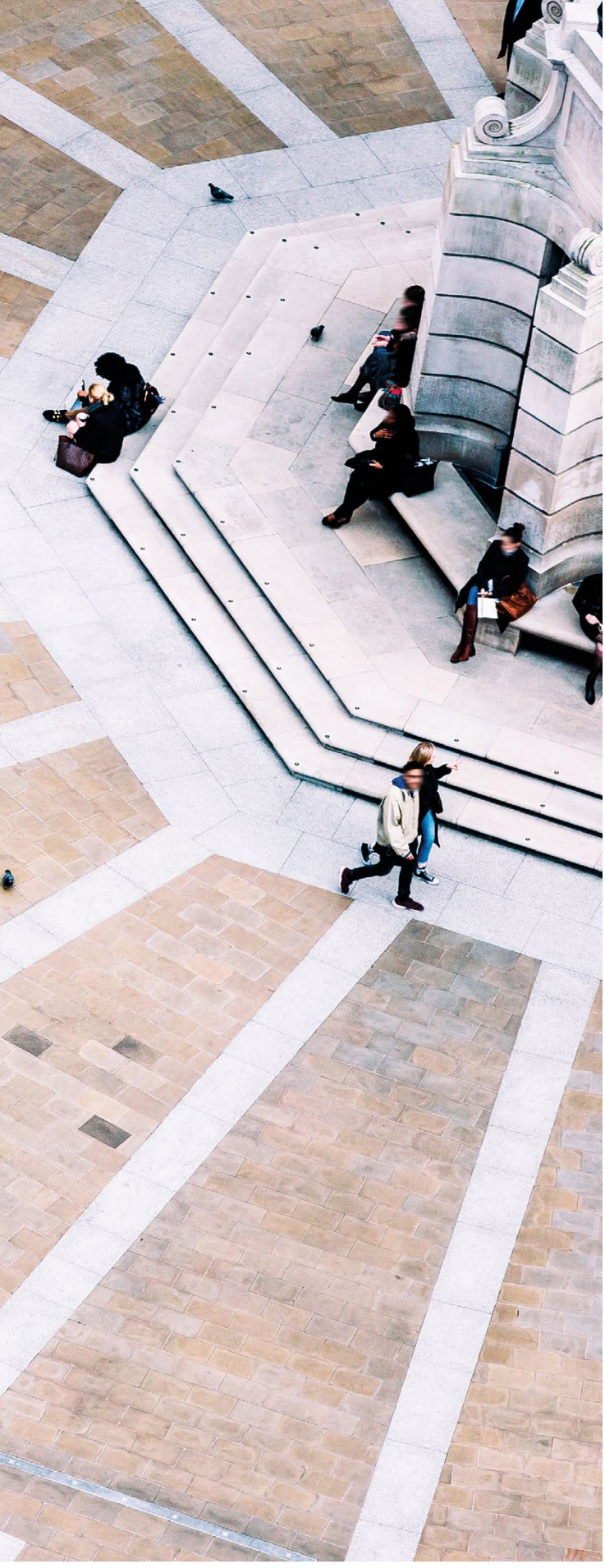
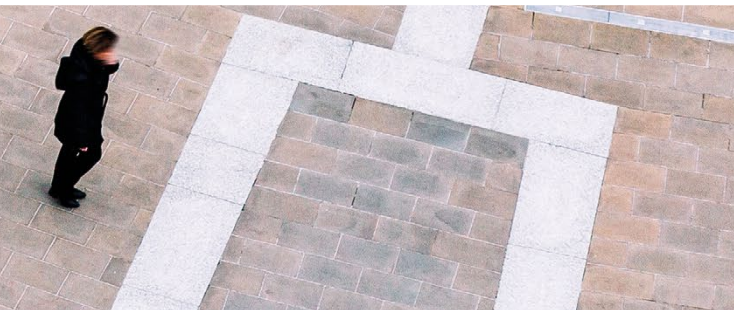
Digital Operational Resilience Act (DORA)

The next big beast on the regulatory horizon

pwc





I.

