TaylorWessing

Digital Operational Resilience Act (DORA): Navigating the new regulatory landscape

1. Introduction

In recent years, the ever-increasing adoption of new technologies for the provision of financial services has reshaped the financial services industry in many different ways. This digital evolution has, nonetheless, made financial institutions largely dependent on the proper functioning of IT systems underpinning their financial infrastructure that have become the backbone of the global financial system in today's digital environment.

This has also opened a new chapter for the financial services industry that is now, more than ever, exposed to new types of risks, particularly those that can jeopardize its resilience to cybersecurity related threats. By recognising the critical need to bolster the digital operational resilience of the financial services industry in the EU, as part of its Digital Finance Package published in September 2020, the EU Commission has proposed the Regulation on digital operational resilience of the financial services industry, commonly known as the Digital Operational Resilience Act "DORA".

The rules on digital operational resilience applicable to financial institutions are currently fragmented and placed in various sector specific pieces of EU financial regulation (e.g., MiFID II, CRD, PSD2 etc.) as well as the Guidelines of the European Supervisory Authorities (ESAs) that are the in many ways the cornerstone of the EU regulatory framework on outsourcing arrangements that the financial services industry has been increasingly dependent on in recent years. However, a lack of proper harmonisation of sector specific regulations as well as the scope of application of the Guidelines on outsourcing of European Supervisory Authorities (ESAs) combined with their rather non-binding character (i.e. application on a comply-or-explain basis), leave space for regulatory ambiguity in this important area which in the digital age has become a backbone of the proper functioning of the financial services industry.

2. Scope

DORA aims to provide for further harmonisation of the existing rules as well as to bring the EU regulatory framework on digital operational resilience in the financial sector onto the highest legislative footing – a directly applicable EU Regulation, leaving no space for national divergences in interpretation and transposition at the Member State level.

Due to become operational on 17 January 2025, DORA puts new obligations on management of information communication technology (ICT) risks, ICT incidents and shortfalls, that financial institutions from almost every corner of the financial services industry will be required to comply with.

To that end, DORA will directly apply to a long list of financial entities operating in the EU that include:

- 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;
- UCITS 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;

In addition to financial entities, DORA is a very important piece of EU legislation that will have an impact on providers of ICT services to financial entities. DORA will impact ICT service providers in a different way depending on whether they qualify as critical third-party service providers (CTPP) under the new framework or not (more on the new regime for critical third-party service provider is contained below).

Whereas the critical third-party ICT service providers will be directly impacted by the new framework, being required to comply with a number of requirements and become subject to direct supervision of financial supervisory authorities, other ICT service providers will experience rather indirect impact of the new rules. To that end, ICT service providers will be required to ensure compliance with certain rules as a result of their contractual obligations towards financial entities, that are increasingly looking to redraft their existing contractual arrangements to ensure compliance with DORA.

3. Key Pillars of the new Framework

Under the new framework, the in-scope financial entities will be required as of beginning of next year to:

- Have effective internal ICT risk management framework in place that is comprised of a number of policies, procedures and processes aimed at ensuring financial institution's resilience in the digital environment;
- Comply with new requirements on identification, management and reporting of ICT risks;
- Comply with new regulatory requirements on digital operational resilience testing including (for larger entities) specific threat lead penetration testing;
- Have effective internal frameworks in place on management of ICT risks related to third parties that financial institutions rely on for the provision of ICT services (ICT third party risk management);
- Ensure that they meet new comprehensive contractual requirements when it comes to contractual arrangements with ICT third party service providers

4. ICT Governance & Risk Management

The Digital Operational Resilience Act (DORA) requires financial entities to implement robust ICT governance and risk management frameworks that are aimed at proper management of ICT risks that the entities may be exposed.

The management boards will bear ultimate responsibility to approve the digital operational resilience strategy of the entity that shall be in line with the overall risk strategy and business plan of the entity. This document, will in many ways represent the main building block of the internal ICT framework as part of which the entities will be required to:

- Identify all ICT assets (computer software, hardware, servers etc.) incl. physical components such as premises, data centres (i.e. physical and remote access control, information security)
- Identify all sources of ICT risks that their entity may be exposed to;
- Identify, classify and adequately document all ICT supported business functions, roles and responsibilities as well as all ICT assets within the entity;
- Implement effective procedures, processes and tools for effective management of ICT risks in accordance with the new requirements that shall boost the entity's digital operational resilience;
- Implement policies that limit the physical or logical access to information assets and ICT assets as well as strong customer authentication process;
- Implement procedures and controls for ICT change management that shall be used in the case of changes to software, hardware, firmware components, systems or security parameters of the entity;
- Allocate roles and responsibilities within the organisation that shall provide for effective task allocation when it comes to all ICT and ICT risk management related activities;
- Prepare internal documentation that shall serve as the basis for the internal processes and procedures implemented in accordance with the new requirements.

