Kontrollpflichten externer Lieferanten

Wiederherstellungsplanung

Version 12.0, Oktober 2022

1. Definitionen:

„Krise“	ist ein störendes oder sich auf die Reputation auswirkendes Ereignis, das eine über die normale geschäftsübliche Struktur und/oder die normalen geschäftsüblichen Ressourcen hinausgehende Reaktion verlangt und es erforderlich macht, dass zu Entscheidungs- und Koordinationszwecken von leitender Ebene eingegriffen wird.
„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.
„Production Crossover“	Production Crossover ist ein Begriff, der verwendet wird, wenn ein Technologiesystem auf eine alternative Umgebung (DR) umgestellt und für die Ausführung von Produktionsfunktionen über einen längeren Zeitraum verwendet wird.
„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 verwendet wird, um Anforderungen an die Belastbarkeit auf einen Service anzuwenden. Dazu gehören RTO, RPO, Validierungsanforderungen und Häufigkeit.

2. Matrix der Belastbarkeitskritikalität:

Die Dienste des Lieferanten werden von Barclays einer spezifischen Belastbarkeitskategorie (0-4) zugeordnet. 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 Services vorgeschriebene Belastbarkeitskategorie die nachstehend festgelegte Zielvorgabe für die Wiederherstellungszeit (Wiederherstellung Time Objective, RTO) und den Wiederherstellungspunkt (Recovery Point Objective, RPO) erfüllen:

		Bewertung von Risikoauswirkungen	Außergewöhnliche Auswirkung	Hohe Auswirkung	Mäßige Auswirkung	Geringe Auswirkung	Unerhebliche Auswirkung
		Belastbarkeitskategorie	0	1	2	3	4
		Belastbarkeitsart	Kontinuierlich	Sehr belastbar	Belastbar	Wiederherstellen	Unterbrechen/Nur Backup
Störungsereignis	Anwendung	RTO-Ziel (Nicht-Daten-/Cyber-Ereignisse)	bis zu 1 Stunde	bis zu 4 Stunden	bis zu 12 Stunden	bis zu 24 Stunden	Keine geplante Wiederherstellung
		RPO-Ziel (nicht-Daten-/Cyber-Ereignisse)	bis zu 5 Minuten	bis zu 15 Minuten	bis zu 30 Minuten	bis zu 24 Stunden	Keine geplante Wiederherstellung

3. Kontrollen:

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Störende Ereignisse – Anforderungen an die Wiederherstellungsplanung	Barclays schreibt die Belastbarkeitskategorie für die in Auftrag gegebenen Dienste vor. 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. Die Störungsereignisplanung sollte mindestens Folgendes berücksichtigen: ▪ Beeinträchtigung der Erbringung von Services für Barclays durch den Verlust von Gebäuden an mehreren Standorten (Gebäude und zugehörige Infrastruktur sind nicht verfügbar). ▪ 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 (z. B. Pandemieereignis, geopolitisches Ereignis, kritischer nationaler Infrastrukturausfall usw.). ▪ Verlust von Technologieservices (d. h. Verlust von Rechenzentren oder Cloud Service Provider, die sich auf alle Technologieservices auswirken). ▪ Verlust von wesentlichen Unterauftragnehmern (Dienstleistungen oder Warenvorräte).	Für Barclays ist es aus betriebswirtschaftlicher (und risikoorientierter) Sicht erforderlich, erhebliche störende Ereignisse 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
	Störungsereignisse müssen jährlich und kontinuierlich überprüft werden, um die Planungs- und Testteams zu informieren und um zu zeigen, wie sich dies im Laufe der Zeit entwickelt. Der Lieferant muss nachweisen können, dass eine Vielzahl von Schweregradfaktoren berücksichtigt, getestet und validiert wurde.	
2. 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 müssen alle 12 Monate gepflegt und überprüft werden. Zu den zu berücksichtigenden Abhängigkeiten gehören: ▪ Technologie und Daten (intern und von Unterauftragnehmern zur Verfügung gestellt). ▪ Wesentliche(r) Unterauftragnehmer (diejenigen, die für die Erbringung von Dienstleistungen für Barclays von entscheidender Bedeutung sind) ▪ 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 ihren Business-WiederherstellungsPlänen aufzunehmen, um sicherzustellen, dass diese berücksichtigt werden, um die Auswirkungen von Vorfällen zu reduzieren und die Nichtverfügbarkeit der Dienstleistung(en) gegenüber Barclays zu verhindern.
3. Validierung der Anforderungen an die Wiederherstellungsplanung	Der Lieferant muss Business-Recovery-Pläne für die vereinbarten Störungsereignisse pflegen. In den Business-Recovery-Plänen sollten 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 Services abzuwenden. Dabei sollte mindestens Folgendes berücksichtigt werden: ▪ Mögliche Problemumgehungen (Workarounds) ▪ Entscheidungsprotokolle ▪ Kommunikations- und Geschäftspriorisierung, um ein Mindestmaß an funktionsfähigem Service wiederaufzunehmen/aufrechtzuerhalten	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