Background

The Covid-19 crisis has affected our world in a major way. Even the financial sector has had to adapt and rely more on digital systems, due to e.g. increased remote access from people's home office, payment services and all sorts of complex financial services. With this, the crisis has acted as a catalyst for the financial market to become increasing reliant on information and communication technologies (ICT), accelerating a trend which had already begun.

The growing importance of ICT has brought about the necessity to better regulate digital financial services in Europe. Therefore, on 24 September 2020 the European Commission (EC) adopted the Digital Finance Package (DFP). With this comprehensive plan to turn Europe into a digital financial center, the EC wants to make the continent fit for the digital age.

II.

Digital Finance Package

The EC argues that the introduction of the DFP and digital finance would unlock European innovation, create opportunities to develop better financial products for consumers and boosting digital finance would support Europe's economic recovery after the COVID Pandemic. Additionally, it will also create new channels for mobilising funding to support the Green Deal and the new Industrial Strategy for Europe.

By making rules safer and more digital-friendly for consumers, the EC aims to boost responsible innovation in the EU's financial sector, especially for highly innovative digital start-ups, while mitigating any potential risks related to investor protection, money laundering and cyber-crime.

The new rules that will be implemented with the DFP consist in particular of a digital finance strategy and legislative proposals on crypto-assets and digital resilience. Before taking a closer look at this brochure's main focus on digital resilience, we will have a brief look at the other two main points of the DFP:

The Digital Finance Strategy

The Digital Finance Strategy sets out the EC's key priorities and objectives over the next four years and how it plans to achieve them. The four stated priorities are:

- Reducing fragmentation in the Digital Single Market for financial services;
- Adapting the EU regulatory framework to facilitate digital innovation in the interests of consumers and market efficiency;
- Creating a European financial data space to promote data-driven innovation; and
- Addressing new challenges and risks associated with the digital transformation.

The strategy aims at creating a level playing field for incumbents and new players, such as technology firms entering the financial services space. It seeks to promote the uptake of artificial intelligence tools, blockchain technology, innovations in data management, data sharing and open finance.

Regulation on Markets in Crypto Assets

The 'Regulation on Markets in Crypto Assets' (MiCA) will provide legal clarity and certainty for crypto-asset issuers and providers. The new rules will allow operators authorised in one member state to provide their services across the EU. Safeguards include capital requirements, custody of assets, a mandatory complaint holder procedure available to investors and rights of the investor against the issuer. MiCA will boost innovation while preserving financial stability and protecting investors from risks.

The draft MiCA applies to "all representations of value or rights that may be transferred and stored electronically using distributed ledger and similar technology". Despite this broad definition, the EC emphasises that MiCA would not apply to assets that are already within the scope of other EU legislation (with a few exceptions such as e-money tokens).

III.

Digital Operational Resilience Act

Digital or ICT gives rise to opportunities as well as risks. These need to be well understood and managed, especially in times of stress. Policymakers and supervisors have therefore increasingly focused on risks stemming from an overreliance on ICT. They have notably tried to enhance firms' resilience by setting standards and coordinating regulatory or supervisory work. This work has been carried out at both international and European level, and both across industries as well as for certain specific sectors, including financial services.

ICT risks nevertheless continue to pose a challenge to the operational resilience, performance and stability of the EU financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the EU financial sector, only addressing ICT risks indirectly in some areas as part of the measures to address operational risks more broadly. Measures taken in relation to digital operational resilience were characterised by a number of features that limited their effectiveness. For example, they were often devised as minimum harmonisation directives or principles-based regulations, leaving substantial room for diverging approaches across the single market.

With the second main legislative proposal of the DFP, the Digital Operational Resilience Act (DORA), the EC now proposes that all participants in the financial system ensure they can withstand all types of ICT-related disruptions and threats. Banks, stock exchanges, clearing houses as well as fintechs will have to respect strict standards to prevent and limit the impact of ICT-related incidents. The EC also imposes an oversight framework on service providers (such as Big Techs) which provide cloud computing to financial institutions. Therefore, the proposal will create a consistent incident reporting mechanism that will help reduce administrative burdens on financial entities and strengthen supervisory effectiveness.

