**Understanding Digital Operational resilience Act (DORA)**

Over recent years, ICT risk has been addressed differently by various financial supervisors within the European Union. This has caused an inconsistent approach with national non-harmonized regulatory approaches. Meanwhile, cyber threats are growing in number and severity. Incidents such as phishing, identity theft, and particularly ransomware can lead to a potential systemic crisis that threatens financial stability all around the world.

The digital Operational Resilience Act or DORA proposes to harmonize the ICT risk management practices in the EU financial sector by consolidating third-party risk management requirements in financial entities across Europe. It introduces the obligation to address five specific pillars namely ICT risk management, ICT incident reporting, Digital operational resilience testing, information and intelligence sharing, and ICT third-party risk management. It is an important step for banks and firms in the global financial industry as well as ICT service providers to mature their third-party risk management programs and there are penalties for failing to comply with DORA both financial and criminal.

**Impact on organization**

Digital Operational resilience act gives a definition of criticality thresholds for services that are provided to financial institutions. If a particular organization is a direct service provider to a financial institution and its services meet the required thresholds, then the company is subject to DORA. This particularly means that the organization will be directly supervised.

On the other hand, for those organizations that do not meet the DORA thresholds, the regulation still applies, but direct supervision is not required. Instead, the customers are required to demand certain contractual terms to achieve compliance.

**Requirements of DORA**

There are certain rules that all sorts of financial institutions and suppliers should follow. Since this is still in the draft phase, these are the fundamental requirements. These are as follows.

**1. Management of risk**

The Digital Operational Resilience Act provides guidelines and rules which should be followed by all kinds of financial organizations. These guidelines are made to provide help to organizations to formulate a better risk management program.

**2. Testing of resilience**

DORA suggests that all forms of covered organizations implement resiliency testing programs. These are based on their risk assessments. This helps to identify any sort of error before they pose a serious threat.

**3. Sharing of intelligence**

Different malicious actors who are working in the financial industry target different organizations at once. Sharing the threat intelligence, helps the entire industry to become more alert and prepared to face ongoing cyber crimes.

**4. Managing supply chain**

This resilience act imposes different requirements on financial institutions’ relationships with their suppliers. On the other hand, financial institutions are also required to have different strategies to manage the risks that these suppliers create.

**5. Different incident reporting**

Digital Operational Resilience Act extends the scope of incident reporting and also attempts to streamline the process. Using faster reporting also encourages rapid incident investigation and its appropriate response, which helps to reduce the impact of a breach. This can also be used to help detect unknown intrusions in different other networks.

**6. Accessing audit**

This regulation enables regulators and monetary organizations to perform audits throughout the supply chain. This in turn helps to drive compliance.

**7. Analysis of retrospection**

maximum organizations try to learn and introspect from their internal incidents, but this resilience act encourages studying and revising policies that are based on external incidents as well.

**Objectives of DORA**

There are different types of objectives of DORA. These are as follows.

* This resilience act ensures that financial organizations assess the effectiveness and integrity of their prevention and measures and where their ICT vulnerabilities stand.
* The objective of this act is to provide financial authorities with access permission to information on ICT-related incidents to improve their cyber threat knowledge.
* To strengthen the regulations for indirect supervision.
* These acts can allow direct monitoring of all sorts of activities of ICT third-party service providers.
* incentivize the exchange of information about cyber threats.

**References**

1.<https://www.myrasecurity.com/en/digital-operational-resilience-act-dora/>

2.<https://www.checkpoint.com/cyber-hub/cyber-security/what-is-siem-security-information-and-event-management/what-is-the-digital-operational-resilience-act-dora/>

3.<https://www.pwc.com/mt/en/publications/technology/dora.html>

4.<https://www.aima.org/regulation/keytopics/digital-operational-resilience-act.html>

5.<https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/>

6.<https://www2.deloitte.com/nl/nl/pages/risk/articles/digital-operational-resilience-act.html>

7.<https://www.forbes.com/sites/forbestechcouncil/2022/09/12/three-areas-to-consider-in-preparing-for-the-digital-operational-resilience-act-dora/?sh=69ef8a15320b>