BARCLAYS

Kontrollpflichten externer Lieferanten

Wiederherstellungsplanung

Version 13.0, September 2023

1. Definitionen:

„Störungsereignis“	Ein Verzeichnis mit den Auswirkungen von Vorfällen, unabhängig von der Ursache, die Lieferanten mittels Implementierung von Wiederherstellungs- und Belastbarkeitsplanung und -kompetenzen reduzieren wollen.
„**Vorfall**“	ist ein störendes Ereignis, das im Rahmen des Tagesgeschäfts bewältigt werden kann, indem Wiederherstellungspläne aufgerufen werden.
„Wiederherstellungsplanung“	Wiederherstellungspläne sind Dokumente, die die Schritte und Maßnahmen zur Wiederherstellung des Betriebsstatus eines Services detailliert beschreiben. Diese können als Business-Continuity-Plan oder ähnliche Begriffe bezeichnet werden.
„**Wiederherstellungsplanung**“	Der Prozess oder die Planung für die Wiederherstellung von Unternehmensdienstleistungen, Geschäftsprozessen und den zugrunde liegenden Abhängigkeiten
„Zielvorgabe für die Wiederherstellungszeit“	ist die Zeit zwischen einem unerwarteten Ausfall oder einer unerwarteten Unterbrechung von Diensten und der Wiederaufnahme des Betriebs.
„Belastbarkeitskategorie“	Die Belastbarkeitskategorie ist eine Bewertung, die von Barclays verwendet wird, um Anforderungen an die Belastbarkeit auf einen Service anzuwenden. Die Belastbarkeitskategorie bestimmt die Zielvorgabe für die Wiederherstellungszeit (Recovery Time Objective, RTO), die Zielvorgabe für den Wiederherstellungspunkt (Recovery Point Objective, RPO) und die Anforderungen an die Validierungshäufigkeit.

2. Matrix der Belastbarkeitskritikalität:

Die Dienste des Lieferanten werden von Barclays einer spezifischen Belastbarkeitskategorie (0–4) zugeordnet, entsprechend den Auswirkungen, die eine Störung des jeweiligen Diensts für Barclays haben könnte. Eine höhere Belastbarkeitskategorie (d. h. eine niedrigere Zahl) stellt entsprechend der Bedeutung des Dienstes höhere Ansprüche an die Belastbarkeit bzw. Wiederherstellung. Der Lieferant stellt sicher, dass seine Dienste für die zutreffende, von Barclays für die vertraglichen Dienste vorgeschriebene Belastbarkeitskategorie die nachstehend festgelegte Zielvorgabe für die Wiederherstellungszeit (Recovery Time Objective, RTO) und den Wiederherstellungspunkt (Recovery Point Objective, RPO) erfüllen. Die folgende Tabelle gibt an, welche Lieferantenkontrollen auf Grundlage der definierten Belastbarkeitskategorie anwendbar sind. Die Einzelheiten dieser Kontrollen sind in Abschnitt 3 (*Kontrolle*) unten aufgeführt.

Bewertung von Risikoauswirkungen	Außergewöhnliche Auswirkung	Hohe Auswirkung	Mäßige Auswirkung	Geringe Auswirkung	Unerhebliche Auswirkung
Belastbarkeitskategorie	0	1	2	3	4
RTO-Ziel	bis zu 1 Stunde	bis zu 4 Stunden	bis zu 12 Stunden	bis zu 24 Stunden	Keine geplante Wiederherstellung
RPO-Ziel	bis zu 5 Minuten	bis zu 15 Minuten	bis zu 30 Minuten	bis zu 24 Stunden	Keine geplante Wiederherstellung

