

DORA



cybrilliance

Empower Your Business with Cyber Resilience

Digital Operational Resilience Act

The EU Digital Operational Resilience Act (DORA) aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.

DORA entered into force on January 16, 2023 and is set to take effect in January 2025, bringing significant implications for organizations operating within the financial sector. Under DORA's mandate, financial entities and their critical third-party technology service providers must implement stringent ICT system guidelines by January 17, 2025. This initiative aims to establish a universal framework for managing and mitigating ICT risk across the financial landscape.

The regulations are designed to ensure compliance, and penalties for non-compliance can be costly. These penalties can include:

- Financial penalties that amount to the equivalent of one day of trading revenue
- Criminal charges against companies and individuals who do not adhere to DORA

Cybrilliance have identified the following sections from the final text¹ of DORA, indicating existing technology, techniques and policies (TTPs) and highlighting the additional value delivered by the Actifile Data Security Platform.

Actifile fulfills many of the requirements suggested by Gartner for Data Risk Assessment (DRA), Data Security Governance (DSG), Data Breach Response (DBR), Data Discovery and Management (DDM), Data Classification (DC) and other data privacy categories.^{2,3}

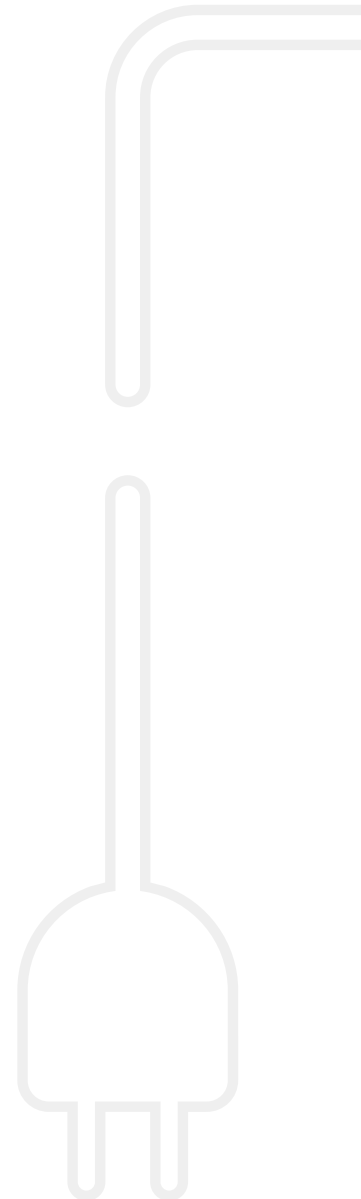
1 - https://www.digital-operational-resilience-act.com/DORA_Articles.html

2 - Hype Cycle for Data Security, 2022, Gartner, Brian Lowans

3 - 2023 Strategic Roadmap for Data Security Platform Adoption, Gartner, Joerg Fritsch, Brian Lowans

Table of content

01	Preamble (51)
02	Article 9 - Protection & Prevention - Para 2
03	Article 9 - Protection & Prevention - Para 3
	Conclusion






Preamble (51)

The propagators of cyber-attacks tend to pursue financial gains directly at the source, thus exposing financial entities to significant consequences. To prevent ICT systems from losing integrity or becoming unavailable, and hence to avoid data breaches and damage to physical ICT infrastructure, the reporting of major ICT-related incidents by financial entities should be significantly improved and streamlined.

Existing TTPs

There are various reporting requirements that financial organizations must comply. The biggest challenge for any organization is to fully appreciate the depth of the data breach as part of their incident response (IR) activities, ensuring they can report correctly. In many occurrences financial organizations need to report to the local regulatory office (Data Protection Commission (DPC), Information Commissioners Office (ICO), etc.) within 72 hours of becoming aware of the breach.

Actifile Policy

-  Actifile has real-time visibility and monitoring of all unstructured data residing and flowing between your devices, department's and users. Any data exfiltrated or amended during a data breach is identifiable via the activity log. This capability ensures that your organization has immediate visibility of data required to inform various regulatory organizations.
-  Actifile has an inbuilt flexible encryption feature that ensures any sensitive data can be encrypted with a Zero Trust or lifecycle appreciation policy. Utilizing these Actifile policies, enables resiliency for data that falls under certain regulations. This data cannot be opened if attempts are made from unauthorized personnel outside of your organization.
-  Actifile ensures your organization has the confidence to know that all encrypted data that has been illegally exfiltrated will continue to be secure and unreadable.

Article 9 – Protection & Prevention - Para 2

Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.

Existing TTPs

A combination of aligned security and data management TTPs remain the standard when designing and implementing levels of maturity to protect an organization's infrastructure and data. Endpoint, network, boundary and communication tools continue to be the correct primary method to detect and mitigate cyber-attacks. When an attack is missed/overlooked, knowledge regarding the exact scope of the data breach cannot always be understood. Data visibility and protection across all devices tends to be restricted to databases, with little to no visibility of data residing on file servers and workstations.