Under the new regime, the risk management framework will need to be reviewed at least on an annual basis. By taking a risk-based-approach, financial entities will also need to ensure that their internal risk management framework is being audited on a regular basis.

DORA also requires financial entities to create a new designated internal function that shall be responsible for the monitoring and management of ICT risks.

This new function appears to be combining the tasks and responsibilities of the risk management and the IT security officer, two separate functions that many incumbent financial institutions already have today.

However, it is questionable whether and to what extent this new function can be blended with any of the aforementioned existing functions due to the fact that the candidates for this new position will need to have deep knowledge and understanding of risk management in the ICT environment, by remaining conscious of the overall risk strategy of the entity.

Senior management will be responsible to maintain continuous overview of the ICT related activities of the entity and will bear ultimate responsibility for the compliance with DORA requirements.

As part of their internal risk management framework, financial entities are also required to put in place a comprehensive ICT business continuity policy that shall set the basis for internal business continuity arrangements, plans, procedures and mechanisms. These shall enable the financial entity to ensure the continuity of the financial entity's critical or important functions and quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and priorities the resumption of activities and recovery actions.

5. ICT incident management

Under DORA, financial entities will need to ensure compliance with new requirements on ICT incident management, that will for many types of financial institutions in the EU represent a brand new regulatory challenge.

Detection

Financial entities will be required to identify and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions and ICT assets.

To that end, they will need to implement processes and procedures that shall enable them to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure.

Classification

As part of their internal ICT governance and risk management framework, financial entities will need to have processes in place for the classification of detected ICT-related in accordance with the new regulatory requirements.

For this purpose, financial entities will need to classify the detected ICT incidents based on the mandatory criteria (like the criticality of the services affected, number of affected clients, financial counterparties and transactions, incidents duration, and service downtime etc.).

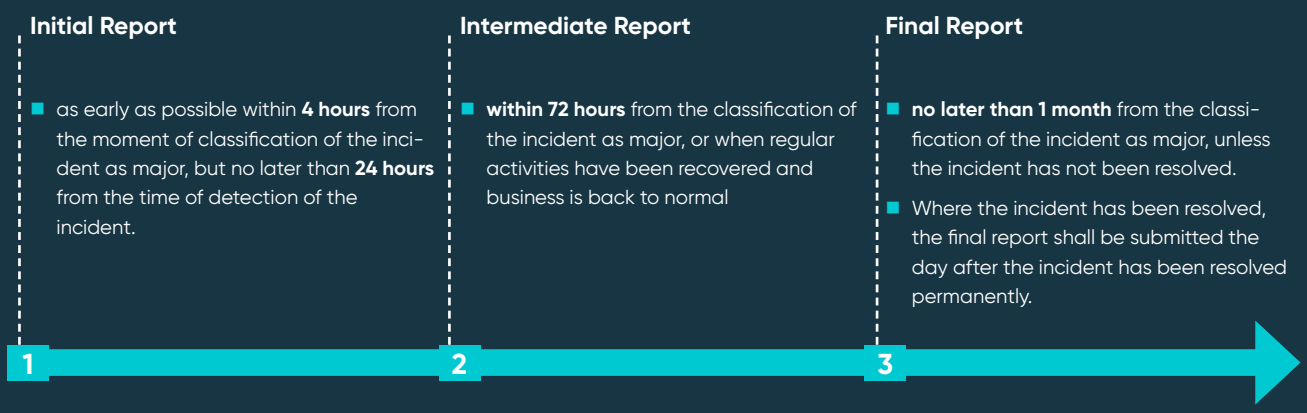
Reporting

The main aim of the classification is to enable financial entities to identify "major ICT incidents" that are to be reported to the NCA in accordance with the requirements on the reporting procedure.

Financial entities are required to report major ICT incidents in three separate steps: (a) immediately after the occurrence of the incident (within the first 24h), the first report needs to be submitted, (b) the intermediate report, once the normal functioning of the service has been restored and finally (c) the final report once the incident is entirely resolved.

The regulatory and implementing technical standards (RTS and ITS) of the European Supervisory Authorities (ESAs) lay down detailed requirements on the content of the each of the abovementioned reports and the timeline within which each of these reports is to be submitted.

In addition to major ICT incidents, financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients.



6. Testing

Under DORA, financial entities will also be required to comply with new testing requirements that will likewise as many other requirements under the new framework represent a novelty for certain types of financial entities.

