Article 9 — Protection and prevention

PRIMARY

Publisher	Digital Operational Resilience Act
Published	2025-01-17
Retrieved	2026-09-24
Cite key	digitaloper2025article
URL	https://www.digital-operational-resilience-act.com/Article_9.html

Regulation (EU) 2022/2554, Article 9, Protection and prevention.

9(1) Financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk.

9(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.

9(3)(a) ensure the security of the means of transfer of data; (b) minimise the risk of corruption or loss of data, unauthorised 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.

9(4)(a) develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data; (b) establish a sound network and infrastructure management structure; (c) implement policies that limit physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions; (d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems.