

Business Continuity für Finanzdienstleistungen

Das sollten Sie wissen

Finanzdienstleister verlagern ihre Daten und Services in die Cloud. Hinsichtlich der operativen Resilienz sind dabei vermehrt Risiken durch Drittanbieter und deren Management zu berücksichtigen.

Der Grund dafür ist, dass die Regulierungsbehörden glauben, dass Ausfälle und Störungen unvermeidlich sind, und die jüngsten Erfahrungen haben dies bestätigt. Führende Unternehmen sind sich darüber im Klaren, dass eine detaillierte Notfallplanung für solche Ereignisse von zentraler Bedeutung für eine effektive Geschäftskontinuität ist.

Die wichtigsten regulatorischen Vorgaben beziehen sich auf den Notfall-Ausstieg, die Austauschbarkeit, das Konzentrationsrisiko sowie den Digital Operational Resilience Act (DORA).

Stressed Exit

Pläne für einen Ausstieg im Notfall sind für das Outsourcing unerlässlich. Aufsichtsbehörden verlangen in jeder Outsourcing-Vereinbarung auch einen Plan für den Stressed Exit. Finanzdienstleister müssen sowohl für den erzwungenen als auch den freiwilligen Exit detaillierte Strategien entwickeln, dokumentieren und testen.

Stressed Exit

Ausstieg aus einer Outsourcing-Vereinbarung in einem stressigen Umfeld nach dem Ausfall oder der Insolvenz des Diensteanbieters. Diese Exits sind naturgemäß ungeplant und häufig reaktiv.

Freiwilliger Exit

Planmäßige und gesteuerte Auflösung einer Vereinbarung aus kommerziellen, leistungsbezogenen oder strategischen Gründen.

Die wichtigsten Bestandteile eines Exit- und Notfallplans:

- Entwickeln Sie einen Business Continuity Plan (BCP) und dokumentieren Sie Maßnahmen für den erzwungenen und freiwilligen Exit – diese werden sowohl für bestehende als auch für neue Outsourcing-Vereinbarungen benötigt.
- Definieren und quantifizieren Sie die im Falle einer Störung oder eines Ausfalls tolerierbaren Auswirkungen.
- Stellen Sie sicher, dass sich BCPs auf die Bereitstellung wichtiger, von Drittanbietern unterstützter Business Services konzentrieren.
- Testen Sie Pläne für einen erzwungenen und freiwilligen Exit für alle wichtigen Outsourcing-Vereinbarungen, um innerhalb der Toleranzgrenze zu bleiben.
- Stellen Sie sicher, dass Diensteanbieter eigene BCPs implementieren, um schwerwiegende Betriebsstörungen zu antizipieren, abzuwenden bzw. darauf zu reagieren und sich von ihnen zu erholen.

Substituierbarkeit und Konzentrationsrisiko

Cloud-Anbieter können aufgrund ihrer Größe und ihres Knowhows eine operative Resilienz bieten, die Unternehmen alleine in der Form möglicherweise nicht erreichen würden. Da der Cloud-Markt jedoch von drei Anbietern dominiert wird, hegen die Aufsichtsbehörden Bedenken hinsichtlich des Risikos von Lock-ins und der mangelnden Substituierbarkeit.

Substituierbarkeit

Die Fähigkeit eines Unternehmens, die Abhängigkeit von einem einzigen oder einer begrenzten Anzahl von Diensteanbietern zu verhindern.

Konzentrationsrisiko

Viele Finanzinstitute, die auf dieselbe begrenzte Anzahl von Anbietern angewiesen sind.

Aufsichtsbehörden wissen, dass Ausfälle unvermeidlich sind. Daher verlangen sie von Finanzdienstleistern einen Nachweis, wie einfach oder schwierig (oder auch schier unmöglich) ein Wechsel zwischen Anbietern ist.

Die Aufsichtsbehörden wollen verhindern, dass Finanzunternehmen oder auch nur bestimmte Geschäftsbereiche zu sehr von einem einzigen Dienstanbieter abhängig werden. Sie befürchten auch, dass Ausfälle zu systemischen Risiken führen könnten. Wenn beispielsweise drei große Banken denselben Cloud-Anbieter nutzen und dieser angegriffen wird oder unerwartet ausfällt, hätte dies katastrophale Folgen für das gesamte System.

