DIGITAL OPERATIONAL RESILIENCE ACT ('DORA')

THIRD-PARTY RISK ASSOCIATION

VIRTUAL CONFERENCE

SEPTEMBER 2023

KIM LABARBIERA

JAMES STEEL

KIM LABARBIERA, DIRECTOR AND COUNSEL, THIRD-PARTY RISK

OVERVIEW

- HIGH LEVEL: DORA REQUIREMENTS AND MANAGEMENT OF THIRD-PARTY RISKS
- SUPERVISION OF CRITICAL THIRD PARTIES
- COMMON CHALLENGES WITH DORA
- COMMON SOLUTIONS AND WRAP UP

HIGH LEVEL: DORA REQUIREMENTS AND MANAGEMENT OF THIRD-PARTY RISKS

DORA is a European Union regulation on digital operational resilience for financial institutions (FI)s. DORA is aimed at systemic and concentration risks caused by the sector's dependence on Information and Communication Technology (ICT) third-party providers (TPPs).

After DORA: FI's risk manage:

1. protection,

2. detection,

3. containment,

4. recovery and repair capabilities

against ICT-related incidents.

DORA refers directly to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring.

Before DORA: FI's risk managed:

1. the operational risk category by balancing it with the allocation of capital funds.

The European Council formally adopted DORA on November 28, 2022. Financial institutions across the EU will now need to ensure that they are compliant with these regulations by Q4 2024,

WHAT ENTITIES ARE IMPACTED?

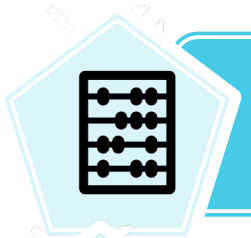
FINANCIAL ENTITIES

- credit institutions,
- payment institutions,
- e-money institutions,
- investment firms,
- crypto-asset service providers,
- issuers of crypto-assets,
- issuers of asset-referenced tokens and of
- significant asset-referenced tokens,
- central securities depositories,
- central counterparties,
- trading venues,
- trade repositories,
- managers of alternative investment funds,
- management companies,
- data reporting service providers,
- insurance and reinsurance undertaking: insurance intermediaries, reinsurance and ancillary insurance intermediaries,
- institutions for occupational retirement pensions,
- credit rating agencies,
- statutory auditors and audit firms,
- administrators of critical benchmarks,
- crowdfunding service providers,
- securitization repositories.

DORA: MANAGEMENT OF THIRD-PARTY RISK

- Management of ICT third party risk - principle of **proportionality**, taking into account:
  - **nature**, **scale**, **complexity** and **importance**
  - **risks**, taking into account **criticality** or **importance** and **potential impact**
- Minimum requirements:
  - some regardless of criticality
  - others critical or important only
- Consider 'flow-down' of other obligations
- Firms must consider ICT concentration risk (including through subcontracting and to providers in third countries)
- Firms and ICT third-party service providers to consider use of standard contractual clauses developed by public authorities for specific services

CRITICAL THIRD PARTY (CTP): SUPERVISION



Define third parties as Critical using objective information such as the systemic impact to the FI.

1. Oversight plans: done yearly
2. Assessment

1. protection,
2. detection,
3. containment,
4. recovery and repair capabilities against ICT-related incidents.

CTPs established in a 3rd country must establish an EU subsidiary (within 12 months of designation)

Lead Overseer will impute fees that address required expenditure

Fines: (daily up to 1% av. daily "worldwide turnover", cap at 6 months)

Does Not Include:
1. Firm OpCos, 2. firms providing ICT services to other FIs, 3. nexus within single member state

DORA: COMMON CHALLENGES

- No clear and consistent definitions of operational resilience
- No effective coordination and communication
- Not At All Prescriptive

DORA: SOLUTIONS

Organizations should seek to achieve a highly customized, flexible and resilient recovery solution by (among other steps):

1. Solidifying their standard disaster recovery plan,
2. Creating backup solutions and an isolated recovery environment in a Cloud based environment.
3. Creating an isolated recovery environment which can provide additional options for recovery, customization, security, integration and compliance.

DORA: WRAP UP

Questions?

THANK YOU