FINANCIAL SERVICES | DATASHEET

# Business continuity for financial services

Key things you need to know

Financial services institutions are moving to the cloud. In turn, Operational Resilience must increasingly focus on third-party risk and how to manage it.

The reason is that regulators believe outages and disruptions are inevitable, and leading organizations understand that detailed contingency planning for such events is central for effective business continuity.

The key regulatory developments to be aware of include Stressed Exit, Substitutability and Concentration Risk and The Digital Operational Resilience Act (DORA).

## Stressed Exit

Stressed Exit plans are essential for third party outsourcing. Regulators require a Stressed Exit plan to be in place for each material outsourcing arrangement. Financial Services institutions must develop, document and test their exit strategy, which should cover and differentiate Stressed Exit and Non-stressed Exit scenarios.

**Stressed Exit**

Exiting an outsourcing agreement in stressed circumstances following the failure or insolvency of the service provider. By their nature, these exits are unplanned and often reactive.

**Non-stressed Exit**

Moving away from an agreement for commercial, performance, or strategic reasons in a planned and managed way.

Some of the key exit and contingency planning actions include:

- Develop a business continuity plan ('BCP'), and document plans for Stressed Exit and Non-Stressed Exit – these are needed for both existing and new important outsourcing arrangements
- Define and quantify your impact tolerances in the event of a disruption or outage
- Ensure BCPs are focused on the ability to deliver important business services that are supported by third parties
- Test Stressed Exit and Non-Stressed Exit plans for all important outsourcing arrangements ensuring you stay within impact tolerances
- Ensure service providers implement their own BCPs to anticipate, withstand, respond to, and recover from severe but plausible operational disruptions

## Substitutability and Concentration Risk

The scale and expertise of cloud providers may provide Operational Resilience that is beyond the capability of a firm acting alone. However, as just three providers dominate the cloud market, regulators have concerns about concentration risk and a lack of substitutability.

**Substitutability**

The ability for a firm to mitigate over-reliance on a single or limited number of service providers.

**Concentration risk**

Large numbers of financial institutions becoming reliant on the same limited number of service providers.



teradata.

Regulators understand that outages are inevitable. So they require financial services firms to prove how easy, difficult, or impossible it is to move between providers.

They do not want any single financial firm, or even a specific business area, to become overly reliant on the same service providers. They are also concerned that potential outages may create systemic risk. For example, if three of the United Kingdom's largest banks use the same cloud service provider, and it is attacked or shuts down unexpectedly, the result would be catastrophic for the whole system.

## The Digital Operational Resilience Act (DORA)

Digitalization efforts have accelerated within Financial Services. Regulation that previously focused on manual finance processes are no longer fit for purpose. DORA sets out to redress this within the EU with common rules for mitigating digital transformation risks.

**DORA aims to:**

- Streamline and upgrade existing rules to make them fit for purpose
- Introduce new requirements to cover new technologies
- Manage ICT risks and related incident reporting
- Support firms' mandate to contain instability from ICT vulnerabilities

DORA covers digital testing, information sharing, and the management and monitoring of ICT third-party risks. Most notably, it requires contracts to contain a complete description of services, the locations and storage of data, plus relevant provisions on the accessibility, availability, integrity, security, and protection of personal data.

Contracts must include notice periods and reporting obligations of ICT third-party service providers, along with clear termination rights and dedicated exit strategies.

## What action should you take?

A hybrid and multi-cloud infrastructure is needed to ensure 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 and seamless – 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 infrastructure 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**

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

Teradata and the Teradata logo are registered trademarks 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.

© 2021 Teradata Corporation All Rights Reserved. Produced in U.S.A. 09.21

teradata.