, takes precedence over national law.

10. Overlaps | What is the interplay between DORA and AI Act?

AI systems and software components provided by third-party providers that implement general-purpose models, as defined in the Artificial Intelligence Act, may be qualified as ICT services under DORA. Similarly, ancillary services related to AI, such as system development and data operations necessary for AI, may be considered ICT services as well, including services supporting critical or important functions of financial institutions.

Even when AI systems are not provided or supported by third-party providers, they may still be subject to DORA's general requirements as ICT infrastructure, which must maintain high resilience and security levels.

This necessitates addressing these systems adequately in various security strategies, policies and plans. If AI systems used by the financial institution are recognised as high risk then risk analysis should be carried according to AI Act requirements. Examples may include systems for assessing creditworthiness or calculating minimum capital requirements.

11. Overlaps | Does DORA impact the way personal data is protected under GDPR?

DORA, which includes many information security requirements, also has significant implications for personal data protection. Institutions should ensure that the security mechanisms implemented to comply with DORA provisions are also applied to ICT services and systems that process personal data. In this regard, implementing DORA regulations can help financial institutions maintain compliance with the GDPR.

Regardless of the above, it should be remembered that if the GDPR requires a higher standard of protection than DORA, then the GDPR requirements should take precedence over DORA requirements. It is because the GDPR protects a special category of data.

Similarly, many requirements of DORA and the GDPR will be applied independently of each other. An example of these actions is conducting a risk analysis focused on the processing of personal data in accordance with the GDPR, independently of the risk analysis obligation under DORA. Another example is entering into data processing agreements with personal data processors that meet the GDPR requirements, independently of the contractual clauses specified in DORA.

12. Overlaps | Do companies with ISO 27001 certification also need to implement DORA?

Having an information security management system based on the ISO (International Organisation for Standardisation) 27001 standard does not exempt a financial institution from the obligation to implement DORA requirements.

Although ISO 27001 addresses many of the requirements specified in DORA, the two frameworks also have significant differences. The risk management foundations, security measures and audit and compliance mechanisms implemented by the financial institution according to ISO 27001 will therefore need to be reviewed and appropriately supplemented during the DORA implementation project.

This includes critical aspects such as testing operational digital resilience and managing risks from external ICT service providers. ISO 27001 and other recognised international standards do not address specific requirements related to reporting certain information to supervisory authorities, which is a key requirement of DORA. Therefore, while ISO 27001 standards help move towards DORA compliance, they can never fully ensure it.

Contacts

If you have further questions or need personalised advice, please do not hesitate to contact our DORA regulation experts:

Szymon Ciach
Counsel
Poland
+48 22 152 42 04
szymon.ciach@osborneclarke.com

Lukasz Wegrzyn
Partner
Poland
+48 22 152 42 42
lukasz.wegrzyn@osborneclarke.com

Tanja Aschenbeck
Partner
Germany
+49 221 5108 4196
tanja.aschenbeck@osborneclarke.com

Nunzia Melaccio
Partner
Italy
+39 02 5413 1787
nunzia.melaccio@osborneclarke.com

Juliet de Graaf
Partner
Netherlands
+31 20 702 8924
juliet.degraaf@osborneclarke.com

Jan Herrmann
Counsel
Germany
+49 221 5108 4478
jan.herrmann@osborneclarke.com

Gregoire Dumas
Counsel
France
+33 1 84 8 24548
gregoire.dumas@osborneclarke.com

Kamil Prokopowicz
Associate
Poland
+48 22 152 42 65
kamil.prokopowicz@osborneclarke.com

Giovanni Luca Andriolo
Junior Associate
Italy
+39 02 5413 1728
giovanni.andriolo@osborneclarke.com

Osborne Clarke is the business name for an international legal practice and its associated businesses.

Full details here: osborneclarke.com/verein

These materials are written and provided for general information purposes only. They are not intended and should not be used as a substitute for taking legal advice. Specific legal advice should be taken before acting on any of the topics covered