

Digital Operational Resilience Act & FileCloud

white paper

EU Financial institutions and their third-party Information and Communication Technology (ICT) service providers have until the end of 2024 to achieve full compliance with the Digital Operational Resilience Act (DORA). Here we explore what DORA implementation entails and the built-in FileCloud features that can help enhance DORA readiness.

Preparing for the EU Digital Operational Resilience Act with FileCloud

The new EU Digital Operational Resilience Act was enacted by the EU in early 2023. Financial institutions and their third-party ICT providers have two years to achieve full compliance with the regulation. DORA provisions include stringent requirements aimed at harmonizing digital operational resilience throughout the single market and avoiding competition distortion.

Here we examine the central provisions of DORA, including its five main pillars. We also describe some features within FileCloud's hyper-secure file-sharing and sync solution that can greatly enhance the ability of financial entities to comply with DORA.



DORA sets stringent requirements for ICT security, including measures to prevent unauthorized access, detect and respond to cyber threats, and protect sensitive data.



Backdrop to DORA

In recent years, certain vital sectors that were traditionally paper based, even in the face of widespread digitization, have become dependent on digital technologies to operate. These include health, transportation, energy, and of course the financial sector.

As digital transformation progressively permeates almost all sectors, saturating previously mundane aspects of everyday life through the rise of the Internet of Things (IoT), cybercriminals are becoming incrementally more polished and audacious.

In her State of the European Union address at the European Parliament in Strasbourg, France, 15 September 2021, European Commission President Ursula von der Leyen made it clear that digital resilience was a major EU priority, stating, "If everything is connected, everything can be hacked."

The sudden requirement for a pandemic response in 2020 also highlighted certain areas of concern in the financial sector specifically. These include the pressing need to:

- Achieve full understanding of the ability of third-party technology providers to remain resilient in challenging environments.
- Safeguard confidential and sensitive data in the face of remote working environments.
- Identify and proactively address risks across the supply chain, including offshore hubs.
- Implement workable business continuity plans and/or exit and transfer plans in the event of third-party provider outages.

Driven by these and other considerations, at a meeting of the Special European Council in October 2020, EU leaders discussed possibilities for accelerating digital transformation throughout the single market. They called for multiple measures to enhance protection against cyber threats, including quantum encryption to secure communications and enhanced data access for law enforcement and judicial operations.

Following on from this, the EU Commission and the European External Action Service (EEAS) unveiled a new [EU Cybersecurity Strategy](#) in December 2020. The stated aims of this strategy were to:

- **Fortify resilience** against cyber threats across the EU.
- **Provide a concrete framework** for the deployment of regulatory, investment, and policy instruments.

The EU Council adopted conclusions from this strategy in March 2021, with the observation that enhanced cybersecurity is essential for a resilient Europe.



Rising Incidences of Cybercrime

This broad recognition across EU institutions of the need for stronger digital resilience is indicative of the increasing sophistication of cybercriminals' methodologies. If there is an attack vector that represents potential profitability, cybercriminals will invariably find a way to exploit it. This is usually at the expense of thousands of customers or the proper functioning of vital institutions, such as healthcare and financial institutions.

Despite often having technical know-how, cybercriminals are ethically the same as most organized crime practitioners, i.e., unbound by any meaningful ethical code. Through the deployment of malware, they engage in activities such as money laundering, child exploitation, the creation of counterfeit passports and credit cards, and the illegal sale of weapons.

The exponential rise in cybercrime was not only exacerbated by the remote working arrangements suddenly required by the pandemic, but also, simultaneously, by several sources of geopolitical upheaval. In addition, vulnerabilities are common in devices we use for banking and other private transactions daily:

- **79% of Windows systems** have at least one open vulnerability with known exploits.
- **63% of mobile apps** contain an average of 39 known vulnerabilities in open-source components.

The overall recognition of the need to identify digital dependencies within and between sectors and create a proactive framework for security and resilience throughout the EU has resulted in the creation and adoption of several legal instruments. In relation to the financial services sector, the main such regulation is the Digital Operational Resilience Act (DORA).

