cyberunity

the who, what, when, and why:
Digital Operational Resilience Act (DORA), 2023 (EU)

who (will DORA impact)?

The Digital Operational Resilience Act (DORA) will impact various stakeholders in the EU digital economy, cybersecurity ecosystem, and regulatory landscape. It will shape the digital operational resilience of **financial institutions** (banks, investment firms, clearing houses, insurers, and fintechs) and **digital service- and infrastructure-providers** (providers of tech-solutions and cybersecurity services). This includes non-EU entities providing services to EU financial institutions, whether they are unaffiliated third parties or group companies affiliated with EU financial institutions.

DORA will also impact **regulatory authorities** (European Supervisory Authorities who will be tasked with enforcing DORA compliance) and **end-users** (consumers who will benefit from improved operational resilience through a reduction in service disruptions, cyberattacks, and data breaches).

what (is DORA)?

DORA harmonises key digital operational requirements by providing a comprehensive digital operational resilience framework for financial entities and ICT service providers. In short, it sets out technical requirements for **ICT (third-party) risk management**, **incident response and reporting**, **information sharing** to authorities regarding cyber threats and vulnerabilities, and **digital operational resilience testing**.

DORA also addresses **contractual requirements** for ICT third-party service providers and financial institutions, defining rules for oversight frameworks that such service providers must adhere to.

when (is the deadline for DORA implementation)?

DORA officially entered into force on January 16, 2023, and the aforementioned parties will be required to achieve compliance by **January 17, 2025**.

cyberunity

why (does DORA matter)?

The financial sector increasingly depends on tech companies and their digital infrastructures to enable financial services. This increases financial institutions' security exposure and makes them more vulnerable to cyber-attacks and incidents.

When not managed properly, ICT risks can not only impede corporate daily business but can critically disrupt financial services, especially across national borders. This in turn, can have significant adverse impacts on individual companies, entire economic sectors and even the European economy as a whole. The fact that ICT risks are multiplying at breakneck speed makes such governance considerations all the more important.

Not least in Switzerland, home to myriad internationally active third-party ICT service providers, more stringent consideration of such risk-related considerations will become increasingly important. While Switzerland is not an EU member and therefore not beholden to DORA, Swiss third-party service providers serving EU financial institutions will increasingly have to abide by the standards set out in DORA if they want to remain at the forefront of the European financial industry.

find out more:

- European Parliament – DORA At A Glance
- Digital Operational Resilience Act.com
- Digital Operational Resilience Act (DORA) - EIOPA

interested in what DORA means for your business?

Joshua Bucheli (cyberunity AG) and John Corona (Osmond GmbH) look forward to hearing from you!

Stay tuned for more - look out for our next **cyberbyte** on Switzerland's new Information Security Regulation