readyworks

Digital Operational Resilience Act (DORA) Compliance

THE PROBLEM: IT and operational complexity make it difficult for financial services institutions to identify and mitigate risks to avoid service disruption and maintain operational resiliency.

The Digital Operational Resilience Act (DORA) aims to ensure the European financial sector maintains operational resiliency through severe business disruption caused by cyberattacks. DORA lays out a unified approach around risk management for organizations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them. It harmonizes the way that risk is managed and formalizes communications channels to give authorities more information to act rapidly and tackle cybercrime at the source.

To achieve compliance with DORA policies, you first need to identify security risks, which requires a comprehensive inventory of all IT hardware and software assets, who is using them, where they are located, and all the interdependencies among systems. You'll also need to understand security policies and risks associated with ICT providers, implement resilience testing, maintain up-to-date incident reports, and rapidly share information regarding threats with other financial services companies. Trying to achieve all of this is near impossible with manual processes.

THE SOLUTION: READYWORKS

ReadyWorks, a digital platform conductor, integrates data from all your IT and business systems to identify and help mitigate security risks including end-of-life systems, missing assets, and systems requiring patches. ReadyWorks uses this information to orchestrate workflows to minimize the risk of cybersecurity attacks. It also orchestrates workflows for enforcing security policies and resilience testing, maintains audit trails including those required for incident reporting, and automates email communications to share information regarding security threats.

BUSINESS IMPACT:

- **Operational Resiliency:** Identify security vulnerabilities and automate workflows to mitigate threats and maintain business continuity. Leverage automation to quickly implement disaster recovery plans in the event of severe business disruption.
- **Improved compliance:** Ensure conformance with DORA guidelines/key performance indicators, and internal policies.
- **Unified Risk Management:** Automate communications to rapidly share information regarding threats with other financial services companies and government agencies.

WITH READYWORKS:

- Implement a risk management strategy that incorporates a holistic automated IT asset management (ITAM) program.
- Merge data from all sources to gain a real-time view of hardware, where it is located, who is using it, associated applications, OS and software versions, configuration settings, and how data is managed.
- Quickly identify vulnerable devices that require a security patch. Categorize risk levels and identify which patches need to take priority and receive immediate attention.
- Identify EOL systems and automate migration, decommissioning, and disposal workflows.
- Automate workflows based on pre-defined dates or events to comply with resilience testing requirements.
- Automate workflows to communicate and enforce security policies.
- Confidently respond to security and compliance audits with highly accurate, validated, asset data.
- Document interactions with third-party ICT providers to maintain compliance with regulations.

WHAT'S INCLUDED:

- Bi-directional connectors to collect asset information from data-sources including, CMDBs, global policy systems, configuration platforms, identity management systems, ITSM tools, and security alert systems. (10 connectors included in standard subscription.)
- Outbound orchestration to update source systems of record.
- Automated workflows for patch management and migration of EOL systems.
- Automated workflows to notify stakeholders of cybersecurity threat scenario.
- Automated workflows for escalations on security violations.
- Customizable communication templates.
- Full suite of asset inventory and audit response reports.
- Configurable dashboards and reporting aligned with DORA reporting requirements including interactions with third-party ICT providers.
- Guided implementation followed by ongoing support and training.

Request a demo today.

GO TO READYWORKS.COM/DEMO