FILECLOUD

www.filecloud.com

Enhance Your Digital Operational Resilience Act (DORA) Readiness with FileCloud

The EU Digital Operational Resilience Act (DORA) was enacted by the EU in early 2023. Its purpose is to **harmonize measures for achieving digital resilience** in the financial sector throughout the Single Market.

Financial institutions and their third-party ICT providers have until **January 2025** to achieve full compliance with the regulation.

Each individual EU member state is responsible for legislating for DORA and for ensuring competent authorities at national level oversee compliance.

The EU-level DORA supervisory authorities, who will devise the technical standards, are:

- European Insurance and Occupational Pensions Authority (EIOPA)
- European Banking Authority (EBA)
- European Securities and Markets Authority (ESMA)

The Regulation covers all ICT third-party service providers, whether located within or outside the single market, including those providing financial entities with:

- Cloud Services
- Data Analytics Services
- Data Center Services
- Software

DORA Pillars

Pillar 1 ICT Risk Management	Senior management of financial entities must take ultimate responsibility for ICT risk management.
Pillar 2 ICT Incident Classification and Reporting	Under DORA, the systems for classifying and reporting ICT incidents will be harmonized across EU financial entities. Major incidents must be reported to competent authorities.
Pillar 3 Digital Operational Resilience Testing	Rigorous testing of ICT systems must be conducted regularly under DORA, using methodologies validated by the European Supervisory Authorities. System dependencies with third-party ICT service providers and other financial institutions must be encompassed in the tests. Financial institutions need to ensure they are ready for independent audits of any tests conducted and have detailed reports and logs at hand.
Pillar 4 ICT Third-Party Risk Management	Concentration risk must be addressed to prevent dominant third-party ICT providers creating instability across the financial system. Plans must be put in place by financial entities and third-party ICT providers for mitigation of disruptions.
Pillar 5 Digital Operational Resilience Testing	The DORA framework requires that structures be put in place to facilitate information-sharing about threats, vulnerabilities, and incidents among all stakeholders. Privacy, data protection, trade secrets, and competition law should be respected.

How Can FileCloud Help?

Choosing a secure platform for a standard function such as file collaboration and sharing should be a given for any digital operational resilience strategy. While no single piece of software that can guarantee DORA readiness, FileCloud's enterprise file-sharing and sync solution has many features that can contribute.

Information Sharing about ICT Threats and Disruptions

Business Continuity & Disaster Recovery Capabilities

FileCloud has multiple features designed to facilitate information exchange, as well as protect your business and its data assets during cyber-attacks and other disruptions:

- Granular file and folder permissions and expiration dates.
- Remote file access from any device without a VPN.
- Data Leak Prevention (DLP) rules that limit access and login from specific IPs, subnets, or countries.
- Automatic data classification, allowing blocking of shares and downloads.
- Digital Rights Management support to allow secure access to files, and the ability to revoke permission at any time after sharing.
- ICAP integration for antivirus scanning of each incoming file to detect malicious content.
- Zero Trust File Sharing^{SM} to ensure that even if your system is compromised, malicious actors cannot access the contents of a Zero Trust file, as the decryption key is not stored in the FileCloud system.
- Data encryption at rest and in transit, and endpoint backup and versioning.
- Comprehensive ransomware protection via a heuristic content scanning engine.
- Remote wiping and blocking of devices in cases of loss, theft, or cyber threat.
- Customized logos, colors, and domain names, making it easier to spot malicious requests.

Robust Analytics & Reports for Information-Gathering About Threats and Disruptions

DORA recommends sharing intelligence and best practices on ICT-related threats, vulnerabilities, and incidents, including national cybersecurity authorities and ICT incident response teams. Organizations covered by DORA must also be ready for audit at any time.

FileCloud's robust analytics and reports can help with these requirements, with features such as:

- An Admin dashboard to monitor abnormal user activity by geo-IP, storage, and file type distribution. Detection of unusual patterns is automated.
- Automation of compliance with privacy regulations through metadata management, file retention policies, and granular access permissions.
- Content classification and version control.
- Generation of reports on compliance violations to quickly address problems.
- Event logs for governance purposes, allowing for quick and easy reporting.
- Detailed audit reports to allow administrators to monitor user activities at a granular level.
- SIEM integration that enables the sending of logs in LEEF/CEF format to tools such as Splunk for analysis.
- User Locks Reports and User Shares Reports, which can be easily generated to show details of locked and shared files.

> “FileCloud is highly secured solution for data storage, sharing and syncing with number of users globally. It is easy to operate by beginners as its interface is so simple and smooth. "
>
> **– Process Engineer**

Gartner peerinsights customers' choice 2018 ™

Gartner peerinsights customers' choice 2019

Gartner peerinsights customers' choice 2020

Gartner peerinsights customers' choice 2021

Gartner Peer Insights Customers' Choice 2022 ™

FileCloud has received the Gartner Peer Insights Customers' Choice Distinction for the fifth consecutive time!