The Single Rulebook

The Single Rulebook was established as a part of the response to the 2008 financial crisis to govern significant aspects of the financial risks associated with financial services. Considering the cross-border nature of ICT risk, the Single Rulebook has a limited effect.

In 2020, the European Systemic Risk Board concluded that localized cyber-incidents had the potential to spread to all EU financial entities, in turn creating a domino effect on the entire global financial system. Although the Single Rulebook and supervisory system were harmonized throughout the EU, ICT security and operational resilience were not sufficiently standardized. Given the pivotal role of digital operational resilience in ensuring the integrity and stability of the market, it is now regarded as equal in importance to the maintenance of common prudential standards.

Regulators were aware that there remained a lack of coordination in national initiatives, resulting in inconsistencies and a duplication of requirements. Additionally, administrative and compliance costs were high, particularly for cross-border financial entities. As a result, ICT risks often remained undetected and therefore unaddressed.



Uneven Regulatory Landscape

This scenario created fragmentation within what purports to be a single market and threatened the overall integrity and stability of the EU financial system. Increased harmonization was required, particularly in relation to digital operational resilience testing and third-party risk management and monitoring.

Approaches to the sharing of cyber threat information have also been inconsistent throughout the member states. The EU recognized that enhanced uniformity would provide financial entities with the freedom to maintain a cross-border market presence and ensure competition remains fair.

Additionally, financial institutions increasingly embraced hybrid ICT infrastructures in many financial institutions, with many separate workstreams and bespoke processes. This can result in problems like slow manual failovers. The need to consolidate all provisions around ICT risk management that were covered in other EU regulations was recognized.

Addressing the Requirement for Consolidation

Fragmented legislation covered risks around credit, markets, counterparty credit, liquidity, and market conduct, but did not deal with all aspects of operational resilience. DORA seeks to resolve inconsistencies between previous regulations and standardize rules on risk management, testing, third-party risk monitoring, and reporting. Under DORA, all financial entities, with some exceptions for microenterprises, must have measures in place to ensure they can withstand, respond to, and recover from all ICT-related disruptions and threats.

Supervisory Authorities

Each individual EU member state is responsible for legislating for DORA. The relevant supervisory authorities are:

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

These competent authorities are responsible for devising technical standards around DORA for all financial services entities. Compliance will be overseen by relevant competent authorities at member state level.

A reduction in the complexity and volume of regulations means compliance will be more cost-effective. Competitive distortions will be reduced, if not eliminated. The overall goal of DORA is to guarantee a homogenous application of ICT risk management across the entire EU financial sector.





DORA Framework Pillars

In December 2022, the full text of the Digital Operational Resilience Act (DORA) was published in the Official Journal of the EU as Regulation (EU) 2022/2554. The Regulation came into force 20 days after publication and will fully apply from January 2025.

DORA sets out an EU framework of common standards for the protection, detection, containment, recovery, and repair in relation to ICT-related incidents affecting EU-based financial institutions and their ICT third-party service providers. It lays down rules for risk management, incident reporting, operational resilience testing, intelligence sharing, and ICT third-party risk monitoring.

The Regulation outlines requirements that apply to all financial entities in relation to network and ICT systems supporting financial entities around the following areas, which have been identified by leading financial institutions as the five pillars of DORA:

1. ICT Risk Management
2. ICT Incident Classification and Reporting
3. Digital Operational Resilience Testing
4. ICT Third-party Risk Management
5. Information Sharing



Pillar 1: ICT Risk Management

Under DORA, an ICT risk management function must be implemented in all financial entities, with a broad focus across all critical business functions. Ultimate responsibility for this function lies with the senior executives of the financial entity.

New Governance Requirements

DORA represents a shift in the governance requirements of the ICT function. Management must organize an assessment of operational resilience, ensuring all the necessary resources and budgets are made available. The scope of the assessment should be broad, including physical security and setting up a robust testing regime for operational resilience.

Management bodies should maintain an ongoing awareness of the arrangements arrived at with third-party service providers, as well as their potential impact. Unless they are microenterprises, senior management must also establish a role to monitor arrangements with third-party providers or designate a member of senior management as responsible for overseeing risk exposure.

