



DORA regulation (EU) 2022/2554 is a legislative text of the European Union on the cybersecurity of financial entities. It creates a regulatory framework on digital operational resilience, which involves the ability to withstand, respond to, and recover from disruptions affecting information and communication technologies (ICT).

January 16, 2023

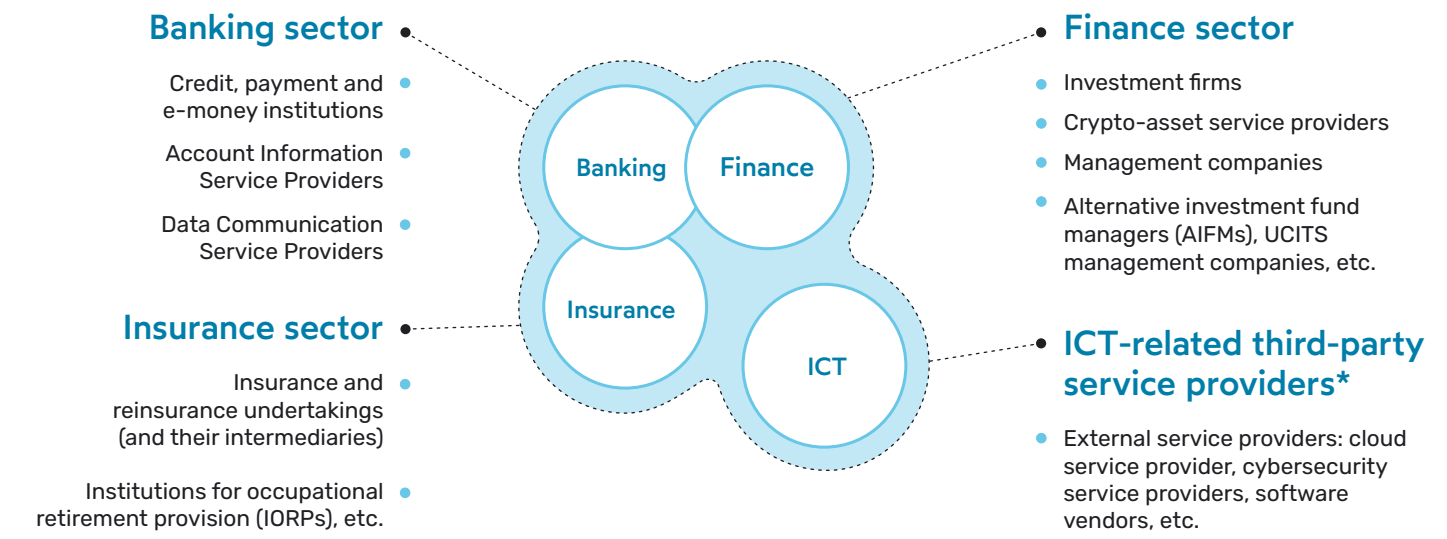
 Regulation enters into force.

Legal application

January 16, 2025

 Regulation becomes enforceable.

