responsiv
simple · effective · distinctive

DORA: ENSURING TRUSTWORTHY DATA ACCESS

OVERVIEW

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

Third-party risk relates to supplier, vendor, and systematic risk. Third parties also pose a threat when they have legitimate access to data and systems to provide their service.

Without independent oversight of data access, organisations do not know where, who, when, or how data is being accessed or used, and cannot easily identify and report on breaches and incidents in line with DORA regulation.

ENSURING TRUSTWORTHY DATA ACCESS

To ensure trustworthy data access, financial institutions should consider their independent oversight and control capabilities, including the monitoring of privileged users.

Privileged users, knowingly or not, are the largest attack vector for data breaches. This includes any third parties who have privileged access to internal environments.

Stolen or compromised credentials, and malicious insiders have the highest mean time to identify and contain a data breach. Compromised credentials takes on average 328 days and malicious insiders 308 days to identify and contain.

Mitigating Privileged User Risk

As a first step, it is important for organisations to understand and define how their data should be accessed and used so they can identify any anomalous activity. These definitions should be clearly documented to ensure consistency.

Organisations can utilise independent (non-native) security tools to automatically detect and alert to these abnormal events to reduce the time to containment. Monitoring all users and data means you are not blind to threats originating from you deem 'privileged'.

Some security tools, such as IBM Guardium, provide the ability to audit all aspects of your data environment, meaning the data is available to create reports following any incident, ensuring you meet this DORA requirement.

Assigning privileged access and ensuring it is continuously maintained is also important to reduce the risks. Implementing an automated process or using a singular identity store can streamline this process to improve the consistency of user access across the organisation in line with the defined requirements.

AT A GLANCE

CHALLENGES

- Business risk
- Regulatory compliance
- Digital resilience
- Third-party data access
- Data security and breaches
- Lack of insight into privileged users

BENEFITS

- DORA compliance
- Digital resilience
- Risk mitigation
- Monitored privileged users
- Incident reporting

HOW CAN RESPONSIV HELP?

Responsiv has a wealth of knowledge around third-party risk and secure data access and monitoring for 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
- Secure and Audit Data with IBM Guardium

CONTACT US

sales@responsiv.co.uk