Häufigkeit der Technologietests	Belastbarkeitskategorie 0	Belastbarkeitskategorie 1	Belastbarkeitskategorie 2	Belastbarkeitskategorie 3	Belastbarkeitskategorie 4
Validierung von Systemwiederherstellungsplänen	Mindestens zweimal jährlich	Mindestens zweimal jährlich	Mindestens alle 12 Monate	Mindestens alle 24 Monate	Keine geplante Wiederherstellung
Validierung des Datenwiederherstellungsplans	Jährliche Validierung des Plans in produktionsähnlicher Umgebung	Jährliche Validierung mittels Desktop-Walkthrough	Optional	Optional	Keine geplante Wiederherstellung
Validierung des Plans zur Neuerstellung von Plattformen und Anwendungen	Jährliche Validierung mittels Desktop-Walkthrough	Jährliche Validierung mittels Desktop-Walkthrough	Optional	Optional	Keine geplante Wiederherstellung

Anwendbarkeit der Lieferantenkontrollen	Belastbarkeitskategorie 0	Belastbarkeitskategorie 1	Belastbarkeitskategorie 2	Belastbarkeitskategorie 3	Belastbarkeitskategorie 4
1. Anforderungen an die Abhängigkeitszuordnung zur Berücksichtigung bei der Wiederherstellungsplanung	✓	✓	✓	✓	O
2. Störende Ereignisse – Anforderungen an die Wiederherstellungsplanung	✓	✓	✓	✓	O
3. Anforderungen an Wiederherstellungsplanung und Validierung	✓	✓	✓	✓	O
4. Anforderungen an integrierte Tests	✓	✓	O	O	O
5. Anforderungen an Systemwiederherstellungspläne und Validierung	✓	✓	✓	✓	O
6. Anforderungen an Datenwiederherstellungspläne und Validierung	✓	✓	O	O	O
7. Anforderungen an Vielfalt der Datenzentren und Cloud-Serviceprovider	✓	✓	✓	✓	O
8. Anforderungen an Pläne zur Neuerstellung von Plattformen und Anwendungen	✓	✓	O	O	O

✓ = Erforderlich	O = Optional

Wenn während der Überprüfung Probleme festgestellt werden oder die Anforderungen während der Kontrolltests nicht erfüllt werden, muss der Lieferant Barclays unverzüglich (in der Regel innerhalb von 10 Tagen) benachrichtigen und die Probleme zu einem vereinbarten Termin beheben.

3. Kontrollen:

Der Lieferant muss über einen strukturierten Ansatz für Belastbarkeit (Business Continuity und Notfallwiederherstellung) verfügen, unterstützt durch ein Dokument mit Richtlinien und Standards, die die Anforderungen an die betriebliche und technische Belastbarkeit gemäß den Best Practices der Branche und den geltenden aufsichtsrechtlichen Anforderungen regeln. Der strukturierte Ansatz für Belastbarkeit muss von der Geschäftsleitung kontrolliert und jährlich auf Effektivität überprüft und getestet werden.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Anforderungen an die Abhängigkeitszuordnung zur Berücksichtigung bei der Wiederherstellungsplanung	Der Lieferant muss Abhängigkeiten definieren und dokumentieren, die für die Erbringung des Services für Barclays von entscheidender Bedeutung sind. Diese Abhängigkeiten sind alle 12 Monate oder bei wesentlichen Änderungen zu pflegen und zu überprüfen. Zu den zu berücksichtigenden Abhängigkeiten gehören: ▪ Technologie und Daten (intern und von Unterauftragnehmern zur Verfügung gestellt). ▪ Wesentliche Unterauftragnehmer (die einen wesentlichen Einfluss auf die Leistung und Bereitstellung des Diensts für Barclays haben könnten). ▪ Ausfall von Personal (Ausfall von Gebäuden oder/und Ausfall von Mitarbeitern; Wiederherstellungsstrategie bei nicht verfügbarem Arbeitsbereich oder Möglichkeit des Arbeitens von zu Hause erwägen)	Dienstleister müssen die Abhängigkeiten bei der Bereitstellung ihrer Dienstleistungen für Barclays verstehen. Alle Abhängigkeiten sind in ihre Business-Recovery-Pläne aufzunehmen, um sicherzustellen, dass diese berücksichtigt werden, um die Auswirkungen von Vorfällen zu reduzieren und die Nichtverfügbarkeit der Dienste für Barclays zu verhindern.
2. Störende Ereignisse – Anforderungen an die Wiederherstellungsplanung	Der Lieferant muss die für die Wiederherstellungsplanung zu berücksichtigenden störenden Ereignisse sowie die erforderliche Planung definieren, damit sichergestellt wird, dass die Dienstleistungen innerhalb der vereinbarten Service-Levels und der entsprechenden Zielvorgaben für die Wiederherstellungszeit erbracht werden können. Der Lieferant muss sicherstellen, dass solche Störungsereignisse die aktuelle Risiko-/Bedrohungslandschaft widerspiegeln, hinsichtlich Schweregrad und Plausibilität bewertet werden und durch Branchen- und Intelligence-Erkenntnisse unterstützt werden. Der Lieferant muss mindestens die folgenden Störungsereignisse in seine Planung einbeziehen. ▪ Beeinträchtigung der Erbringung von Services für Barclays durch den Verlust von Gebäuden an mehreren Standorten (Gebäude und zugehörige Infrastruktur sind nicht verfügbar).	Für Barclays ist es aus betriebswirtschaftlicher (und risikoorientierter) Sicht erforderlich, erhebliche Störungsereignisse zu vermeiden und/oder in der Lage zu sein, sich rechtzeitig von ihnen zu erholen, d. h., Barclays muss hinreichend belastbar sein. Barclays muss die Gewissheit bekommen und in der Lage sein, ihren Stakeholdern die Gewissheit zu geben, dass der Dienst für den Fall des Auftretens von Störungen so konzipiert ist, dass deren Auswirkungen (ob nun auf die Kunden, finanzielle und/oder die Reputation betreffende Auswirkungen) minimiert werden.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
	▪ Datenverlustszenario, einschließlich Cybervorfällen und der möglichen Auswirkungen auf die Erbringung von Dienstleistungen für Barclays. ▪ Verlust von Personalressourcen, die die Erbringung der vereinbarten Service-Level beeinträchtigen würden (Pandemieereignis, geopolitisches Ereignis, kritischer nationaler Infrastrukturausfall usw.). ▪ Verlust von Technologieservices (Verlust von Rechenzentren oder Region des Cloud-Serviceanbieters). ▪ Verlust von wesentlichen Unterauftragnehmern (Dienste oder Lieferungen). Störungsereignisse sind jährlich und kontinuierlich zu überprüfen, damit die Planungs- und Testteams informiert werden und die Entwicklung über einen bestimmten Zeitraum gezeigt werden kann.	
