responsiv
simple · effective · distinctive

PREPARING FOR DORA: PEOPLE RISK

OVERVIEW

The Digital Operational Resilience Act (DORA) seeks to strengthen the Financial Services by improving their operational resilience.

The regulation focuses on the protection, detection, containment, recovery, and repair capabilities against ICT related incidents. DORA explicitly refers to ICT risk and sets rules on ICT risk management, incident reporting, operational resilience testing and ICT third party risk monitoring.

PEOPLE RISK

People risk is concerned with the loss of operational integrity due to the loss of one or more people, and can thus impact DORA compliance.

People may be an unaccounted dependency for their knowledge of the business and its processes and systems; they can be internal or external (third-party). Their absence means a service or system is inoperable or inefficient.

Capacity and Training Risk

People risk also extends to capacity and training or competence. People can be lost because they leave the business or move role, are on holiday or sick, or are overstretched in their workload.

Loss of capacity may reduce departmental throughput but not be catastrophic. Recruiting people to replace critical functions or capacity can introduce additional risk, especially where training is required.

People Cyber Risk

Privileged users are a threat. Stolen or compromised credentials lead to 20% of cyber incidents and on average costs $4.6m to resolve. Malicious insider attacks are less frequent at 5% but more expensive at $4.9m.

Creating policies as part of the ICT Management Frameworks will simplify permission rules and set an expectation for how data can be accessed and used.

Process Automation is the Answer

Utilising process automation to remove reliance on individuals mitigates the risk of staff loss and low capacity. Processes can be fully automated or provide guided prompts for people who have limited training.

Automation can also limit human interaction and access to data and systems to mitigate the risks associated with privileged users, as bots are less likely to lose credentials, be malicious, or respond to phishing attacks.

Monitoring privileged users and how they access and use data is important to be able to identify and report abnormal activity or incidents in line with regulation.

AT A GLANCE

CHALLENGES

- Business and people risk
- Regulatory non-compliance
- Staff loss and low capacity
- Cyber attacks via privileged users

AUTOMATION

- DORA compliance
- Digital resilience
- Risk mitigation
- Knowledge consolidation
- Empower untrained staff
- Monitor privileged users
- Limit human intervention

HOW CAN RESPONSIV HELP?

Responsiv has a wealth of experience mitigating human risk with process automation and other technology solutions. We can map, develop, and support your automation solution 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

CONTACT US

sales@responsiv.co.uk