KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

What Does the DORA Cyber Regulation Mean for Enterprises?

MAY 2022

As cybersecurity concerns seem to only grow, regulators are often stepping in to try to help, such as by standardizing how enterprises assess their security posture. One of the latest examples is the EU's proposed Digital Operational Resilience Act (DORA), which affects the financial services industry and could become finalized in 2022.

While implementation of DORA could take a while — many expect that to occur in 2024 — financial institutions within the EU, as well as potentially globally, should start to think about compliance now. Doing so can help in terms of meeting regulatory requirements as well as strengthening cybersecurity capabilities and risk assessments.

What Is DORA?

At its core, DORA aims to reduce digital risk in the financial sector. As the European Commission (EC) notes, member states within the EU have gone ahead with their own digital initiatives in recent years, but that has led to overlaps, gaps, and related issues. Instead, the EU wants to have a full, consistent framework in place to improve digital resilience.

"It removes obstacles to, and improves the establishment and functioning of the internal market for financial services by harmonizing the rules applicable in the area of ICT (Information and Communications Technology) risk management, reporting, testing and ICT third-party risk," explains the EC.

Some of the specifics may change, but in general, this framework builds on some existing, yet fragmented regulations and ideally will improve how financial institutions and service providers, both in the EU and potentially elsewhere in the world, manage cyber risk.

Who Needs to Comply With DORA?

DORA isn't just something that heavily regulated enterprises, like big banks, need to focus on. Instead, the regulation could apply to businesses both large and small, including those who might be new to this type of compliance.

"Many of these entities are not traditionally regulated financial service providers such as central counterparties, crypto-asset and crowdfunding service providers, management companies, audit firms and ICT third party service providers," explains KPMG.

Including third-party service providers means that the regulation extends to non-financial organizations, "which will include services such as cloud resources, data analytics and audit," notes EY.

And while the regulation is EU-based, that doesn't mean that other organizations around the world are necessarily off the hook. Similar to how the EU's General Data Protection Regulation (GDPR) has affected businesses internationally, so too could DORA.

"If a non-EU financial institution is doing business in the EU or has an EU subsidiary, or a non-EU based technology company serves EU-based financial institutions remotely, then itself and its supply chain are caught by DORA," notes Ilias Chantzos, Global Privacy Officer and Head of EMEA Government Affairs, Broadcom, in a Broadcom article. He adds that DORA could also inspire other regulators around the world to take similar measures.

How to Prepare for DORA

Given the large scope of DORA, many organizations will likely need to comply, and it can pay off to start preparing well in advance of implementation. Even if it turns out that your enterprise doesn't need to comply, certain actions can still be beneficial cybersecurity practices that you might want to engage in to reduce your cybersecurity/financial risk anyway.

For example, to prepare for ICT risk management requirements as part of DORA, "conducting a gap analysis of existing ICT risk management and governance practices, specifically through a critical function lens, will be a worthwhile exercise," notes Deloitte. Similarly, Deloitte adds, reviewing incident reporting capabilities, resilience testing and understanding third-party risk could all be useful for preparing for DORA while also being something that's good to do anyway.

Working with partners like Kovrr can help, such as to understand your current security posture and to identify ways to improve resilience. Kovrr's Quantum cyber risk quantification platform can help enterprises with financial quantification and risk management by looking at what's at stake in terms of first-party assets that companies directly manage, as well as third-party service provider risks.

Other means of preparation, such as penetration testing, would need to be carried out by organizations separately, but it can still be useful to understand the monetary implications first.

Through cyber risk quantification, you can figure out what different types of cyber incidents might mean in terms of financial losses. Seeing what's at stake could then help motivate stakeholders within your enterprise to start complying with DORA early, including investing in pen testing tools, as a way to reduce financial risk, rather than looking at DORA as a compliance burden.

> **Want to see how Kovrr can help your organization financially quantify cyber risk and get on the road toward DORA compliance? Get your FREE ransomware cyber risk exposure today!**

The Author

Shalom bublil

CPO

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models. To learn more please contact the Kovrr team: contact@kovrr.com