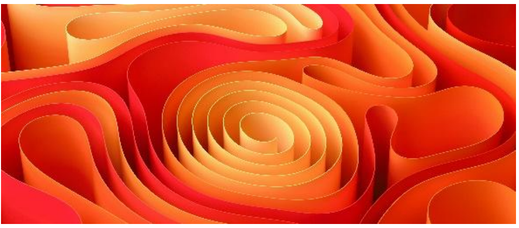
Pills

Regulatory/Supervisory Pills | N.127 September 2025



TOPICS:

Technology

SOURCE

European Central Bank

ECB Finalises Guide on Outsourcing Cloud Services

- The ECB Guide outlines **supervisory expectations for financial institutions outsourcing cloud services to Cloud Service Providers (CSPs)**. It aims to **reinforce operational resilience**, align with the Digital Operational Resilience Act (DORA), and **ensure effective management of ICT third-party risks** without introducing new binding obligations.
- **Governance and Responsibility**: Supervised entities are fully accountable for managing ICT risks associated with cloud outsourcing, even when services are delivered by CSPs. Institutions must define clear internal and contractual responsibilities, perform ex ante risk assessments, and ensure that cloud strategies align with overall business and ICT risk strategies.
- **Risk Management and Resilience**: Entities are expected to assess vendor lock-in, data security, geopolitical risks, and concentration risk, particularly for critical or important functions. Business continuity planning should cover backup, recovery, and failover strategies, including the use of hybrid or multi-cloud models, while ensuring that exit plans are feasible, tested, and aligned with contractual terms.
- **Security and Data Integrity**: Data must be protected across its lifecycle using strong encryption and cryptographic controls.
- The ECB promotes data locality controls, rigorous identity and access management (IAM) policies, and alignment of CSP practices with the supervised entity's own security standards. Risks linked to data processing in third countries and complex sub-outsourcing arrangements should be carefully evaluated.
- **Exit Strategies**: DORA mandates that entities have robust exit strategies in place, especially for critical functions. These strategies must be scenario-based, include cost and resource planning, and allow for the timely transfer or internalization of services. Contractual termination rights should address CSP changes in performance, legal jurisdiction, or ownership.
- **Oversight and Auditing**: Continuous monitoring of CSPs is required, supported by independent tools beyond those provided by the CSP. Incident reporting mechanisms should be contractually enforced. Internal audits must assess outsourcing arrangements independently, and shared audits with other institutions are encouraged where appropriate.