Actifile Policy

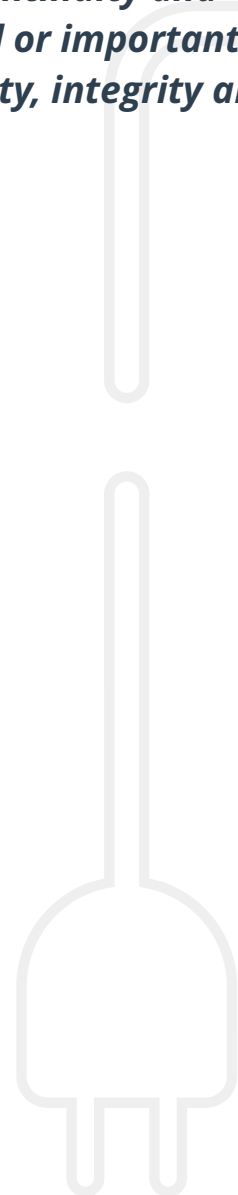
-  Deploying Actifile guarantees that your organization will discover and monitor all data that resides (at-rest), active (in-use) and flowing (in-motion) between devices, departments and users.
-  Discovered data is assigned a classification related to a specific industry regulation, compliance and/ or internal data management policy.
-  Real-time monitoring ensures that you are always aware and understand the monetary risk if such data were exfiltrated or sent in error without authorization.
-  Confidentiality of [sensitive] data can be assured using the Actifile Zero Trust flexible encryption feature. This ensures that data shared or illegally exfiltrated can only be read on devices with the unique Actifile license key.

Article 9 – Protection & Prevention - Para 2

Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.

Actifile Policy Cont.

- Your organization is able to apply the Actifile encryption feature to visually track how their data is being de-risked, contributing to your organization's overall risk management strategy.
- When an employee leaves your employment and you have allowed the use of BYOD devices, the IT support team will [in real-time] know what company data is resident on the devices. In conjunction with the employee, this data can be removed prior to the employee leaving the organization, eliminating subsequent access to sensitive company data.



Article 9 – Protection & Prevention - Para 3

In order to achieve the objectives referred to in paragraph 2, financial entities shall use ICT solutions and processes that are appropriate in accordance with Article 4 (principle of proportionality). Those ICT solutions and processes shall:

(b) minimise the risk of corruption or loss of data, unauthorized access and technical flaws that may hinder business activity;

(c) prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;

(d) ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error.

Existing TTPs

Current TTPs provide organizations with the capability to duplicate systems and data during standard operating activities, offering the ability to fail-over and maintain levels of availability. In addition, data management tools such as Data Loss Prevention (DLP) attempt to stop data from being shared without authorization and file encryption impairs the unauthorized recipient of data from opening/reading the data.

During cyber (exceptional) incidents, the attackers have proved they have the ability to compromise primary and fail-over devices and also exfiltrate production data, deleting backup data and VSCs.

Actifile Policy

- Access to the Actifile portal is allowed via multi-factor authentication. Users have no access to the portal unless specifically assigned as an administrator.
- Deploying Actifile encryption feature will ensure that any attempt to exfiltrate data as part of a ransomware attack, [the data] will not be accessible/read by the attacker(s).
- Actifile discovery ensures that any data residing on devices is authorized to be held and accessed. Unauthorized/mistaken data residency can be rectified immediately ensuring that abuse of data and inadvertent loss from a compromised device is minimized.
- Actifile logs every data activity, ensuring that in a post breach situation the IT support team and Data Protection Officer (DPO) have factual data points for inappropriate data behavior.



Conclusion

The critical nature of the digital-first financial services industry to a country's economic and critical national infrastructure, necessitates compliance with a level of resilience rules.

Implementing DORA rules will be different for each financial organization based on the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

Implementing Actifile Data Security Platform to assist with an organization's implementation TTPs for DORA, will significantly increase its data and security maturity level and elevate its overall cyber resilience status.

Actifile guarantees continual discovery and monitoring of all data entering, leaving and circulating across your infrastructure during its lifecycle. The addition of flexible encryption ensures that data resilience is guaranteed and any attempts to read unauthorized data will fail.



Empower Your Business with Cyber Resilience

Interested in Cybrilliance?

For more information visit: <https://www.cybrilliance.com>

Contact@CyBrilliance.com

CyBrilliance HQ

*Burlington,
Ontario,
L7L 4C4.
Canada.*

CyBrilliance EMEA

*Covent Garden,
London,
WC2H 9JQ.
United Kingdom.*

CyBrilliance Asia

*Ulsoor,
Bangalore,
560008.
India.*