3. Anforderungen an Wiederherstellungsplanung und Validierung	Der Lieferant muss Wiederherstellungspläne für die vereinbarten Störungsereignisse pflegen. In den Wiederherstellungsplänen muss Folgendes dokumentiert sein: die detaillierten Schritte zur Wiederherstellung und die Reaktion des Lieferanten, die möglich ist, um die Auswirkungen zu reduzieren und/oder die Nichtverfügbarkeit der für Barclays erbrachten Dienste abzuwenden. Dabei sollte mindestens Folgendes berücksichtigt werden: ▪ Mögliche Problemumgehungen (Workarounds) ▪ Entscheidungsprotokolle ▪ Kommunikations- und Geschäftspriorisierung, um ein Mindestmaß an funktionsfähigem Service wiederaufzunehmen/aufrechtzuerhalten ▪ Abhängigkeiten Wiederherstellungspläne müssen alle 12 Monate oder bei wesentlichen Änderungen getestet und validiert werden, um nachzuweisen, dass die vereinbarten Service-Levels erfüllt werden können und dass die Dienste den von Barclays vorgeschriebenen Anforderungen laut Belastbarkeitskategorie entsprechen. Erfüllt der Plan die vereinbarten Service-Levels oder anwendbaren Anforderungen laut Belastbarkeitskategorie nicht, muss der Lieferant Barclays umgehend	Test- und Validierungsarbeiten werden durchgeführt, um Barclays die Gewissheit zu geben, dass die Konzeption der Dienstleistungen und die Planung (einschließlich aller Abhängigkeiten) bestimmungsgemäß funktionieren und um nachzuweisen, dass die vereinbarten Service-Levels erfüllt werden können und dass die Dienstleistungen den von Barclays vorgeschriebenen Belastbarkeitsanforderungen entsprechen.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
	benachrichtigen (in der Regel innerhalb von 10 Tagen) und detaillierte Abhilfepläne (einschließlich der zu ergreifenden Maßnahmen und der entsprechenden Termine für die Fertigstellung) vorlegen.	
4. Anforderungen an integrierte Tests	Um sicherzustellen, dass die wechselseitigen Abhängigkeiten zwischen Barclays und den Lieferantendiensten in Bezug auf die Dienstwiederherstellung verstanden werden, muss der Lieferant auf Verlangen von Barclays und zu einem gemeinsam vereinbarten Termin an einem integrierten Test teilnehmen, um die gemeinsame Belastbarkeit/Kontinuität des Lieferanten und von Barclays zu validieren. Sofern frühere integrierte Tests keine wesentlichen Mängel gezeigt haben bzw. kein Vorfall eingetreten ist, der eine Unterbrechung der Services verursacht hat, stellt Barclays diese Anfrage maximal einmal alle 2 Jahre.	Gemeinsame Übungen helfen zu gewährleisten, dass angemessene Protokolle zur Wiederherstellungsplanung vorliegen, effektive Kommunikationsstrategien übernommen wurden und sowohl der Lieferant als auch Barclays einen koordinierten Ansatz verfolgen, um Geschäftsunterbrechungen zu handhaben und die Auswirkungen auf die Kunden von Barclays sowie das Finanzsystem im Allgemeinen zu minimieren.
5. Anforderungen an Systemwiederherstellungspläne und Validierung	Der Lieferant muss über einen Systemwiederherstellungsplan verfügen, in dem die erforderlichen Maßnahmen zur Wiederherstellung der Systeme nach einer Störung aufgeführt sind. Die Pläne müssen getestet und validiert werden, um (mit Nachweis) zu zeigen, dass das System innerhalb der definierten RTOs (Recovery Time Objectives, Zielvorgaben für die Wiederherstellungszeit) und RPOs (Recovery Point Objectives, Zielvorgaben für den Wiederherstellungspunkt) wiederhergestellt werden kann, wie von der definierten Belastbarkeitskategorie gefordert. Bei Systemen, die in einer aktiven/passiven Konfiguration ausgelegt sind, muss die passive Umgebung aktiviert und lange genug als BAU-Produktionsumgebung genutzt werden, um die Kapazität und vollständige Integrationsfunktionalität zu belegen. Bei Diensten, die als aktiv/aktiv ausgelegt sind, muss die Validierung den fortgesetzten Betrieb bei Verlust eines Knotens, einer Instanz oder einer Verfügbarkeitszone (für in der Cloud gehostete Dienste) des Systems nachweisen (mindestens 60 Minuten). Die Anforderungen an die Validierungshäufigkeit werden durch die Belastbarkeitskategorie für das System definiert. Siehe oben stehende Matrix der Belastbarkeitskritikalität:	Fehlende oder unzulängliche Systemwiederherstellungspläne können zu nicht hinnehmbaren Ausfällen von Technologie-Diensten für Barclays oder seine Kunden nach einem Vorfall führen. Wenn die Dokumentation zur Belastbarkeit auf dem aktuellen Stand gehalten wird und Übungen dazu durchgeführt werden, entsprechen die Wiederherstellungspläne auch weiterhin den geschäftlichen Bedürfnissen.