Management must also consistently maintain a good grasp of ICT incidents and their impact, the response and recovery, and corrective measures.



In DORA, a microenterprise is defined as employing less than 10 people, with an annual turnover of less than €2 million.



Pillar 1: ICT Risk Management (continued...)

Asset Management Requirements

Several banks had difficulties identifying the location of their Log4j vulnerabilities, due to the lack of an inventory of ICT resources within their organizations. In response to this and other similar occurrences, DORA requires that each financial entity perform rigorous asset management, including producing an inventory of all ICT system accounts, hardware and other physical equipment, configurations, and dependencies.

Further examples of identification activities required under DORA include:

- Undertaking an annual review of all information assets.
- Identifying and assessing cyber threats and vulnerabilities continuously and reviewing risk scenarios at least annually.
- Documenting all processes that rely on ICT third-party providers and identifying all dependencies.
- Performing risk assessments in relation to any major change in network or ICT infrastructures.
- Conducting an ICT risk assessment on all legacy ICT systems at least annually.
- Providing documentation on risks as required to competent authorities.

Protection and Prevention Requirements

Another area of risk management emphasized by DORA is protection and prevention. Requirements of financial entities in this area include:

- Devising an information security policy that defines rules to protect the confidentiality, integrity, and availability of ICT resources and data.
- Designing and implementing ICT security strategies and tools to ensure resilience and continuity of ICT systems, as well as maintaining high standards of confidentiality and data integrity.
- Establishing a risk-based approach to network and infrastructure management, as well as implementing automated mechanisms to isolate information assets in the event of a cyber-attack.
- Creating strategies, protocols, procedures, and controls for robust authentication mechanisms, ICT change management, patches, and updates.



Pillar 2: ICT Incident Classification and Reporting

DORA sets out requirements for the harmonization of systems for triaging of incidents that have an adverse impact on the financial entity, its customers, or the financial system. It requires reporting of substantial ICT incidents, as well as voluntary notification of major cyber threats to the competent authorities. Competent authorities must also be informed of sizable incidents related to operational or security payments.

Rules are established in DORA requiring cooperation between different competent authorities, as well as supervision and enforcement in relation to all areas covered in the regulation. Each financial entity is required to have a playbook or manual outlining how incidents will be handled.

Further requirements in relation to business continuity in the face of incidents include:

- Demonstrating the ability to implement ICT strategies through appropriate and documented arrangements, procedures, and mechanisms.
- Recording of all incidents, and in the event, immediate activation of containment measures.
- Providing preliminary estimations of impacts, damage, and losses.
- Keeping records of activities before and during disruptions.
- Setting out communication and crisis management plans and testing them.
- Implementing an associated ICT Disaster Recovery Plan, subject to independent audit reviews.
- Creating a crisis management function for scenarios in which the ICT Business Continuity Policy or ICT Disaster Recovery Plan are activated. Clear procedures must be in place to manage internal and external crisis communications.
- Reporting all costs and losses related to incidents to competent authorities.



Pillar 3: Digital Operational Resilience Testing

DORA requires financial entities to conduct regular, rigorous testing of all ICT systems to help guarantee resilience and business continuity in the face of disruptions. The testing should be based on methodologies and scenarios developed by the European Supervisory Authorities. It must also encompass dependencies with other financial entities and third-party service providers.

The legislation specifies various testing requirements, including:

- Implementing, maintaining, and testing appropriate ICT business continuity plans, most importantly in relation to critical or important functions outsourced to ICT third-party service providers.
- Testing plans for cyber-attack scenarios, and switchovers between the primary infrastructure and the redundant capacity, backups, and redundant facilities.
- Testing of the ICT Business Continuity policy and ICT Disaster Recovery plan at least annually.
- Planning and testing crisis communications plans.
- Conducting a proportional risk-based digital operational resilience program annually, and threat-led penetration testing every three years.



Audit Readiness

Competent authorities have powers to conduct independent audits of any testing that is conducted. Financial entities must have the ability to provide detailed reports and logs of test results to these authorities.

For change management purposes, financial entities must also be able prove that recovery plans are relevant following changes to their infrastructures. This means it is necessary to maintain a comprehensive runbook library.



