The Digital Operational Resilience Act (DORA): what (re)insurers and (re)insurance intermediaries must expect



Ms. Olivia Santantonio
Counsel
olivia.santantonio@lydian.be

Mr. Bastiaan Bruyndonckx
Partner
bastiaan.bruyndonckx@lydian.be

Ms. LIese Kuyken
Associate
liese.kuyken@lydian.be

In September 2020, the European Commission adopted the Digital Finance Package, including a digital finance strategy and legislative proposals on crypto-assets and digital resilience, for a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection and financial stability.

As part of this Digital Finance Package, the European Commission published its Proposal of Regulation on digital operational resilience for the financial sector, the so-called Digital Operational Resilience Act (Proposal of Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014)).

BACKGROUND

Currently the legal framework for ICT risk and operational resilience is fragmented and is constituted by various legislative acts as well as guidance from the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Market Authority.

With the Proposal of Digital Operational Resilience Act, the European Commission aims to adopt harmonised legislation regarding digital operational resilience, including identification, mitigation and management of cyber-risk, outsourcing and concentration risk in order to set a common standard across the EU financial system.

The Digital Operational Resilience Act will apply to all financial entities, including credit institutions, payment institutions, (re)insurers and (re)insurance intermediaries as well as ICT third-party service providers.

KEY ELEMENTS

The key elements of the Digital Operational Resilience Act for financial entities are the following:

- financial institutions must have a sound, comprehensive and well-documented ICT risk management framework to address ICT risk quickly, efficiently and comprehensively. Such framework must include a wide range of strategies, policies, procedures, ICT protocols and tools;
- financial institutions must manage ICT third-party risks and must have in place contractual arrangements for the use of ICT services to run their business operations;
- financial institutions must implement an ICT-related incident management process to detect, manage and notify ICT-related incidents and shall put in place early warning indicators; and
- financial institutions must have the possibility to exchange information on cyber threats and intelligence.

NEXT STEPS

The Proposal of Digital Operational Resilience Act is now going through the EU's ordinary legislative procedure. The final text is expected to come into effect in the first months of 2022 and will transform the provisioning of financial services significantly across the European Union.