Digital Operational Resilienz Act (DORA)

Die Digitalisierung im Finanzdienstleistungsbereich hat sich beschleunigt. Regulierungen, die sich bisher auf manuelle Finanzprozesse konzentrierten, sind nicht mehr zielführend. DORA will dies EU-weit mit gemeinsamen Regeln zur Eindämmung der Risiken der digitalen Transformation beheben.

Ziel von DORA:

- Zweckdienliche Optimierung und Aktualisierung bestehender Regeln
- Einführung neuer Anforderungen zur Abdeckung neuer Technologien
- Verwaltung von IKT-Risiken und damit verbundenen Vorfallmeldungen
- Unterstützung des Mandats von Unternehmen zur Eindämmung von Instabilität durch IKT-Schwachstellen.

DORA umfasst digitale Tests, den Informationsaustausch sowie das Management und die Überwachung der Risiken durch IKT-Drittanbieter. Insbesondere müssen Verträge eine vollständige Beschreibung der Dienstleistungen, der Speicherorte und -verfahren sowie relevante Bestimmungen zur Zugänglichkeit, Verfügbarkeit, Integrität und Security sowie zum Schutz personenbezogener Daten enthalten.

Verträge müssen Kündigungsfristen und Meldepflichten von IKT-Drittanbietern sowie klare Kündigungsrechte und dedizierte Exit-Strategien umfassen.

Was sollten Sie tun?

Um Flexibilität zu gewährleisten, ist eine Hybrid- und Multi-Cloud-Infrastruktur erforderlich. Sie ermöglicht Ihnen, Daten und Workloads zwischen mehreren Cloud-Anbietern zu verschieben und bei Bedarf sogar wieder on-Prem zu verwalten. Jegliche Datenverschiebungen werden schnell und nahtlos – mit nur minimalen Störungen – erfolgen.

Durch eine Multi-Cloud-Backup-Strategie, bei der Daten synchronisiert und kopiert werden, stärken Finanzinstitute ihre Widerstandsfähigkeit und verringern langfristig das Risiko eines Datenverlusts erheblich.

Unabhängig von den aktuellen regulatorischen Bedenken bezüglich Ihrer Daten sind Sie also immer bereit und bleiben immer konform.

Teradata bietet erstklassige Hybrid- und Multi-Cloud-Lösungen für jedes Szenario, mit denen Sie behördliche Auflagen in Ihre neue Chance verwandeln können.

Über Teradata

Teradata ist das Unternehmen für vernetzte Multi-Cloud-Datenplattformen. Unsere Unternehmensanalysen lösen geschäftliche Herausforderungen vom Start bis zur Skalierung. Nur Teradata bietet Ihnen die Flexibilität, die massiven und verschiedenen Daten-Workloads der Zukunft schon heute zu bewältigen. Die Teradata Vantage-Architektur ist Cloud-nativ, wird „as-a-Service“ bereitgestellt und basiert auf einem offenen Ökosystem. Diese Designmerkmale machen Vantage zur idealen Plattform für die Optimierung des Preis-Leistungs-Verhältnisses in einer Multi-Cloud-Umgebung. Weitere Informationen finden Sie auf [Teradata.de](https://www.teradata.de).

17095 Via Del Campo, San Diego, CA 92127 [Teradata.com](https://www.teradata.com)

Teradata und das Teradata-Logo sind eingetragene Marken der Teradata Corporation und/oder ihrer Tochtergesellschaften in den USA und weltweit. Mit der Verfügbarkeit neuer Technologien und Komponenten entwickelt Teradata seine Produkte ständig weiter. Teradata behält sich daher das Recht vor, Spezifikationen ohne vorherige Ankündigung zu ändern. Die hier beschriebenen Merkmale, Funktionen und Lösungen werden möglicherweise nicht überall auf der Welt vermarktet. Weitere Informationen erhalten Sie bei Ihrem Teradata-Ansprechpartner oder auf [Teradata.com](https://www.teradata.com).

© 2021 Teradata Corporation Alle Rechte vorbehalten. Hergestellt in den USA. 01.22



teradata.