responsiv
simple · effective · distinctive

DORA: THIRD PARTY RISK

OVERVIEW

The Digital Operational Resilience Act (DORA) seeks to strengthen the Financial Services by improving their operational resilience. It aims for convergence of resilience and security practices to do so.

DORA extends to third-party ICT providers that are not in the Financial Services market, such as cloud providers.

THIRD-PARTY RISK

This encapsulates the operational risks that originate from an external party.

Third-party risks tend to be invisible until they occur, and can threaten an organisation in various ways such as providing an attack vector, or removing the provision of a critical service.

Immediate, strategic, regulatory, and/or systematic failure can arise from an affected third-party. Incidents can cause the inability to operate, add unexpected additional costs, and/or cause loss of control or oversight.

Financial services should ensure contracts between third parties include streaming metrics from the service and the right to inspect, consider all likely threats that can be mitigated, and provide tangible exit strategies and failsafes to ensure the continuation of services and data access.

Organisations should understand their reliance on third parties, and clearly define the responsibilities of each party. It is important for firms to know if third parties will prioritise business recovery in the event of an incident, and consider how they will engage and escalate during an outage.

Threat and Error Management

Threats are external events with the potential to disrupt operational integrity. This includes events originating in third parties.

Threat response determines the possibility of errors; mistakes made by people responding to threats can make a situation worse.

It is important to:

- Identify critical threats, assess the long or short term impacts, and identify the systematic threats across multiple systems (cloud hosting).
- Prioritise based on the threats, plan response to each one, and document potential errors in the response.
- Respond to threats by establishing processes and working practices to minimise risk, instigate regular testing, and engage third parties to establish a joint response.

AT A GLANCE

Third parties are a critical factor for consideration when analysing ICT risk, as many services such as cloud, sit with these external providers.

Financial organisations maintain responsibility for data security and integrity, despite it being hosted and stored in third-party storage environments.

Organisations need to plan for the unavailability of these environments and limited or no access to their data.

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

Discover your DORA maturity with Responsiv. Get in touch to find out more.

sales@responsiv.co.uk