This brochure includes our assessment of the most important aspects of the DORA proposal and the practical implications that these reforms could hold for firms.

These include:

ICT Risk Management[1]

DORA is designed to better align financial entities' business strategies and how they carry out ICT risk management tasks. Therefore, the management body is required to maintain a crucial active role in steering the ICT risk management framework. The full responsibility of the management body in managing the financial entity's ICT risk includes a set of specific requirements, such as assigning clear roles and responsibilities for all ICT-related functions, continuously engaging in monitoring the ICT risk management and in allocating ICT investments and training.

Furthermore, to keep pace with a quickly evolving cyber threat landscape, financial entities are required to set up and maintain resilient ICT systems and tools that minimise the impact of ICT risk, identify all sources of ICT risk on an ongoing basis, set up protection and prevention measures, promptly detect anomalous activities and put in place dedicated and comprehensive business continuity policies as well as disaster and recovery plans as an integral part of the operational business continuity policy. The latter components are required for a prompt recovery after ICT-related incidents, in particular cyber-attacks, by limiting damage and prioritising the safe resumption of activities.

The regulation also covers the integrity, safety and resilience of physical infrastructures and facilities that support the use of technology and the relevant ICT-related processes and people as part of the digital footprint of a financial entity's operations.

[1] Art 4-14 Proposal COM(2020) 595 final.

ICT-Related Incidents: Management, Classification and Reporting of Risks[2]

Harmonising and streamlining the reporting of ICT-related incidents is achieved first of all via a general requirement for financial entities to establish and implement a management process to monitor and log ICT-related incidents, followed by an obligation to classify them in order to specify materiality thresholds.

Second, only ICT-related incidents that are deemed major must be reported to the competent authorities. The reporting should be processed using a common template and following a harmonised procedure. Financial entities should submit initial, intermediate and final reports and inform their users and clients where the incident has or may have an impact on their financial interests. Competent authorities should provide pertinent details of the incidents to other institutions or authorities, for example to the European Supervisory Authorities (ESAs), the European Central Bank (ECB) and the individual contact persons designated under Directive (EU) 2016/1148.

Lastly, to initiate a dialogue between financial entities and competent authorities that would help minimise the impact and identify appropriate remedies, the reporting of major ICT-related incidents should be complemented by supervisory feedback and guidance.

[1] Art 4-14 Proposal COM(2020) 595 final.

Digital Operational Resilience Testing[3]

The capabilities and functions included in the ICT risk management framework need to be periodically tested for preparedness and the identification of weaknesses, deficiencies or gaps, as well as for the prompt implementation of corrective measures. DORA allows for a proportionate application of digital operational resilience testing requirements depending on the size, business and risk profiles of financial entities. While all entities should test out ICT tools and systems, only those identified by competent authorities as significant and cyber mature should be required to conduct advanced testing based on Threat Led Penetration Testings (TLPTs).

DORA also sets out requirements for testers and the recognition of TLPT results across the European Union for financial entities operating in several member states.

Management of ICT Third-Party Risks[4]

Finally, DORA is also designed to ensure a sound monitoring of ICT third-party risks. This objective shall be achieved, first through the use of principle-based rules applying to financial entities' monitoring of risk arising through ICT third-party providers.

Second, DORA harmonises key elements of the service and relationship with ICT third-party providers. These elements cover the minimum aspects deemed crucial to enable a complete monitoring of ICT third-party risk by the financial entity throughout the conclusion, performance, termination and post-contractual stages of their relationship. Most notably, the contracts governing that relationship will be required to contain a complete description of services, an indication of the locations where data is to be processed, full service level descriptions accompanied by quantitative and qualitative performance targets, relevant provisions on the accessibility,

[3] Art 21-24 Proposal COM(2020) 595 final.
[4] Art 25-39 Proposal COM(2020) 595 final.

availability, integrity, security and protection of personal data. They must also include guarantees for access, recovery and return in the case of failures of the ICT third-party service providers, notice periods and reporting obligations of the ICT third-party service providers, rights of access, inspection and audit by the financial entity or an appointed third-party, clear termination rights and dedicated exit strategies. Moreover, as some of these contractual elements can be standardised, DORA promotes a voluntary use of standard contractual clauses which are to be developed for the use of cloud computing services by the EC.

