WHITE PAPER

Operational Resilience in the Cloud

Why financial services leaders and regulators are concerned, and what you can do about it.

Graham Corr, Senior Industry Consultant,
EMEA Financial Services Practice

03.22 / DATA ANALYTICS / WHITE PAPER

teradata.

Table of Contents

Data at the heart of operational resilience

It's 7am and the working day is just starting when your cloud provider updates its status page to announce a power failure at a data centre. Will it affect your services – which ones, and for how long? Can you maintain critical operations – and what are the consequences if you can't?

It's impossible to predict how and where the next failure will be or to prepare for every eventuality. Operational resilience in a connected cloud-first world is the challenge that's keeping financial services leaders and regulators awake at night. Significant dependency on a handful of global providers is introducing new systemic risks to the sector. Action is needed, and the time to act is now.

Moving applications and operations to the cloud does not mean that operational resilience is 'built in.' Reliance on single-cloud or 'cloud only' implementations actually creates risk of significant disruption when a provider suffers an outage. And, as recent events have demonstrated, even the biggest cloud vendors can have multiple failures for multiple reasons. Independent experts recorded 21 separate outages of major cloud platforms in 2020, and 2021 continued in the same vein with AWS, Microsoft, Google, and Facebook all experiencing serious outages.

Financial services businesses must invest in their own operational resilience to absorb shocks and react quickly to maintain operations whatever the circumstances.

Operational resilience must include detailed awareness of risks to the flow of data across the enterprise and precise plans for access, recovery, and continued use of data to support ongoing viability of critical functions.

Regulators increasingly want proof of resilience, and the costs of not being able to provide important business services could be catastrophic. Ensuring continued access to critical data must be one of the most significant planks in any operational resilience plan.

teradata.

Understanding operational resilience in the new cloud landscape

The cloud offers many opportunities and advantages for financial services companies. Accordingly, more and more companies are shifting more and more of their workloads to the cloud.

- Between 40 and 90% of banks' workloads globally could be hosted on public cloud or software-as-a-service within a decade.[1]

The efficiencies and cost savings of the cloud are clear. But cloud-centric operations introduce new risks, and present different challenges, for those tasked with maintaining operational resilience. Managing data and workloads in the cloud necessitates trading some control in exchange for flexibility and cost-savings. Full consideration of what these trade-offs mean for operational resilience is necessary; cloud-first strategies should not become cloud-only strategies without detailed exploration of these new risks.

Cloud commercial risks

Moving to the cloud means working with new partners and trusting them with your data. Ensuring full and complete understanding of the terms and conditions that govern those relationships is essential to maintain operational resilience. How easy is it to repatriate data from cloud partners if necessary? What will it cost?

Financial Service organizations must also assess the impact on operational resilience of the terms and conditions imposed by cloud service providers (CSPs).

- Globally, nearly two-thirds of all cloud services (61%) are provided by the top three Big Tech CSPs (Amazon, Microsoft, and Google).[2]
- 70% of banks and 80% of insurers rely on just two cloud providers for IaaS (Infrastructure as a service).[3]

This concentration gives Big Tech significant power to set terms and define the nature of commercial relationships. Are their terms compatible with internal governance and compliance, do they align with operational resilience plans? Does the business have the flexibility it needs to be resilient or is it locked-in to a single supplier which can dictate commercial terms?

> **"That concentrated power on terms can manifest itself in the form of secrecy, opacity, not providing customers with the sort of information they need to monitor the risk in the service."**
>
> Andrew Bailey, Governor of the Bank of England[4]

Commercial aspects of operational resilience should also consider data protection and exposure to cyber-risks. Although cloud service providers have made significant investments in privacy and cybersecurity no one is immune from attacks.

In addition, compliance with GDPR and similar protections for personal data, must be maintained as central to operational resilience. Knowing exactly where data resides and being able to prove that any transfer of data is fully compliant with local law is essential. This includes movement to and between, cloud service providers.

1 https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report

2 https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers

3 https://www.imf.org/en/News/Articles/2021/06/16/sp061721-bigtech-in-financial-services

4 https://www.reuters.com/business/retail-consumer/bank-england-crack-down-secretive-cloud-computing-services-2021-07-13

teradata.