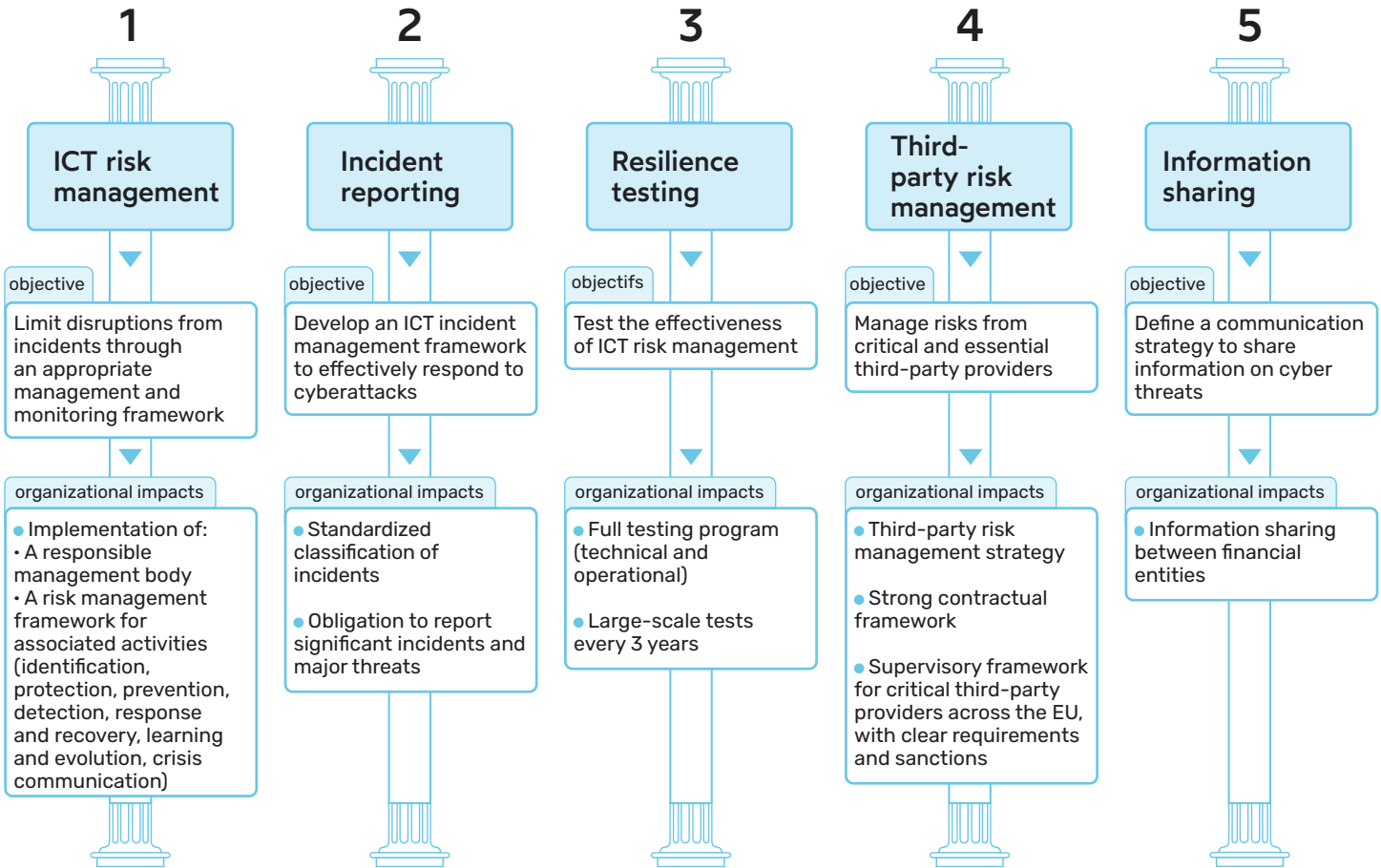
21 categories of entities concerned



Note: Only micro-enterprises (less than 10 employees and annual turnover < €2M) are excluded from the regulation.

**Information and Communication Technologies*

The 5 pillars of the regulation



DORA requirements and Oodrive solutions: guaranteed compliance

Oodrive solutions aligned with ICT risk management requirements

Articles 9 to 12: ICT risk management

Financial entities design, acquire, and implement ICT risk management strategies, policies, procedures, and tools to ensure the resilience, continuity, and availability of ICT systems. These aim to maintain high levels of availability, durability, integrity, and confidentiality of data, whether at rest, in use, or in transit.

Authentication

To enhance security, access to Oodrive solutions requires **multi-factor authentication** (MFA) using methods such as one-time passwords (OTP) via SMS or TOTP, Authenticator, and FIDO2, in addition to LDAP and SAMLv2 protocols.

Data encryption key management

Oodrive's key management complies with ANSSI recommendations and the General Security Framework (RGS). Data flows are secured with **SSH and TLS protocols**. Data is encrypted at rest using HSM (hardware security modules).

Access management

Oodrive applies **governance rules to manage the access lifecycle** with role-based and functional options, as well as granular access control policies and user event tracking (creation to deletion).

User activity traceability and control

Administration modules ensure **full traceability** of user activities and provide security analytics on all types of users, **including mobile**. Export and filtering features allow for automatic report generation.

Monitoring and detection of abnormal activity

Oodrive's SOC (security operations center) uses **SIEM** (security information and event management) to collect and analyze events from various components of its environments. This allows for efficient incident detection, quick response, and **continuous improvement of security indicators**.

Data backup and restoration

Oodrive **manages data backup and restoration (data, logs, applications)** across multiple datacenters located in France. Data is backed up daily, secured, and regularly tested for restoration. The Oodrive Save solution enables clients to back up and restore data from their own servers and workstations.

Comprehensive ICT business continuity policy

Oodrive ensures service continuity by using an architecture with redundant components and real-time data synchronization across multiple data centers located in France. This guarantees the implementation of a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) covering all of our services.

Security audits and controls

To ensure optimal security, Oodrive regularly performs audits and controls according to standards such as SecNumCloud and ISO 27001. **Various types of audits are performed: internal, organizational, external penetration tests, and intrusion tests**, ensuring client confidence and internal ISMS compliance.

In addition, Oodrive allows its clients to conduct their own audits and penetration tests in order to validate the compliance of Oodrive's services with their internal Information Security Policy.

Oodrive as an ICT third-party service provider

Article 28-5

Financial entities may not enter into contracts with third-party ICT service providers that fail to meet appropriate security standards. Any contractual agreements with ICT providers must comply with the most demanding security and information protection standards.

Oodrive guarantees the highest level of data protection and confidentiality. Its offerings have been **SecNumCloud-qualified** since 2019 and meet more than 400 requirements defined by ANSSI. By choosing Oodrive, clients benefit from best practices and remain fully compliant with the fourth pillar of the DORA regulation.