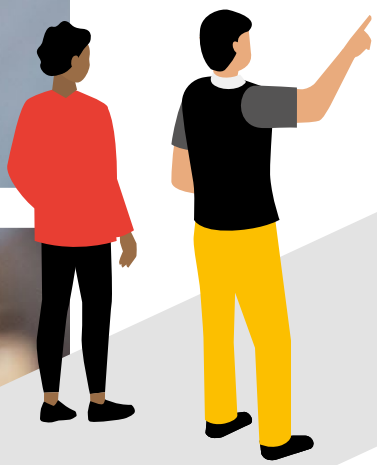
Finally, DORA seeks to promote convergence on supervisory approaches to the ICT-third-party risk in the financial sector by subjecting critical ICT third-party service providers to a European Union oversight framework. Through a new harmonised legislative framework, for which the ESA is designated as lead overseer, each critical ICT third-party service provider receives powers to ensure that technology services providers which fulfil a critical role to the functioning of the financial sector are adequately monitored at pan-European level. The oversight framework envisaged builds on the existing institutional architecture in the area of financial services, whereby the Joint Committee of the ESAs ensures cross-sectoral coordination in relation to all matters regarding ICT risk in accordance with its tasks regarding cybersecurity, supported by the relevant subcommittee (oversight forum).

Enforcement & Applicability

DORA is currently in the middle of its feedback period and the final text is expected in Q3 2021. Afterwards, DORA will be published in the Official Journal of the European Union and will enter into force. The Act is expected to become applicable around Q1 2023.

How can we support you?

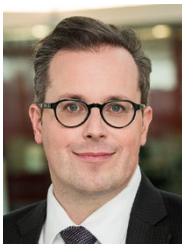
- DORA – ICT regulatory gap analysis
- Design ICT risk compliant management framework
- Digital operational resilience testing
- Design information sharing arrangements
- Support in the ICT transformation



Contacts

Dr. Antonios Koumbarakis
Head Strategic Regulatory and Sustainability Services, PwC Switzerland

antonios.koumbarakis@pwc.ch
+41 58 792 45 23

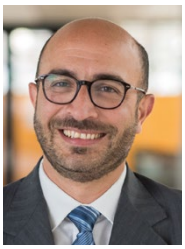


Dr. Günther Dobrauz
Partner, Leader Legal FS Regulatory and Compliance Services, PwC Switzerland

guenther.dobrauz@pwc.ch
+41 58 792 14 97

Alexandra Burns
Partner, Head Risk & Compliance / Internal Audit, PwC Switzerland

alexandra.burns@pwc.ch
+41 58 792 46 28

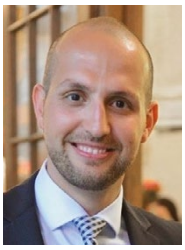


Patrick Akiki
Partner, FS Management Consulting, Lead, PwC Switzerland

akiki.patrick@pwc.ch
+41 58 792 25 19

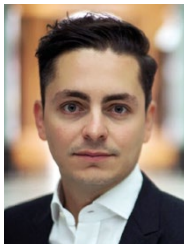
Matthias Leybold
Partner, Data & Analytics, PwC Switzerland

matthias.leybold@pwc.ch
+41 58 792 13 96



Morris Naqib
Director, Business and Regulatory Transformation

morris.naqib@pwc.ch
+41 79 902 31 45



Mark A. Schrackmann
Manager, Strategic Regulatory and Sustainability Services, PwC Switzerland

mark.schrackmann@pwc.ch
+41 58 792 25 60

Moritz Obst
Strategic Regulatory and Sustainability Services, Legal, PwC Switzerland

moritz.obst@pwc.ch
+41 58 792 47 19

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00