External Supplier Control Obligations

Wiederherstellungsplanung

Version 11.0, Oktober 2021

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.
„Vorfall“	ist ein störendes Ereignis, das im Rahmen des Tagesgeschäfts bewältigt werden kann, indem Wiederherstellungspläne aufgerufen werden.
„Wiederherstellungsplanung“	Der Prozess oder die Planung für die Wiederherstellung von Unternehmensdienstleistungen, Geschäftsprozessen und den zugrunde liegenden Abhängigkeiten
„Störungsereignis“	Ein Verzeichnis mit den Auswirkungen von Vorfällen, unabhängig von der Ursache, die Lieferanten mittels Implementierung von Wiederherstellungs- und Belastbarkeitsplanung und -kompetenzen reduzieren wollen.
„Zielvorgabe für die Wiederherstellungszeit“	ist die Zeit zwischen einem unerwarteten Ausfall oder einer unerwarteten Unterbrechung von Diensten und der Wiederaufnahme des Betriebs.

2. 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 Planung 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 Kategorien von Störungsereignissen sollten mindestens Folgendes berücksichtigen: ▪ Ausfall von Gebäuden an mehreren Standorten, die dadurch den Geschäftsbetrieb nicht mehr unterstützen können; ▪ Datenverlustszenario, einschließlich Cybervorfällen und der möglichen Auswirkungen auf die Erbringung von Dienstleistungen für Barclays. Ausfall von Mitarbeiterressourcen, der sich auf die Erbringung der vereinbarten Service-Levels auswirken würde;	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
	▪ Nichtverfügbarkeit von Dienstleistungen für Barclays aufgrund potenzieller Cyber-/Nicht-Cyber-Vorfälle und der möglichen Auswirkungen auf die Erbringung von Dienstleistungen für Barclays; ▪ Einzelne und gleichzeitige Wiederherstellung von Technologiediensten (z. B. bei Ausfall des Rechenzentrums) 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 der Dienstleistung Barclays gegenüber entscheidend sind, um sicherzustellen, dass diese für den Lieferanten gleichermaßen belastbar sind. Diese Abhängigkeiten müssen alle 12 Monate gepflegt und überprüft werden. Zu den zu berücksichtigenden Abhängigkeiten gehören: ▪ Ausfall/Verlust aller Technologien und Daten ▪ Nichtverfügbarkeit von Dienstleistungen wesentlicher Subunternehmen (diejenigen, die für die Erbringung von Dienstleistungen gegenüber 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) Diese müssen im Rahmen des Business-Recovery-Plans getestet und validiert werden, um zu zeigen, dass die Dienstleistungen die von Barclays festgelegten Anforderungen laut Belastbarkeitskategorie erfüllen, um sicherzustellen, dass diese gleichermaßen belastbar sind und die erforderlichen Service-Levels erfüllen.	Dienstleister müssen die Abhängigkeiten bei der Bereitstellung ihrer Dienstleistungen für Barclays verstehen. Alle Abhängigkeiten sind in ihren Business-Recovery-Plänen aufzunehmen, um sicherzustellen, dass diese berücksichtigt werden, um die Auswirkungen von Vorfällen zu reduzieren und die Nichtverfügbarkeit der Dienstleistung(en) gegenüber Barclays zu verhindern.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
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 bereitgestellten Dienstleistung 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 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.	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.
4. Integrierte Prüfung	Auf Verlangen von Barclays muss der Lieferant an einer integrierten Prüfung teilnehmen, um die gemeinsame Belastbarkeit/Kontinuität des Lieferanten und Barclays zu validieren.	Gemeinsame Übungen helfen zu gewährleisten, dass angemessene Protokolle zur Wiederherstellungsplanung vorliegen, effektive Kommunikationsstrategien übernommen wurden und sowohl der Lieferant als auch Barclays einen

