How the digital operational resilience act (DORA) helps your continuity, come rain come shine

The Digital Operational Resilience Act (DORA) aims to harmonise and upgrade Information Communication Technology ('ICT') risk requirements throughout the EU financial sector and establish a streamlined digital operational resilience framework across the EU. Concurrent with DORA, the Network and Information Security 2 (NIS2) directive was published. This directive was formed with a similar goal of improving EU infrastructure resilience. Financial institutions are within the scope of NIS2 too, where DORA is more specific DORA takes precedence. The legislation is geared at ensuring and enforcing a robust financial sector in recognition of the vital importance of it in our day to day lives - because we, as consumers, depend on it and at the same time entire value chains cannot function without financial infrastructure(s).

The lens of the legislator is thus to keep the whole ecosystem running. This can be easily aligned with the objective of the individual organisations as they also aim to maintain the integrity of their business, not solely for the role they play in the ecosystem but for their continuity. The result of which is that the requirements should be recognisable instruments and objectives because these should ideally already be part of your IT & technology risk management. Now is a good time to re-evaluate your ICT risk management practices to ensure they are greater than the sum of the parts to effectively keep your business up and running come rain come shine.

What is unique about DORA and whom does it affect?

The regulation is unique in introducing a Union-wide end-to-end holistic legislative framework for effective ICT risk management, ICT and cybersecurity operational capabilities in addition to third party management to ensure a consistent provision of ICT services across the entire value chain. Oversight is executed by the European Supervisory Authorities (ESAs). ESAs will take on the role of regulating financial institutions and third-party providers. This means third-parties providing critical services to financial institutions are in scope of supervision directly, as part of this oversight, and indirectly, through requirements placed upon financial institutions to properly dictate and check risk mitigation measures at their service providers.

DORA will bring into scope more than 22,000 financial entities operating in the EU including traditional financial sector entities such as exchanges and clearing houses, credit institutions, investment firms, alternative fund managers, insurance undertakings and intermediaries, crypto asset providers, data reporting providers and cloud service providers and ICT service providers.

Although DORA builds on familiar practices in information risk management which already existed albeit less holistic, in previous regulation for banks and insurers, the requirements will be novel for other market participants that fall under the regulation. The key difference between DORA and previous regulations is the breadth and depth of requirements that the regulation will introduce to ensure the ecosystem doesn't have any weak links and individual institutions take a holistic approach. The regulation will introduce specific and prescriptive requirements not just for financial entities but all market participants operating in the EU that provide critical services to the financial entities including third party service providers.

How to overcome challenges associated with the new DORA requirements

Getting insight into the extent in which your organisation is complying with DORA requirements and the (to be released) technical standards is of course essential for the development of your DORA compliance roadmap. Below we present an overview of the most important elements for financial sector companies in their journey to comply with DORA based on our experience.

In line with the regulatory agendas of both DNB and ECB, we foresee the biggest challenge to be the process of embedding ICT third-party risks as an integral part of your organisations ICT risk management. Overseeing and managing the ICT risks for the full third-party chain in sufficient depth, and responding in the right way to the risks arising from third parties (or their third-parties) will be a big undertaking. A key challenge will be getting the relevant information in a timely manner from the third-party chain. This will be necessary to identify risks and incorporate those findings as an integral part of your risk management. Without this your ability to make the right decisions will be hindered. A closely related challenge will be ensuring that your organisation has a full grasp on which (business) services rely on which (business) processes, supported by which systems and which data they process. Once that picture is complete, and your organisation understands the process and systems you depend on with which vendor, you should have a pretty good idea where your risks reside, how they are mitigated and if these are concentrated with particular third parties.

As DORA extends the oversight of the regulator to these third parties and certain third parties are commonly used by financial institutions, we expect a natural force to increase maturity at these said third parties over time.

Please find below the most important elements to focus on:

- Make sure a holistic and solid ICT strategy is in place aligned with your ICT risk management strategy to ensure resilience of your business. This needs to be aligned with business strategy and requires senior management ownerships which ensures senior management is sufficiently knowledgeable and skilled on ICT risk topics and timely ICT risks reporting is in place covering all ICT related risk for their decision making.
- Make sure a high level of maturity ICT asset management is in place which ensures identification and assessment of all assets connected to business processes and services as a basis for identifying and mitigating risks.
- Make sure a high level of maturity (security) incident management is in place, including scaling up on resources, which provides the basis for timely response and recovery on (security) incidents while enabling timely reporting to your key stakeholders such as the regulator.
- Make sure the detection of anomalous activity is multi-layered and covers all critical assets to ensure a high degree of certainty that unauthorised activities are captured and fed into the incident process for follow-up.
- Make sure a solid digital operational resilience testing program is in place that covers all critical IT systems and applications, which has a multidimensional security view and a sound risk- based approach to ensure all relevant security aspects are covered. Work on different testing scenarios – including vulnerability tests, penetration testing, etc.
- Make sure your ICT outsourcing approach has a full value risk chain perspective which integrates the risks for the full chain of your organisations ICT outsourcing chain and ensures the potential impact on the organisation is known and accounted for.

What do you stand to gain?

In the past decade various ESA`s have released guidance on ICT risk management and outsourcing which has been used by financial regulators (e.g. ECB, DNB) to execute their oversight function resulting in an increased focus on maturing the ICT risk management in the financial sector.

The release of DORA is a natural moment to reassess the maturity of your ICT risk management practices and to identify the gaps in your capabilities to comply with the DORA regulation. Taking stock by assessing your current ICT risk posture should be your starting point to consolidate improvements in your controls and capabilities (standardising, eliminating, automating) and to determine your direction going forward. This will enable you as an organisation to make ICT risk management more (cost-)effective and efficient at the same time while preparing yourself for audits and on-site regulatory inspections that we expect DORA to trigger.

For some organisations in the financial sector DORA will be a starting point to accelerate moving to the minimal required maturity level and for other organisations it will be an opportunity to further enhance their capabilities to make them more efficient and effective at keeping your business up and running, as we said, come rain come shine.

Who to contact

Anthony Kruizinga
Partner,
Risk & Regulation lead
anthony.kruizinga@pwc.com

Seda Foppen
Director,
IT Risk & Regulation
seda.foppen@pwc.com

Martijn Koopal
Partner,
Legal Services Lead
martijn.koopal@pwc.com

Job van Ommen
Senior Manager,
Cybersecurity & Data Privacy
job.van.ommen@pwc.com

Take a look at our **website.**

pwc