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
	▪ Abhängigkeiten Wiederherstellungspläne müssen alle 12 Monate getestet und validiert werden, um nachzuweisen, dass vereinbarte Service-Levels erbracht werden können und dass die Dienstleistungen die von Barclays festgelegten Anforderungen laut Belastbarkeitskategorie erfüllen. Erfüllt der Plan die vereinbarten Service-Levels oder zutreffenden Anforderungen laut Belastbarkeitskategorie nicht, muss der Lieferant Barclays umgehend benachrichtigen und detaillierte Abhilfepläne (einschließlich der zu ergreifenden Maßnahmen und der entsprechenden Termine für deren Fertigstellung) vorlegen.	von Barclays vorgeschriebenen Belastbarkeitsanforderungen entsprechen.
4. Integrierte Prüfung	Belastbarkeitskategorie 0–1 Auf Verlangen von Barclays muss der Lieferant an einem gegenseitig vereinbarten Termin an einer integrierten Prüfung teilnehmen, um die gemeinsame Belastbarkeit/Kontinuität des Lieferanten und 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. Systemwiederherstellungspläne	Der Lieferant muss für alle benötigten Technologie-Systeme/-Dienste, die zur Unterstützung der Erbringung von Services für Barclays und der Wiederherstellungszeit (RTO) und den Wiederherstellungspunkt (RPO) benötigt werden, einen oder mehrere Systemwiederherstellungspläne (SRP) besitzen. Der Plan muss/die Pläne müssen mindestens einmal alle 12 Monate auf Genauigkeit überprüft werden.	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. Datenwiederherstellungspläne	Ausfallsicherheit Kategorie 0-1 Der Lieferant muss für jedes Technologiesystem/jeden Service, der zur Unterstützung der Erbringung von Services für Barclays erforderlich ist, über Datenwiederherstellungspläne verfügen. Pläne müssen mindestens alle 12 Monate 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	Datenverlust zählt zu den größten Bedrohungen, denen wir gegenüberstehen. 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. Vielfalt der Datenzentren	Der Lieferant muss sicherstellen, dass alle Technologie-Systeme/-Dienste, die zur Unterstützung der Erbringung von Services für Barclays benötigt werden, über die entsprechenden Datenzentren hinweg belastbar und weit genug voneinander entfernt sind, um das Risiko zu verringern, dass mehrere Datenzentren gleichzeitig von einem einzelnen Vorfall betroffen sind. Wenn das Technologiesystem auf einem Cloud-Serviceprovider gehostet wird, sollte der Service in verschiedenen Verfügbarkeitszonen verfügbar sein, um einen AZ-Ausfall zu vermeiden. ResCat 0-1-Services sollten in allen Cloud-Regionen ausfallsicher sein.	Die Datenzentren sollten über alternative Stromquellen, Netzwerkverbindungen usw. verfügen und weit genug voneinander entfernt sein, um das Risiko zu verringern, dass mehrere Datenzentren gleichzeitig von einem einzelnen Ereignis betroffen sind.
8. Validierung von Systemwiederherstellungsplänen	Der Lieferant muss die Systemwiederherstellungspläne testen und validieren, um nachzuweisen, dass das Technologiesystem / die Services wiederhergestellt werden können und das Recovery Time Objective und Recovery Point Objective gemäß der Resilience Criticality Matrix erfüllen. Für alle Technologie-Systeme/-Dienste, die zur Unterstützung der Erbringung von Diensten der Belastbarkeitskategorie 0–1 benötigt werden und die in einer aktiven/passiven Konfiguration auf Belastbarkeitsmaßnahmen ausgelegt sind, muss die passive Umgebung gemäß dokumentiertem Systemwiederherstellungsplan aktiviert und lange genug als BAU-Produktionsumgebung genutzt werden, um die Kapazität und vollständige Integrationsfunktionalität (Produktionsübergang) zu belegen. Bei Services, die als aktiv/aktiv ausgelegt sind, muss die Validierung den fortgesetzten Betrieb unter dem Verlust einer aktiven Umgebung nachweisen (Szenario mit reduzierten Verarbeitungsressourcen).	Von Drittanbietern zur Verfügung gestellte Technologiesysteme können sich auf die Barclays-Kundenbetreuung auswirken. Die Gewährleistung, dass Drittanbieter, welche die betrieblichen Abläufe bei Barclays unterstützen, über hinreichende, geprüfte Belastbarkeitspläne verfügen, ist für Barclays entscheidend und zudem eine gesetzliche Vorgabe, um bei der Betreuung unserer Kunden ordnungsgemäße Kontrolle walten zu lassen. Beim Produktionsübergang (PCO) handelt es sich um eine Methode zur Validierung, dass die passive Instanz eines aktiv-passiv konfigurierten Systems wie erwartet und mit einer Kapazität arbeitet, wie sie im BAU-Betrieb nötig ist. Darüber hinaus validiert ein PCO auch, dass