For example, the Court of Justice of the European Union (CJEU) Schrems II ruling puts clear responsibility on firms to ensure additional levels of protection for personal data if it cannot be guaranteed by cloud service providers.[5]

Cloud technology risks

Financial institutions who are used to weekly 'fail-over' tests of on-premise data centres may soon need to consider similar resilience tests for cloud-based infrastructures. In the UK, for example, the Prudential Regulation Authority is seeking ways to access more information from major cloud providers in order to better assess risk from technical failures of cloud services.[6]

According to reports in the Financial Times, one person familiar with the Regulator's plans said: "We are looking at cloud providers from an operational resilience perspective. Do we need to step in more, how do we get confidence in them? We are starting to consider them critical third parties that we need more oversight of."[6]

Hybrid and multi-cloud strategies are gaining traction to reduce risk of single points of failure and from vendor lock-in.

- Google Cloud's own research highlights that 28% of financial services currently rely on a single vendor.
- But 88% of those not already using multi-cloud are considering it.[7]

When considering technical barriers to operational resilience, lock-in risks, as well as the ease of replicating specific workloads in different clouds must be assessed. The ability to repatriate to owned on-premise infrastructure must also be taken into account.

Cloud systemic risks

Regulators are concerned that systemic risks are increasing as the proportion of services dependent on cloud increases.

- Nearly half of financial services workloads are now executed in public clouds.[8]
- "The increasing reliance on a small number of CSPs and other critical third parties could increase financial stability risks without greater direct regulatory oversight of the resilience of the services they provide." The Bank of England, July 2021.[9]

5 https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2022

6 https://www.ft.com/content/29405a47-586b-4c5a-b641-0f479b4cee1d

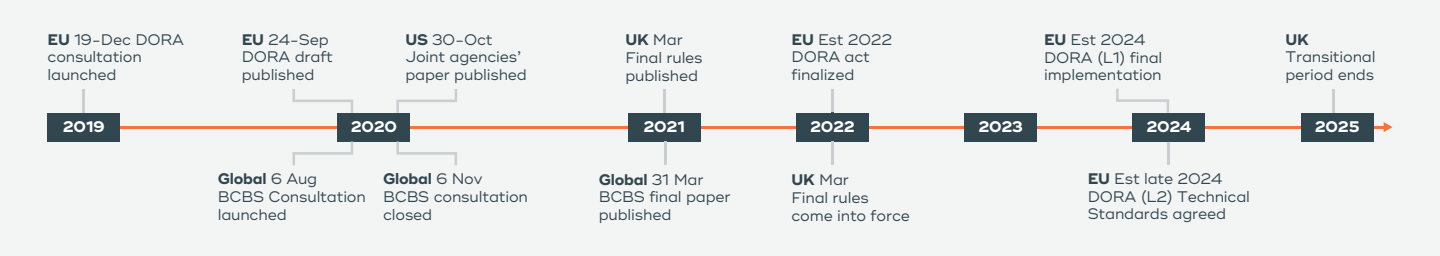
7 https://cloud.google.com/blog/topics/inside-google-cloud/new-study-shows-cloud-adoption-increasing-in-financial-services

8 https://www.statista.com/statistics/1257930/cloud-workloads-financial-services-banking

9 https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management

teradata.

What regulators are doing



Regulators around the world are already starting to act on these risks.

For example in the UK, one of the first jurisdictions to take action, new rules for operational resilience were introduced in March 2021. The rules gave financial institutions just one year to implement, and the constrained timelines require firms to fully demonstrate their ability to stay within their impact tolerances. The Prudential Regulatory Authority went so far as to make explicit mention of both ICT outsourcers and the dangers of concentration risk in its Policy and Supervisory Statements (PS7/21 and SS2/21) issued in March 2021. The specific focus of these was to manage resiliency in a cloud-first environment.

They emphasize the importance of avoiding over-reliance on any one provider of outsourced ICT (including cloud services) as well as avoiding lock-in and ensuring substitutability of cloud services (including the identification of suitable alternate providers). They also call for evidence of planned temporary measures to continue operations in the event of a stressed exit for any reason.

By the end of the transitional period in March 2025, firms must be able to show how operational resilience can be maintained for any asset (including data and technology) linked to the delivery of any important business service. The PRA states that ***"it expects firms to assess the resilience requirements of the service and data that are being outsourced and, with a risk-based approach, decide on one or more available cloud resiliency options."***

In Europe, also early to take action, there is a slightly different approach. The Digital Operational Resilience Act, known as DORA, targets many of the same risks and is a fundamental pillar of the wider European Digital Finance Act. As well as outlining the digital resilience requirements for firms, including calling for multi-vendor strategies for ICT and mapping of technology dependencies, it goes further than other regulations by extending oversight to significant third-party providers.