Pillar 4: ICT Third-Party Risk Management

A crucial element of DORA is its application to critical third parties that provide ICT services to financial entities, including cloud providers, data centers, and software vendors.

The DORA framework incorporates a notification system for financial entities that wish to outsource critical ICT functions, as well as granting monitoring and auditing powers by the European Supervisory Authorities and the European Central Bank.

Asset Management Requirements

Third-party ICT service providers to financial entities must have measures in place under DORA to ensure resilience in the face of ICT disruptions and threats.

This provision addresses a combination of factors that have made the financial services environment more complicated in recent years.

Outsourcing to third parties has become increasingly normalized.

However, the ever-intensifying lack of homogeneity of ICT systems means that financial institutions no longer have full control over the application stack and underlying infrastructures.



While ICT outsourcing creates certain business efficiencies, it has also resulted in a web of dependencies within the financial system that could potentially cause a harmful and widespread system collapse. Given that the average cost per hour of a critical application failure is \$500K to \$1M, regulation to create uniform resilience measures in relation to third-party providers has become essential.



Pillar 4: ICT Third-Party Risk Management (continued...)

Concentration Risk

Third-party ICT providers are often in competition with one another, making switching services in the event of an outage difficult, particularly towards the top of the technology stack. If a dominant third-party provider is serving several major financial institutions, and has a major disruption or outage, this has the potential to become a single point of failure that ultimately threatens the financial stability of the entire single market.

Concentration risk depends heavily on the criticality of the services provided and plans in place for mitigation on the part of the financial entities and third-party providers.

To address concentration risk, financial entities must adhere to certain enhanced requirements in relation to ICT third-party providers, including:

- Creating and maintaining a standard register of third-party technology providers, including details about services they provide, functions they support, their locations, and details of the contractual arrangements entered into with them.
- Conducting a thorough risk assessment of third-party providers, in line with the criteria of the European third-party risk management framework for financial services. This includes an assessment of dependencies and ICT concentration risk.
- Implementing rigorous measures for ICT third-party risk management. This should be defined, implemented, and monitored by the management of the financial entity.
- Adhering to specified requirements for contractual arrangements between financial entities and ICT third-party service providers. Conducting rigorous due diligence prior to entering into these contracts, as well as terminating contracts under certain specified conditions.
- Ensuring the Lead Overseer can inspect third-party providers, and that those providers located outside the EU establish a subsidiary within the EU. Facilities outside the EU can still be used for service provision. However, inspections can be conducted, and penalties imposed, in countries outside the EU.
- Documenting measures in place in the event of a third-party provider suffering an outage. Financial entities are responsible under DORA for service recovery.



Pillar 5: Information Sharing

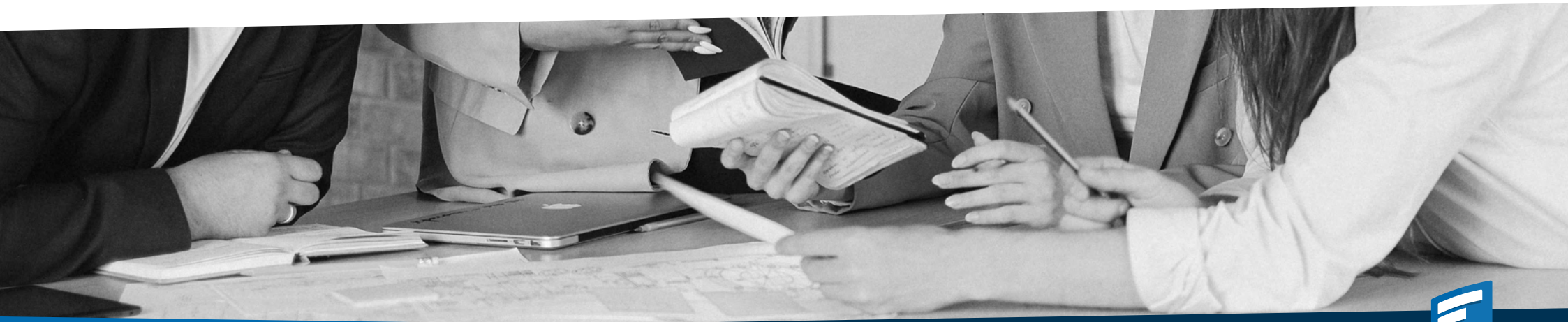
DORA facilitates the sharing of intelligence and best practices on ICT-related threats, vulnerabilities, and incidents among financial entities, competent authorities, and other relevant stakeholders. This intelligence sharing should include national cybersecurity authorities and ICT incident response teams.