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
	Sofern frühere integrierte Tests keine wesentlichen Mängel gezeigt haben bzw. keine wesentlichen Änderungen an den Diensten vorgenommen wurden, stellt Barclays diese Anfrage maximal einmal alle 2 Jahre.	koordinierten Ansatz verfolgen, um Geschäftsunterbrechungen zu handhaben und die Auswirkungen auf die Kunden von Barclays sowie das Finanzsystem im Allgemeinen zu minimieren.
5. Verfahren für das Vorfall-/Krisenmanagement	Beim Lieferanten muss es ein dokumentiertes Verfahren für das Vorfall- und Krisenmanagement geben, das unter anderem den Prozess zur Eskalation von Vorfällen/Krisen an Barclays beinhaltet. Verfahren für das Vorfall- und Krisenmanagement müssen nach den vom Lieferanten alle 12 Monate vorzunehmenden erfolgreichen Test- und Validierungsarbeiten genehmigt werden. In dem Verfahren müssen die für das Management und die Handhabung des Vorfalls bzw. der Krise vom Beginn des Lebenszyklus bis hin zum Abschluss minimal erforderlichen Aktivitäten und Ergebnisse definiert sein. Der Lieferant benennt folgende Personen: (i) eine Einzelperson als die genehmigende Person für das Verfahren, die dafür verantwortlich ist, zu bestätigen, dass das Verfahren für seinen Zweck geeignet ist; (ii) einen Hauptansprechpartner und einen Stellvertreter (im Fall der Abwesenheit des Hauptansprechpartners) für jede Funktion bei Krisen.	Beim Lieferanten muss Klarheit über seine Verfahren für die Handhabung und Verwaltung seiner Dienste bei einem Vorfall oder einer Krise herrschen. Der Lieferant und Barclays müssen ein gemeinsames Verständnis des Eskalationsprozesses bei Vorfall- und Krisensituationen haben. Test- und Validierungsarbeiten werden durchgeführt, um sicherzustellen, dass die betreffende Einzelperson bzw. das betreffende Team über hinreichend Fähigkeiten, Kenntnisse und eine ausreichende Organisation zum Management von Vorfällen und Krisen verfügt, sofern und sobald diese eintreten.
6. Nachbereitende Berichterstattung zu einem Vorfall/einer Krise	Nach einer Störung des Dienstes ist Barclays innerhalb von vier Kalenderwochen nach Wiedereinsetzung des Dienstes in den normalen Betriebszustand ein nachbereitender Bericht zu dem Vorfall/der Krise vorzulegen. Der Bericht muss mindestens einen Bericht zu Folgendem enthalten: ▪ Die Ursache des Vorfalls bzw. der Krise ▪ Abgeschlossene Abhilfemaßnahmen und alle sonstigen Maßnahmen zur kontinuierlichen Verbesserung, um ein erneutes Auftreten zu verhindern ▪ Jegliche Auswirkungen auf Kunden von Barclays, die dem Lieferanten bekannt sind	Die nachbereitende Berichterstattung zu einem Vorfall/einer Krise ist erforderlich, um Barclays die Gewissheit zu geben, dass Probleme rechtzeitig identifiziert/behoben und zeitnah Lehren daraus gezogen werden.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
7. Systemwiederherstellungspläne (System Recovery Plans; SRP)	Der Lieferant muss für alle benötigten Technologie-Systeme/-Dienste, die zur Unterstützung der Bereitstellung von Diensten der Barclays-Belastbarkeitskategorie 0–3 sowie der Erfüllung der entsprechenden Zielvorgaben für die 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. Hinweis: Für Technologie-Systeme/-Dienste der Belastbarkeitskategorie 0–1, die in einer aktiven/passiven Konfiguration auf Belastbarkeitsmaßnahmen ausgelegt sind, verlangt die Validierung des SRP, dass das System länger in der wiederhergestellten Umgebung verbleibt und als BAU fungiert, um sicherzustellen, dass alle Elemente effektiv arbeiten. Praktisch handelt es sich dabei um ein Produktionsübergangsereignis (PCO).	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.
8. Datenintegritätswiederherstellungspläne (Data Integrity Recovery Plans, DIRP)	Der Lieferant muss für alle Technologie-Systeme/-Dienste, die zur Unterstützung der Bereitstellung von Diensten der Barclays-Belastbarkeitskategorie 0–1 benötigt werden, einen oder mehrere Datenintegritätswiederherstellungspläne (DIRP) besitzen. Der Plan muss/die Pläne müssen mindestens einmal alle 12 Monate auf Richtigkeit überprüft werden.	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.
9. Vielfalt der Datenzentren	Der Lieferant muss sicherstellen, dass alle Technologie-Systeme/-Dienste, die zur Unterstützung der Bereitstellung von Diensten der Barclays-Belastbarkeitskategorie 0–3 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.	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.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
10. SRP-Validierung	Um nachzuweisen, dass das Technologiesystem/die Technologiedienste wiederhergestellt werden können, um den von Barclays vorgeschriebenen Anforderungen laut Belastbarkeitskategorie 0–3 zu entsprechen, muss der Lieferant den/die Systemwiederherstellungsplan/-pläne (SRP) testen und validieren. Für alle Technologie-Systeme/-Dienste, die zur Unterstützung der Bereitstellung 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 SRP aktiviert und lange genug als BAU-Produktionsumgebung genutzt werden, um die Kapazität und vollständige Integrationsfunktionalität (Produktionsübergang) zu belegen. 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 eine Prüfung 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. Der Lieferant muss Barclays informieren, bevor der PCO ausgeführt wird.	Von Drittanbietern bereitgestellte 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 jedwede Abhängigkeit von vorgelagerten oder nachgelagerten Systemen weiter wie erwartet funktioniert.
11. DIRP-Validierung	Um die Integrität der Daten während der Wiederherstellung nachzuweisen, muss der Lieferant den bzw. die Datenintegritätswiederherstellungspläne (DIRP) für alle Technologie-Systeme/-Dienste, die zur Unterstützung der Bereitstellung von Diensten der Barclays-Belastbarkeitskategorie 0–1	Daten sind ein kritisches Element, das auf vielerlei Weise beeinträchtigt werden kann. Der dokumentierte Plan zur Zurückgewinnung, Wiederherstellung oder Neuerstellung von Daten

