

Third-party outsourcing for financial services

Key things you need to know

Financial services institutions are moving to the cloud at pace and at scale. In turn, Operational Resilience must focus on third-party risk and how to manage it. The reason is that as firms migrate to cloud-based solutions and transform their business, they increasingly use third parties to deliver critical services to customers.

Third party risk management (TPRM) and the key industry and regulatory guidelines that have been issued are now key concerns and will also impact financial institutions outside the EU conducting business there. These include the European Cloud User Coalition (ECUC) Position Paper and the European Banking Authority (EBA) guidelines on outsourcing arrangements, driven primarily by the BoE Policy Statement, PS7/21 Outsourcing and third party risk management, published in March 2021.

Third party risk management (TPRM)

TPRM is a form of risk management that focuses on identifying and reducing risks relating to the use of third parties for critical services. TPRM is now high up on the risk agenda for executives and board members because regulators have issued new guidelines that significantly raise the bar in how firms should manage this risk.

Challenges include:

- Insufficient resources and capabilities to manage all third-party risks
- Inconsistent and ineffective approaches to risk management through the lifecycle of a relationship or service
- Failure to harness technology and data-enabled automation for decisioning, monitoring and workflows
- Sustaining a complex operating model that spans multiple business areas

Your TPRM framework should cover all forms of cloud arrangement. It should include the materiality and risk of each arrangement, the resilience requirements of services and data hosted in the cloud, and detailed resilience options.

A business continuity plan (BCP) and non-stressed and stressed exit plans should also be included.

The European Cloud User Coalition (ECUC)

The purpose of the ECUC is to strengthen the public cloud ecosystem for the entire European financial industry. Its primary objective is to develop a joint position on common challenges and solutions with cloud services providers to meet regulatory expectations.

Challenges identified by ECUC:

- Public cloud adoption is challenging due to the specifics of cloud computing being regarded as outsourcing
- Legislation such as Digital Operation Resilience Act (DORA) and rulings such as Schrems II currently make it difficult to adopt public cloud services
- Engaging CSPs individually leads to additional administrative effort and time, as well as misdirection of priorities

The ECUC positioning paper covers requirements for privacy, security, governance, regulation and standard contractual clauses. It provides solutions to some of the challenges presented by cloud adoption. The aim is to provide guidance for ensuring long-term compliant use of cloud technology.

European and UK guidelines on outsourcing arrangements

Regulators such as the European Banking Authority (EBA) and the Bank of England (BoE) are pushing financial service institutions to improve their cloud flexibility. These guidelines also encourage good governance, risk assessments, accessibility and auditability.

The BoE guidelines broadly align with those of the EBA, but are more current. Both include requirements around:

- Governance and record keeping
- Considerations before outsourcing agreements are made
- Actions to take while outsourcing agreements are in place
- Access, audit and information rights

You can find out more by reviewing the **BoE guidelines** and the **EBA guidelines**.

Provisions must be made in the outsourcing contract for regulators to exercise the same access and audit rights. The difference is that for regulators, those rights must be able to be exercised for all outsourcing, not just critical or important ones.

What action should you take?

In material cloud outsourcing arrangements, options for cloud resiliency may include multiple data centers in different locations, multiple or back-up vendors, a combination of on-premises and public cloud data centers, or retaining the ability to bring systems back on premises.

A new hybrid and multi-cloud infrastructure will bring the ultimate flexibility. It will grant the ability to shift data and move workloads between multiple cloud providers, and even back on-premises if necessary. And any data move will be swift – with minimal disruption.

So, no matter the regulatory concerns of the day regarding your data, you will always be ready and you will always remain compliant.

Teradata is the only provider that excels in every scenario, with the hybrid and multi-cloud solution to turn regulatory oversight into your new opportunity.

About Teradata

Teradata is the connected multi-cloud data platform company. Our enterprise analytics solve business challenges from start to scale. Only Teradata gives you the flexibility to handle the massive and mixed data workloads of the future, today. The Teradata Vantage architecture is cloud native, delivered as-a-service, and built on an open ecosystem. These design features make Vantage the ideal platform to optimize price performance in a multi-cloud environment. Learn more at **Teradata.com**