responsiv
simple · effective · distinctive

DISTRIBUTED VS CONCENTRATED THIRD PARTY RISK

OVERVIEW

The Digital Operational Resilience Act (DORA) aims to address digital operational risk within financial services.

Part of this digital operational risk includes dependencies on third-party providers for cloud, skills, data storage, and more. It is important to remember that data stored in third-party cloud platforms and data centres, still falls under the financial entity's responsibility.

It is important to understand how your organisation has set up its third-party model to assess the potential risk in the event of them having an incident or going out of business.

DISTRIBUTED vs CONCENTRATED

Distributed Third-Party Risk

Having a distributed third-party model has its benefits, such as access to a variety of capabilities, but it also poses risks.

This includes the number of skills required to maintain and manage, the need to manage and control all the applications, the number of vendors requiring access, and the risk of unreliable or underdeveloped vendor relationships.

Whilst the risk of losing one vendor that takes out a large number of operational systems is reduced using a distributed model, other costly risks arise to threaten resilience and service provision.

Concentrated Third-Party Risk

Putting all your eggs in one basket can also threaten digital operational resilience.

Whilst you can limit the range of skills required, nurture vendor relationships, and more easily manage installations, in the case of these key vendors becoming unavailable, you risk losing a larger number of systems and services.

This can impact operational compliance, as businesses can be cut off from their data, processes, systems, and capabilities.

Managing Third-Party Risk

Understanding who your third-party vendors are, what services they provide, their risk in the market and as a critical provider (think hyper-scale cloud providers), and the impacts of losing them is critical to DORA compliance.

It is not the responsibility of the third-party to plan and mitigate these risks, so ensuring you have updated contracts, policies, exit strategies and failsafes in the case of an incident is crucial for DORA preparations.

AT A GLANCE

CHALLENGES

- Third-party reliance
- Regulatory non-compliance (DORA)
- Unclear vendor distribution
- Access to critical data and systems

BENEFITS

- DORA compliance
- Digital resilience
- Improved vendor insight
- Risk mitigation
- Clear exit strategies

HOW CAN RESPONSIV HELP?

Responsiv has a wealth of knowledge around third-party risk and DORA compliance.

Read more on DORA below:

- Preparing for DORA
- DORA: The Human Aspect of Digital Resilience
- Navigating Digital Operational Resilience Ensuring Trustworthy Data Access

CONTACT US

sales@responsiv.co.uk