These explicitly include cloud service providers. Depending on the scale, complexity, and importance, firms will need to keep a register of all contractual arrangements provided by ICT third-party providers. The vendors themselves will be subject to regulatory oversight to ensure that they have plans and procedures in place to protect firms from technology risks.

The complexity of this legislation timelines could be extended, but the initial DORA draft was published in September 2020 and a final draft expected in 2022 with European Parliament, Council, and Commission due to debate in trialogue. Enforcement is expected from a year after adoption of the Act. In parallel, further enhancements and extension (level 2) are expected to be published soon for discussion and agreement 2 to 3 years later. It will have significant impacts on how European financial institutions contract and manage their cloud service providers, and they are advised to start planning now.

UK and EU regulators so far have the most advanced measures in place for operational resilience. However other jurisdictions around the world, including the USA, are starting to implement similar measures. Organizations need to follow local regulations for operational resilience in the markets where they operate, but the signs are that regulation is only going to increase in this area.

teradata.

Answering the hard questions now makes good business sense

The common thread that links all of these regulatory moves is the need for firms to demonstrate operational resilience in the face of a sudden, unplanned 'stressed' exit from a cloud service. Regulators will demand to see detailed plans, and their effectiveness proven with stringent testing. Published rules and proposed regulation from the PRA[10], ECB[11], and Federal Reserve[12] all point to more testing in this area. But financial institutions can prepare for these demands at the same time as building-out the scalable, fast, and flexible data platforms they need to compete in the digital world.

Robust questioning from the regulator will go to the heart of firms' cloud strategies and their ability to deal with sudden shocks ranging from cloud 'outages' to contractual disagreements and business failure of suppliers. From a data perspective, they will want to test plans to access and use data from across the organization to support the analytics and automated decision-making even during an extended outage from a cloud service provider.

Knowing where data is, which important business services rely on which data sets, and where crucial analytics models run, is the fundamental first step in building this resilience. Leading organizations are already advanced in answering these questions. Allowing data to flow unhindered across the enterprise so that it can be used in innovative ways to create new services and enhance customer experience is core to the digital transformation of the industry. Viewed from this perspective, the demands of the regulator to demonstrate operational resilience are added benefits that can be derived from these ongoing projects.

Instead of seeing the increased scrutiny of regulators, and the need to develop operational resilience to handle the loss of 'too big to fail' cloud service providers, as a separate and onerous task, firms can integrate these demands as additional signposts towards effective data infrastructures.

Operational Resilience Checklist

Data and data analytics must be fully considered in your operational resilience plans. Have you asked these questions and are you happy with the answers you have?

- Have you discussed exit plans with your cloud service providers?
- Do they provide compliant contractual clauses that ease 'stressed exit' provisions?
- Have you reviewed the security, recovery, and restoration commitments of CSPs?
- Do you know where all your data is?
- Have you undertaken workload placement analysis?
- Can you map data dependencies of important business services?
- Can you identify all the data analytics workloads essential for important business services and know where they run?
- How quickly can you replicate analytics models on alternative platforms?

10 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=D6335BA4712B41473OC697DC8BEB353F3EE5A628

11 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Financial-services-improving-resilience-against-cyberattacks-new-rules-_en

12 https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm

teradata.

What you need to do now

Many financial institutions have already decided on multi-cloud approaches. Whether this is for financial or operational reasons, or to match specific workloads to specific technology features, a multi-cloud approach provides the basis for operational resilience. However, on their own, multi-cloud architectures may not provide enough resilience. Technical, cost, and contractual barriers might still exist that make it difficult to move workloads out of one cloud and into another.

Adding (or retaining) some on-premise infrastructure can add another level of resilience. Retaining the ability to deliver critical services from owned infrastructure under the bank's direct control can act as a buffer should cloud-based resources become inaccessible for any reason.

