citalid

2023

How can Cyber Risk Quantification help comply with *DORA*

Info Sheet

– Sapere aude - Osez savoir - Dare to know – Sapere aude - Osez savoir - Dare to know –

CONTEXT

Introducing DORA & CRQ

A European framework for digital resilience

The Digital Operational Resilience Act (DORA) is an initiative from the European Commission aiming to strenghten the digital operational resilience of the financial sector by ensuring that organizations can whistand and recover from operational disruptions affecting their information and communication technologies.

DORA emphasizes the importance of implementing strong measures and controls across systems, tools, and third-party entities. Additionally, it underscores the necessity of developing and testing effective continuity plans.

DORA primarily targets financial organizations, encompassing banks, investment firms, and electronic money entities. However, the initiative's strategic focus extends beyond these entities to ensure digital resilience throughout the entire value chain.

The initiative recognizes that the interconnected nature of the financial sector introduces escalating risks from a wide array of cyber threats and associated vulnerabilities. This heightened risk landscape underscores the importance of extending the scope of DORA to include third-party providers, such as those offering cloud services and operating data centers. By doing so, DORA acknowledges the critical role played by these ITC service providers in the overall cybersecurity posture of the financial ecosystem.

In addition, DORA has a primary objective of establishing a unified regulatory framework across European Union (EU) countries. This goal is pursued through the introduction of a comprehensive and synchronized regulatory framework. The intention is to create a cohesive structure that allows every EU member state to actively contribute to the development and maintenance of a stable financial system. By fostering regulatory consistency and coordination, DORA seeks to enhance the collective resilience and integrity of the financial landscape within the European Union.

Cyber Risk Quantification (CRQ)

Cyber Risk Quantification is the process of assigning financial metrics to various aspects of cybersecurity risks in order to assess and measure the potential impact and likelihood of those risks. This approach involves using quantitative methods to analyze and express cyber threats and vulnerabilities in terms of financial, operational, or other relevant impacts on an organization.

The goal of cyber risk quantification is to provide a more objective and data-driven understanding of the potential impacts of cybersecurity threats. This involves evaluating the probability of a cyber event occurring, estimating the potential financial losses or operational disruptions, and assessing the effectiveness of existing security measures in mitigating these risks.

REQUIREMENTS

Leveraging CRQ towards DORA's requirements

Leverage Citalid's Cyber Risk Quantification platform outcomes to support your compliance efforts towards DORA.

ICT Risk Management Processes & Governance

An effective ICT risk management framework aims to identifying, evaluating, and mitigating potential risks. Simultaneously, a comprehensive information set is instrumental in documenting systems and protocols, enabling vigilant monitoring to detect and address threats within the system. This integrated approach is complimented by recovery and backup plan, ensuring organizations are proactive in risk management and well-prepared to respond swiftly to any disruptions or security incidents.

- **For any given risk scenario, Citalid estimates the likelihood and the impacts of an attack targeting your company. You get a quantified risk to prioritize mitigation efforts towards threats and business assets.**
- **Citalid provides prioritized recommendations for controls which help prevent or mitigate risks, including backup and recovery controls.**
- **Citalid can model insurance strategies that complement backup, recovery and continuity plans.**

Incident Reporting & Information Sharing

The ICT incident management process involves a systematic and organized approach to handle and mitigate ICT incidents. A crucial component of this process is the reporting to competent authorities, fostering a coordinated and collaborative response.

- **Citalid enables evidence-based reporting on the effectiveness of implemented controls for handling and mitigating ICT incidents.**

Third-Party Risk Management

Ensuring compliance and clearly defining rights and obligations are integral aspects of engaging with ICT services and cloud providers through contractual agreements. Additionally, a crucial component of effective risk management involves conducting third-party risk assessments and implementing continuous monitoring mechanisms. This proactive approach enables organizations to evaluate and address potential risks associated with their external service providers.

- **Citalid enables 3rd party listing and connects to risk rating solutions to help organizations classify 3rd parties depending on their cyber risk score.**
- **Citalid enables modelling of attack scenarios coming through 3rd party providers.**

Digital Resilience Testing

Within the framework of ICT risk management, there is a crucial component— a comprehensive ICT incident testing program. This program is designed to systematically assess information systems, aiming to identify and address vulnerabilities. By proactively subjecting the ICT infrastructure to various testing scenarios, organizations can enhance their preparedness and responsiveness to potential incidents.

- **Citalid uses patented attack simulations of any given risk scenario so organizations can quantify vulnerabilities at scale and effectively prioritize mitigation efforts towards assets.**

Want to know more? Book a demo now!