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
6. Anforderungen an Datenwiederherstellungspläne und Validierung	Der Lieferant muss für jedes Technologiesystem, das zur Erbringung von Diensten für Barclays erforderlich ist, über Datenwiederherstellungspläne verfügen. Pläne müssen mindestens alle 12 Monate oder bei wesentlichen Änderungen auf ihre Richtigkeit überprüft werden und sollten mindestens Folgendes berücksichtigen: ▪ Datenquellen und Datenfluss (vor- und nachgelagert) ▪ Backup- und Replikationsquellen ▪ Anforderungen für die Datensynchronisierung nach der Wiederherstellung Der Lieferant muss die Datenwiederherstellungspläne für jedes Technologiesystem, das zur Erbringung von Diensten für Barclays erforderlich ist, testen und validieren, und er muss (mit Nachweis) belegen, dass durch den Wiederherstellungsprozess Daten in den erwarteten Betriebszustand innerhalb des erforderlichen RPO (Recovery Point Objective) zurückversetzt werden können.	Datenverlust zählt zu den größten Gefahren, denen Barclays ausgesetzt ist. Böswillige Aktivitäten oder Systemausfälle können hierfür der Auslöser sein. Ein entsprechender Plan für solche Szenarien ist wichtig und hilft, Datenquellen und Abhängigkeiten zu ermitteln und zu verstehen.
7. Anforderungen an Vielfalt der Datenzentren und Cloud-Serviceprovider	Der Lieferant muss sicherstellen, dass alle Technologiesysteme, die zur Erbringung von Diensten für Barclays benötigt werden, über die entsprechenden Datenzentren hinweg belastbar und geografisch weit genug voneinander entfernt sind, um das Risiko zu verringern, dass mehrere Datenzentren gleichzeitig von einem einzelnen Vorfall betroffen sind. Wenn das Technologiesystem bei einem Cloud-Serviceanbieter gehostet wird, muss es in verschiedenen Verfügbarkeitszonen verfügbar sein, um die Folgen eines Ausfalls in einer Zone abzuschwächen. Kritische Systeme sind erforderlich, um die Fähigkeit zur Wiederherstellung nach einem Ausfall der Region des Cloud-Serviceanbieters nachzuweisen.	Technologiesysteme sollten zum Schutz vor dem Ausfall eines Rechenzentrums in mehreren Rechenzentren eingesetzt werden. Dies gilt auch für Systeme, die bei Cloud-Serviceprovidern gehostet werden; diese sollten über mehrere CSP-Regionen hinweg bereitgestellt werden.
8. Anforderungen an Pläne zur Neuerstellung von Plattformen und Anwendungen	Der Lieferant muss einen Plan für die Neuerstellung von Plattformen und Anwendungen für jedes Technologiesystem erstellen, das zur Erbringung von Diensten für Barclays erforderlich ist. Mindestens alle 12 Monate oder bei	Es ist von entscheidendem Stellenwert, dass für Technologiedienste und Supportvereinbarungen angemessene Wiederherstellungspläne im Falle eines Cyber-/Datenintegritätsereignisses vorliegen.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
	wesentlichen Änderungen ist eine Prüfung, Genehmigung und ein Test erforderlich. Diese Pläne sind für Situationen vorgesehen, in denen herkömmliche Wiederherstellung/Restore-Optionen nicht verwendet werden können und das System von Grund auf neu aufgebaut werden muss. Die Pläne müssen Folgendes berücksichtigen: ▪ Betriebssystem-/Infrastruktursoftware ▪ Anwendungsbereitstellung und -konfiguration ▪ Sicherheitskontrollen/-konfiguration ▪ Abhängigkeiten des Systemökosystems und Reintegration ▪ Datenanforderungen (Datenwiederherstellungsplan) ▪ Tooling-Abhängigkeiten zur Ausführung von WiederherstellungsPlänen	