For the purposes of ensuring compliance with the new requirements, financial entities will be required to establish a comprehensive digital operational resilience testing program (DRTP). The DRPT needs to set the basis for regular testing of internal ICT systems of the financial entities with the aim enabling them to assess their preparedness for ICT-related incidents and identify of weaknesses, deficiencies, or gaps in their digital operational resilience.

The digital operational resilience testing is to be performed on an annual basis.

Smaller group of financial entities will be required to perform the advanced testing by means of threat led penetration testing (TLPT) which is a testing practice that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat to the financial entity. The TLPT needs to be performed by certified professional testing providers (by accreditation body at the Member State level) every three years and shall cover at least critical functions.

ESAs have developed RTS specifying criteria based on which it will be determined which entities shall be subject to this obligation (these will include for instance, operators of trading venues, large credit institutions, central counterparties etc.)

7. Managing third party ICT risks

Conscious of the increasing dependency of the entire financial services industry on the IT expertise and infrastructure of specialized third-party providers (like big IT companies), the EU lawmakers have created a new set of requirements under DORA that will impose new obligations on financial entities when it comes to management of third-party related risks.

Pre-contractual phase

Financial entities must conduct thorough risk assessments and due diligence before engaging third-party ICT service providers. This involves evaluating the provider's ability to provide the required services in compliance with the applicable law, relevant security standards, ensure continuous performance of the service and process and store data in accordance with applicable requirements (incl. with respect to locations, access management procedures etc.).

Financial entities will also be required to assess and manage concentration risks associated with relying on a limited number of critical third-party providers. The concentration risk may arise when the financial entity is relying on a third-party service provider is not easily replaceable or when the financial entity is relying on one third-party providers for multiple areas of its operation (this can also be the case where the great number of group entities relies on one third-party provider).

Contractual Phase

By following the key principles anchored in the EBA guidelines on outsourcing arrangements, DORA creates the legislative basis for mandatory contractual terms that the financial entities need to have in place in their contractual agreements with third-party providers. Same as the EBA Guidelines, DORA differentiates between the arrangements supporting critical or important functions and all other arrangements by specifying top-up requirements for the former. For this purpose, financial entities are required to implement contractual provisions that provide the basis for efficient business continuity management, incident reporting and required ICT testing, grant necessary access and inspection rights as well as specify efficient exit management strategies that the entities can rely on.

The contractual requirements under DORA go in many ways beyond the scope of the existing EBA requirements. To that end, the financial entities are expected to evaluate the necessity for re-drafting of their existing contractual agreements with particular emphasis on ensuring the compliance with their overall requirements under DORA, conscious of their dependency on third-party providers' cooperation and assistance in many areas.

Post-contractual phase

Throughout the contractual relationship with the third-party provider, financial entities will be required to continuously monitor their performance, actively exchange information and closely cooperate in relevant areas with them (e.g. incident management and testing).

In addition to third-party providers, which are the first entities in the service providers' chain, financial entities must ensure that any subcontractors engaged by third-party providers also adhere to the same requirements laid down in the agreement concluded between them and the third-party provider. Further, when it comes to arrangements supporting critical or important functions, financial entities are expected to put a contractual obligation on third-party providers to conduct proper due diligence prior to onboarding their subcontractors as well as to put processes in place that provide for monitoring of their performance.

8. Critical third-party ICT-service providers (CTPPs)

Further, DORA is the very first piece of EU financial regulation that creates a supervisory framework for third-party providers of ICT services to financial entities that are deemed as critical.

For this purpose, the ESAs will have the mandate to assess which third-party providers, due to their presence in the EU and the number of financial entities relying on their services, are to be designated as critical (the so called critical third-party providers "CTPPs").

Once designated by the ESAs as such, CTPPs will be subject to direct regulatory oversight by one of the ESAs, that will be empowered (among other) to conduct on-site inspections, audits and impose fines that are in many ways reminding of the GDPR enforcement regime (stipulating fines in the amount of up to 1% of the global turnover).

9. Where do we stand with level 2 and level 3 acts?

Given that the level 1 text has left many questions unanswered, the ESAs were mandated to develop a number of RTS and ITS as well as level 3 Guidelines to specify DORA requirements in more detail. These are expected to provide clarity primarily in some more technical and complex areas of DORA like, digital operational resilience testing, incident management as well as the questions around the subcontracting that both financial entities and ICT service providers are becoming increasingly anxious about.