Information sharing should be done through dedicated platforms or networks established by European Supervisory Authorities and European Central Bank. It must be done with respect for privacy and data protection regulations, trade secrets, and competition law.















DORA has provisions requiring EU-wide standardized reporting

for serious incidents to ensure that authorities have an accurate overview of the ICT incidents affecting the single market.







DORA Scope

DORA has a broad scope, covering the following types of financial entities:

	Central securities depository Central counterparties		Insurance and reinsurance undertakings (partly)		Insurance and reinsurance intermediaries & ancillary insurance intermediaries		Institutions dealing with occupational retirement pensions
	Administrators of critical benchmarks		Trading venues & trade repositories		Managers of alternative investment funds		Statutory auditors and audit firms
	Crowdfunding service providers		Credit rating agencies (partly)		Management companies		Securitization repositories

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 Center Services	Data Analytics Services	Software



How Can FileCloud Support DORA Compliance?

The following pages describe FileCloud features that can help organizations to achieve compliance with the EU Digital Operational Resilience Act.



Requirement to Ensure Digital Resilience During ICT Threats & Disruptions

Secure File-Sharing & Remote Access

With FileCloud, you can securely share files and folders internally and externally, setting granular permissions and expiration dates. You can also access files remotely from any device without the need for a VPN.

Features that help with DORA compliance include:

- **Data Leak Prevention (DLP)** rules that limit access and login from specific IPs, subnets, or even countries.
- **Automatic data classification** based on the content of documents, allowing blocking of shares and downloads.
- **DRM 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 protect against malicious content.

These features can play a key role in helping financial entities to secure service continuity by facilitating information exchange during ICT disruptions and cyber-attacks.

FileCloud's industry-first **Zero Trust File Sharing** feature also provides fail-safe data protection in the event of system compromise. You can enable this feature by creating Zip files in FileCloud and adding password-protection. The decryption key is not stored within the FileCloud system, so you retain complete control over your data. Even if your system is compromised, malicious actors are unable to open or view the contents of the Zip file.

FileCloud uses encryption at rest and in transit, as well as endpoint backup and versioning, to protect data. A heuristic content scanning engine provides comprehensive ransomware protection.

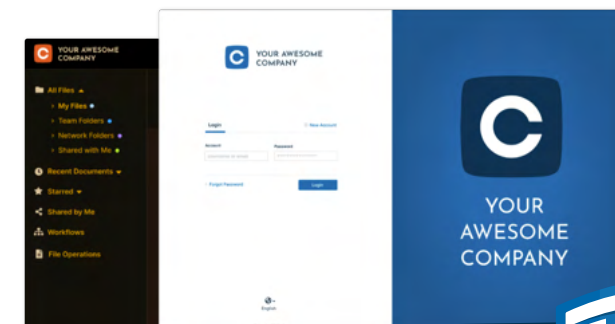
FileCloud admins can remotely wipe or block devices in cases of loss, theft, or cyber threat. These and other FileCloud features help financial entities to ensure data availability and integrity regardless of incidents and disruptions.

Custom Branding and Integration

FileCloud allows financial entities to customize the product to reflect their brand identity. Customized logos, colors, domain names, and email templates can all be easily incorporated into FileCloud. Integration with line-of-business cloud applications is seamless using FileCloud's flexible APIs.

This allows banks and other financial services organizations to retain affinity with their brand among users and leverage their existing infrastructure and tools. It also helps to ensure data security by retaining all files in the same location, eliminating the need for transfer to a third-party file-sharing provider.

You can run URLs under your financial institution's domain with FileCloud, making it easier for staff to spot malicious requests.