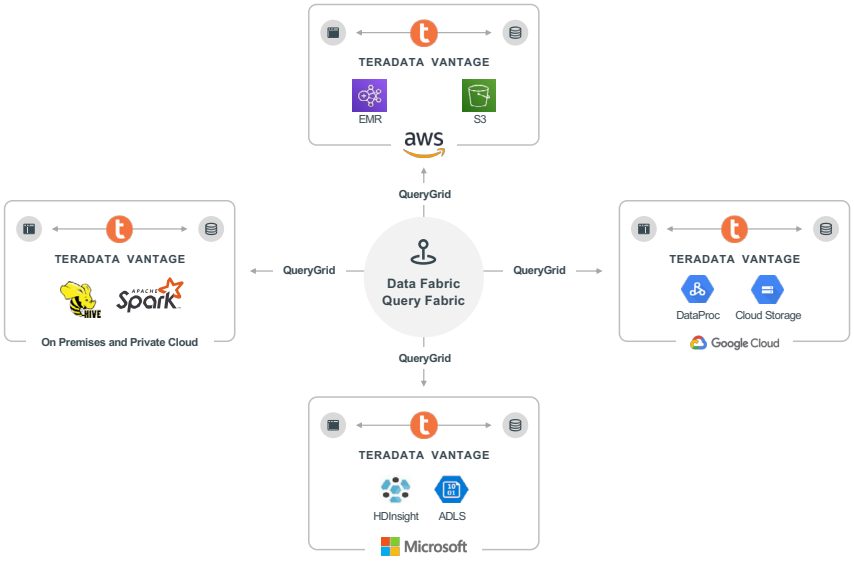
Blending the two approaches with a connected cloud data environment provides a solution. Creating a data platform that works seamlessly with clouds from any vendor, as well as on-premise solutions, provides not only operational resilience, but flexibility to cost effectively pursue digital transformation objectives. Such a solution can connect and synchronize data from any application and support the firm's data needs from basic data warehousing to advanced analytics.

What it could look like

Organizations around the world are leveraging the performance and multi-dimensional scalability of Teradata to create enterprise-wide cloud data platforms that future-proof their evolving analytic needs. Acting as a single point of truth that integrates data from any source, Teradata ensures data flows to where it's needed. As the diagram below illustrates, it also allows them to connect to any cloud service provider whilst retaining on-premise capabilities. Not only does this provide the flexibility to keep their digital transformation options open but delivers the requirements of operational resilience as an added benefit.

Operational Resilience

Architectural blueprint of how to seamlessly switch between multiple cloud providers and move back on-premises to ensure business continuity. Teradata's hybrid multi-cloud data platform increases your flexibility and avoids you being locked into a single public cloud vendor.



High speed data fabric connects workloads in a highly distributed environment.

Choice of entry point provides ability to originate queries at scale on any system on the fabric, spanning on-premises and multiple public cloud environments.

Pushdown processing enables minimal data transfer and egress charges by moving queries to execute closest to the data.

Reviewed for technical accuracy February 2022

teradata.

A hybrid and multi-cloud world

Financial services organizations are rapidly adopting cloud architectures as the foundation of agile, customer-centric business models. They are doing so to reduce cost and give them the flexibility to not only respond to volatile economic and customer environments, but to help predict and plan for the next waves of change. But clouds themselves are not static. As part of their strategies financial institutions must carefully assess, and continuously monitor, risks to operational resilience implicit in cloud infrastructures.

Commercial, technology, and systemic risks exist, and regulators are already concerned. Where Europe and the UK have led, others will surely follow. Leading organizations are already anticipating and preparing for inevitable regulation - the time to act is now.

The operational risks associated with the cloud can be mitigated with hybrid multi-cloud approaches that retain flexibility and resilience.

Today, Teradata is working with financial institutions around the world as they build operational resilience into their cloud strategies.

Teradata's hybrid multi-cloud approach enhances operational resilience by providing the flexibility to move data and workloads seamlessly between clouds, and from any cloud to an on-premise infrastructure as needed. It can support planned or stressed exits from a particular cloud and, in the event of an outage, data can quicky be restored to whatever on-premise or cloud systems remain unaffected allowing operations to resume almost immediately.

The Teradata hybrid, multi-cloud approach makes good business sense for any financial services business looking to thrive in the fast moving digital world. The combination of these advantages with enhanced operational resilience capabilities has led many financial services companies to turn to Teradata to help plan and execute their risk mitigation strategies.

About Teradata

Teradata leverages all of the data, all of the time, so you can analyze anything, deploy anywhere, and deliver analytics that matter. By providing answers to the complexity, cost, and inadequacy of today's analytics, Teradata is transforming how businesses work and people live. Get the answers at Teradata.com.

Author

Graham Corr Senior Industry Consultant,
EMEA Financial Services Practice

17095 Via Del Campo, San Diego, CA 92127 Teradata.com

The Teradata logo is a trademark, and Teradata is a registered trademark of Teradata Corporation and/or its affiliates in the U.S. and worldwide. Teradata continually improves products as new technologies and components become available. Teradata, therefore, reserves the right to change specifications without prior notice. All features, functions and operations described herein may not be marketed in all parts of the world. Consult your Teradata representative or Teradata.com for more information.

© 2022 Teradata Corporation All Rights Reserved. Produced in U.S.A. 04.22

teradata.