Below is a brief overview of the current state of level 2 and level 3 text:

	First Batch	Second Batch
Content	■ RTS on ICT risk management framework and RTS on simplified ICT risk management framework; ■ RTS on criteria for the classification of ICT-related incidents; ■ ITS to establish the templates for the register of information; ■ RTS to specify the policy on ICT services performed by ICT third-party providers.	■ RTS and ITS on content, timelines and templates on incident reporting ■ GL on aggregated costs and losses from major incidents ■ RTS on subcontracting of critical or important functions ■ RTS on oversight harmonisation ■ GL on oversight cooperation between ESAs and competent authorities ■ RTS on threat-led penetration testing (TLPT)
Consultation	■ **Closed (11 September 2023)**	■ **Closed (4 March 2024)**
Finalization date	■ **17 January 2024 (Final Reports published)**	■ **17 July 2024 (Final Reports expected – due date)**

Even though the ESAs work has provided some clarity on certain provisions of the level 1 text that required further clarifications, there is still a number of areas where certain level of ambiguity exist, primarily in terms of the extent of certain requirements as well as the subsequent supervisory expectations that both financial entities and critical ICT service providers will need to meet.

10. Conclusion and practical considerations

There is no doubt that DORA is becoming (if not being already) the number 1 regulatory priority for the EU financial institutions in 2024 whose implementation process is slowly but surely reminding us of some major EU regulatory change projects that we witnessed the past (like MiFID II and the SFDR for instance).

In contract to the aforementioned regulatory change projects that have largely upgraded the existing service specific regulatory frameworks, that financial entities have naturally been familiar with, DORA represents a new challenge for two reasons: First, the level of technical complexity and detail of new requirements that are much more understandable for the experts from the IT world (rather than financial services industry) is posing new challenges for financial entities and their legal and compliance teams. Second, the amount of effort that needs to be put in the implementation process, on the legal, operational and the technical front, is significantly higher than anything many financial entities have experienced in the past.

With only 6 months left until the go-live date, the implementation process will be everything but an easy task to accomplish and in-scope entities across the board are slowly but surely becoming aware of this.

Whereas in some EU Member States financial institutions are already subject to more restrictive regulatory requirements on management of ICT risks (like in Germany) the significance of the DORA framework shall not be underestimated: new requirements are not to be seen as a mere "EU replication" of national requirements on IT allowing German institutions to rely on their existing frameworks in full - On the contrary, financial institutions in Germany shall use this implementation period to conduct thorough gap analysis of their existing internal processes, procedures and documentation with the aim of identifying areas that will need to be aligned with the new DORA requirements that in many parts go way beyond the existing national requirements on IT based on BaFin circulars such as BAIT, KAIT and ZAIT.

In order to ensure compliance with DORA framework, financial entities will need to dedicate sufficient time and resources and aim to start with the preparation early on. For this purpose, they will need to:

- Conduct thorough gap analysis with the aim of identifying the level of their compliance with the new rules;
- Align their internal frameworks on management of ICT risks, ICT incident management, testing and other key requirements (that shall consist of robust and effective

internal processes, systems and procedures as well as proper documentation etc.) with the new framework;

- Start reviewing and redrafting (i.e. renegotiating the terms) of their contractual arrangements with ICT service providers in accordance with new requirements.

On the other side, ICT service providers shall likewise not underestimate the impact of the new framework on them, regardless of whether they are expecting be designated as CTPPs or not.

Starting with the re-drafting of the existing contractual agreements and preparation of internal processes that may get in focus of their customers (due to the new requirements that financial entities will be subject to) are some very first steps that ICT service providers shall consider making if they want to leverage "the first mover advantage" rather than waiting on the sidelines for the wave of customers' queries that will inevitably start to pile in by the year's end.

Contacts

Dr. Verena Ritter-Döring
Banking & Finance Regulatory
Partner

v.ritter-doering@taylorwessing.com

Miroslav Đurić, LL.M.
Banking & Finance Regulatory
Senior Associate

m.duric@taylorwessing.com

TaylorWessing

2000+ people
1200+ lawyers
300+ partners
28 offices
17 jurisdictions

Austria	Klagenfurt | Vienna
Belgium	Brussels
China	Beijing | Hong Kong | Shanghai
Czech Republic	Brno | Prague
France	Paris
Germany	Berlin | Düsseldorf | Frankfurt | Hamburg | Munich
Hungary	Budapest
Netherlands	Amsterdam | Eindhoven
Poland	Warsaw
Republic of Ireland	Dublin
Slovakia	Bratislava
South Korea	Seoul*
UAE	Dubai
Ukraine	Kyiv
United Kingdom	Cambridge | Liverpool | London | London TechFocus
USA	New York | Silicon Valley

* In association with DR & AJU LLC

Taylor Wessing statistics published are correct as of June 2024.