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
	benötigt werden, testen und validieren. 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.	muss geprobt werden, um seine Genauigkeit und Tragfähigkeit zu bestätigen.
12. Pläne zur Neuerstellung/Neuplanung von Plattformen und Anwendungen	Zur Unterstützung der Wiederherstellung nach Störungsereignissen wie z. B. einem Cyber-Exploit muss der Lieferant für jeden Technologiedienst/jedes Technologiesystem, der bzw. das zur Unterstützung der Erbringung von Dienstleistungen gemäß der Barclays-Belastbarkeitskategorie 0–1 erforderlich ist, über einen Plan zur Neuerstellung/Neuplanung von Plattformen und Anwendungen verfügen. Ferner sind Prüfung, Genehmigung und Tests mindestens einmal alle 12 Monate erforderlich. 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.	Für Technologiedienste und Supportvereinbarungen liegen angemessene Wiederherstellungspläne im Falle eines Cyber-/Datenintegritätsereignisses vor.

3. 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 vorgeschriebene Belastbarkeitskategorie die nachstehend festgelegte Zielvorgabe für die Wiederherstellungszeit (Recovery Time Objective, RTO) erfüllen:

		ERMF - Risk Impact Assessment	Exceptional Impact	High Impact	Moderate Impact	Low Impact	Insignificant Impact
		Resilience Category	0	1	2	3	4
		Resilience Type	Continuous	Highly Resilient	Resilient	Recover	Suspend / Backup Only
Disruption Event	Application	RTO for Application Recovery (non-data events)	Up to 1 hour	Up to 4 hours	Up to 12 hours	up to 24 hours	No planned recovery
		RPO	Up to 5 minutes	Up to 15 mins	Up to 30 mins	Up to 24 hours	No planned recovery