Requirement to Share Intelligence about Cyber Threats and Disruptions

DORA outlines requirements for financial entities to share intelligence and best practices on ICT-related threats, vulnerabilities, and incidents with competent authorities and other relevant stakeholders, including national cybersecurity authorities and ICT incident response teams. FileCloud's robust analytics and reports have the ability to help detect patterns and threats.

Analytics & Alerts

You can track data through the FileCloud business intelligence layer, gaining information on usage trends, user access by geography, storage use, and content mix.

Through the Admin dashboard, FileCloud administrators can monitor for abnormal user activity that might indicate a security breach. This comprehensive dashboard displays usage trends, access by geo-IP, storage, and file type distribution.

Unauthorized sharing of sensitive content outside the organization can be quickly spotted. Detection of unusual patterns occurs automatically.

You can plan for greater process efficiencies based on the existing usage patterns, allowing for continuous process improvement.

Further features that provide analytics include:

- Ransomware protection through a heuristic scanning engine.
- 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 via the FileCloud Compliance Center to quickly address problems.
- Event logs for governance purposes, allowing for quick and easy reporting.



Detailed Audit Trails and Reports

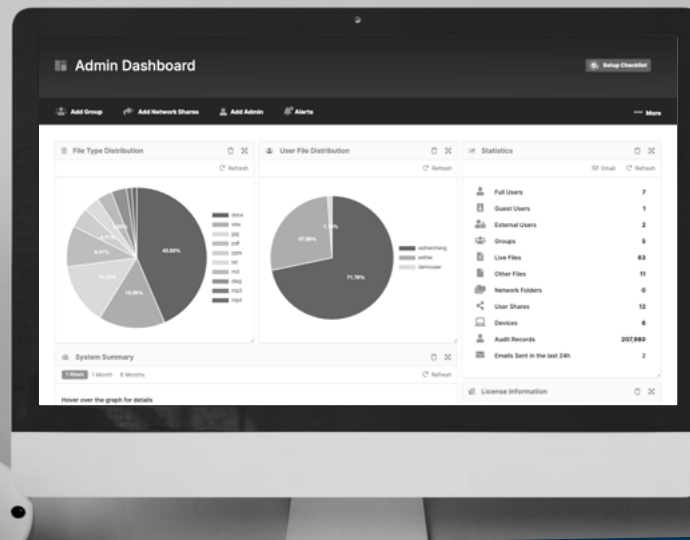
Audit reports allow system administrators to monitor user activities and understand user patterns. The centralized FileCloud Admin dashboard provides a variety of filters to allow administrators to produce customized reports.

All user logins and file activities are monitored, including uploads, downloads, and deletions, and these can be listed in reports if required. Reports can be filtered by date range, username, and text search.

SIEM integration enables the sending of logs in LEEF/CEF format to tools like Splunk for analysis.

Using the Admin dashboard, administrators can easily create a User Locks Report to view a list of locked files. Similarly, they can generate a User Shares Report, which includes information such as username, location, expiration, share type (private or public).

