REALCGR®
Regulatory Technology

RealCGR® provides "RaaS" ("RegTech" or Regulatory Technology as a Service).
We provide secured integrated software that automates, simplifies and embeds compliance into company governance processes. We optimise compliance effectiveness, while keeping cost-of-governance in control.

SIX PILLARS OF THE DIGITAL OPERATIONAL RESILIENCE ACT

*The **D**igital **O**perational **R**esilience **A**ct ("**DORA**") is the proposal for a European legislation regarding risk management and third-party risks within the financial sector. The first draft of this regulation emerged in September 2020. Multiple drafts have been created since and a final version is expected to arrive and be implemented in 2022.*

The Risk Management Framework

The DORA law aims to better link business strategy with ICT strategy and ICT-risk management performance within financial institutions. In order to do this, the management body will have to play a critical and active role in driving the ICT risk management framework. This framework will include risk policies, processes, strategies, controls, and instruments that must be reviewed at least once a year
or after each major incident.

An overarching principle of the DORA act is the fact that management is fully responsible for managing ICT risks within their financial entity. The DORA act also sets out specific requirements, such as the assignment of clear roles and responsibilities for all ICT-related functions, a continuous engagement in the control of the monitoring of the ICT risk management. Therefore, financial entities must ensure sufficient budget and resources are allocated to fulfil the financial entity's digital operational resilience needs.

ICT risk management requirements

The requirements for ICT risk management are based on appropriate international, national, and industry-set standards such as ISO 27001, ISO 22301, guidelines, and recommendations, and center around certain functions in ICT risk management. Financial institutions must put up and maintain resilient ICT systems and technologies to limit the effects of ICT risks and be able to ensure they can keep pace with a rapidly expanding cyber threat landscape. In order to manage ICT risks, financial entities must also identify all sources of risk and implement prevention and detection mechanisms. Every financial institution must have dedicated and thorough operational business continuity policies and disaster recovery strategies in place.

ICT-related incident reporting

The DORA regulation aims to harmonize and streamline ICT-related incident reporting. As a result, financial institutions must put in place procedures to track and document all ICT-related incidents. These incidents are then classified according to factors such as duration, amount of data lost, severity, and economic impact. A uniform template must be used to create an initial, intermediate, and final report for each big incident. If the incident has the potential to affect their clients' financial interests, the financial body must notify them as well.

Digital operational resilience testing

The ICT risk management framework's capabilities and functions must be tested on a regular basis for preparedness and to identify any flaws, inadequacies, or gaps. Corrective steps must be implemented based on the results of these tests. This regulation allows for proportionate application of digital operational resilience testing requirements based on the size, business, and risk profiles of financial entities: while all entities should test ICT tools and systems, only those deemed significant and cyber mature by competent authorities should be required to conduct advanced testing.

ICT third-party risks

The regulation is intended to ensure that third-party ICT risks are properly monitored. As a result, financial institutions must keep an eye on the risks related to their ICT third-party service providers. However, monitoring alone will not suffice. Contracts with these service providers must also be governed by financial entities, with precise explanations of essential components such as service descriptions, location, service levels, availability, integrity, and recovery in the event of failure. Financial institutions may also conduct audits to ensure that the third party meets all standards.

This objective will be achieved first through the respect of principle-based rules applying to financial entities' monitoring of risk arising through ICT third-party providers. Second, this legislation harmonizes important service and relationship features with ICT third-party providers. These sections include the basic requirements for a thorough monitoring of ICT third-party risk by the financial entity during the conclusion, performance, termination, and post-contractual stages of their relationship.

Information Sharing

The DORA regulation authorizes financial companies to set up agreements to share cyber threat information and intelligence among themselves in order to improve awareness of ICT risks, reduce their spread, and support their defensive capabilities and threat detection methodologies.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

REALBCP® Business Continuity

Business Continuity, governance
ISO 22301, ISO 77001

REALDPG® Data Protection Governance

Dataprotection Governance
GDPR, ISO 27001 EU & UK GDPR, ...

REALDSR® Data Subject Rights

Data Subjects Rights
Using blockchain tables

REALCRC® Crisis Communication

Smart Alerting and Crisis Communication

Please visit **www.realcgr.com** for more information.