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
	Die Validierungshäufigkeitsanforderungen müssen von der zugehörigen Belastbarkeitskategorie unterstützt werden, d. h.: - Belastbarkeitskategorie 0: Die SRP-Validierung muss mindestens viermal pro Jahr via PCO durchgeführt werden. - Belastbarkeitskategorie 1: Die SRP- und PCO-Validierung muss mindestens zweimal jährlich via PCO durchgeführt werden. - Belastbarkeitskategorie 2: Die SRP-Validierung muss mindestens alle 12 Monate durchgeführt werden; - Belastbarkeitskategorie 3: Die SRP-Validierung muss mindestens alle 24 Monate durchgeführt werden; Erfüllt ein Plan die Mindestwiederherstellungsanforderungen für die entsprechende Belastbarkeitskategorie nicht, muss der Lieferant Barclays umgehend benachrichtigen und detaillierte Abhilfepläne (einschließlich der zu ergreifenden Maßnahmen und der entsprechenden Termine für die Fertigstellung) vorlegen.	jedwede Abhängigkeit von vorgelagerten oder nachgelagerten Systemen weiter wie erwartet funktioniert.
9. Validierung des Datenwiederherstellungsplans	Belastbarkeit der Kategorie 0-1 Der Lieferant muss die Datenwiederherstellungspläne für jedes Technologiesystem/jeden Service testen und validieren, die zur Unterstützung der Erbringung von Services für Barclays erforderlich sind, und nachweisen, dass der Wiederherstellungsprozess Daten in den Betriebszustand zurückversetzen kann. Diese Validierung sollte mindestens alle 12 Monate erfolgen. Erfüllt ein Plan die Mindestwiederherstellungsanforderungen für die entsprechende Belastbarkeitskategorie nicht, muss der Lieferant Barclays umgehend benachrichtigen und detaillierte Abhilfepläne (einschließlich der zu ergreifenden Maßnahmen und der entsprechenden Termine für die Fertigstellung) vorlegen.	Daten sind ein kritisches Element, das auf vielerlei Weise beeinträchtigt werden kann. Der dokumentierte Plan zur Zurückgewinnung, Wiederherstellung oder Neuerstellung von Daten muss geprobt werden, um seine Genauigkeit und Tragfähigkeit zu bestätigen.
10. Pläne zur Neuerstellung von Plattformen und Anwendungen	Resilienz Kategorie 0-1 Der Lieferant muss einen Plan für die Neuerstellung von Plattformen und Anwendungen für jeden Technologiedienst / jedes Technologiesystem erstellen, der zur Unterstützung der Bereitstellung von Services für Barclays erforderlich ist und der mindestens alle 12 Monate einer Prüfung, Genehmigung und Tests unterzogen werden muss.	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
	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 Erfüllt ein Plan die Mindestwiederherstellungsanforderungen für die entsprechende Belastbarkeitskategorie nicht, muss der Lieferant Barclays umgehend benachrichtigen und detaillierte Abhilfepläne (einschließlich der zu ergreifenden Maßnahmen und der entsprechenden Termine für die Fertigstellung) vorlegen.	