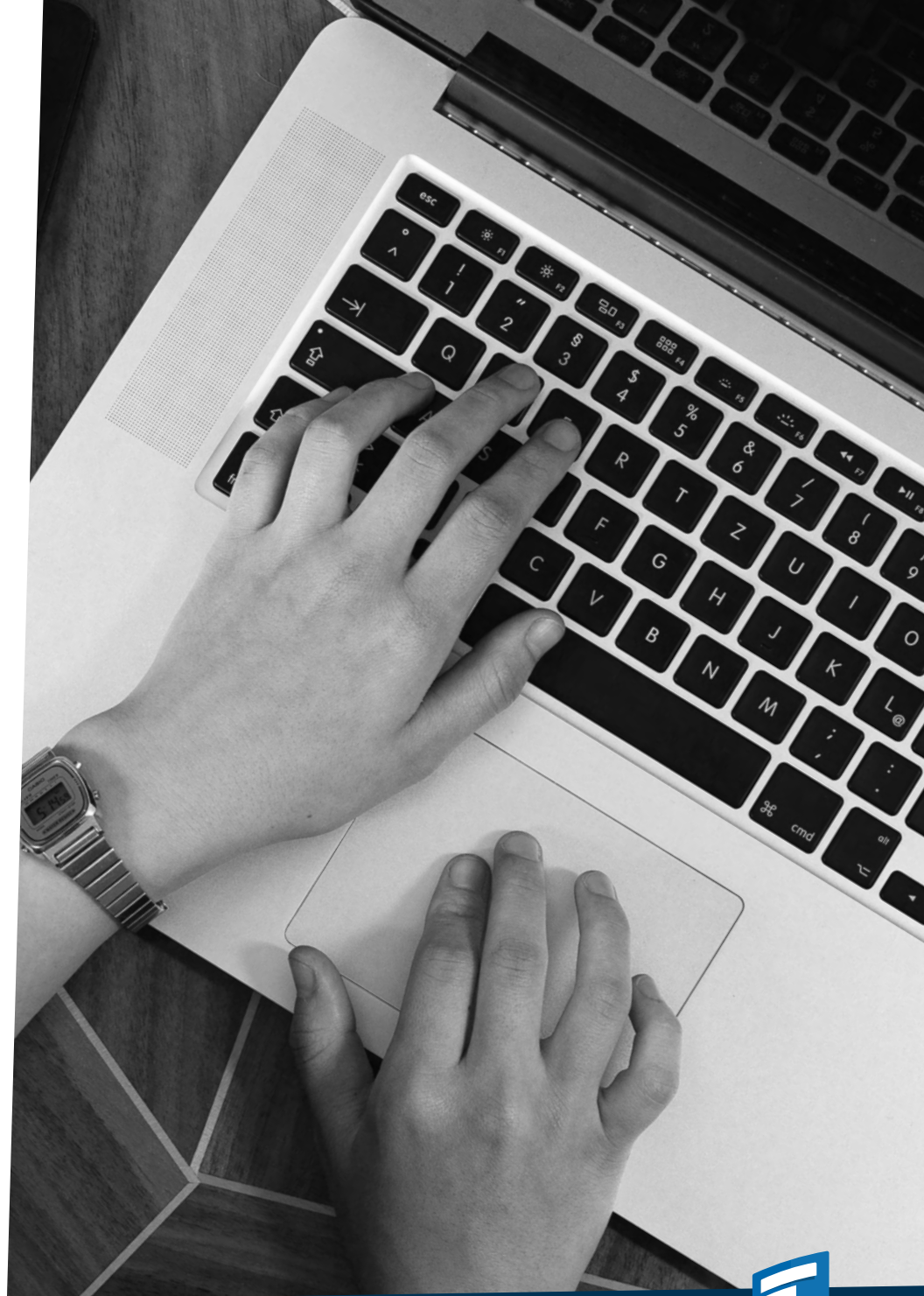
The most recent files and users added are displayed in a quick view, allowing administrators to continuously monitor changes to the user base.



Conclusion: Embracing A New Era in Cybersecurity with FileCloud

As stationary networks become increasingly rare, it has become necessary to shift the security focus to information assets and users. One estimate suggests that only 7% of organizations are completely confident that they know the location of all of their sensitive data in hybrid cloud deployments. Zero Trust is a significant step in the evolution of the cybersecurity mindset that focuses on assets, users, and resources. Many organizations have recognized the need to embrace a Zero Trust approach, focusing on areas such as identity governance, analytics, and continuous adaptive user authentication.

Regulations such as DORA recognize the need to address the move away from the network and toward more complex, cloud-based infrastructures in ensuring digital resilience. FileCloud's security features are constantly fine-tuned to allow organizations to achieve that all-important balancing act between day-to-day operational efficiency and digital resilience. When it comes to file-sharing and collaboration, our capabilities can make a meaningful contribution to accomplishing DORA readiness.



About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.



1M+
USERS



3000+
ENTERPRISES



100+
RESELLERS



90+
COUNTRIES



13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480

Fax: +1 (866) 824-9584

CONTACT US



**US Army Corps
of Engineers**



Deloitte.

Copyright Notice

© 2023 FileCloud. All rights reserved.
No reproduction without written permission.

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.

