

# Kontrollpflichten externer Lieferanten Technologierisiko

Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Obsoleszenzmanagement	Sicherstellung fortlaufender Supportmaßnahmen	Der Lieferant muss Barclays bekannte Änderungen seiner direkten oder indirekten Fähigkeit zum Leisten von Support für IT-Ressourcen, die zum Erbringen von Diensten für Barclays verwendet werden, sofort anzeigen, unter anderem wenn Produkte Sicherheitsschwachstellen aufweisen, und er muss für die rechtzeitige Aufrüstung oder Aussonderung dieser IT-Ressourcen sorgen.	Wenn Unterlagen und/oder Verfahren für Hardware- und Software-Ressourcen, bei denen der Support endet, unzureichend sind, oder wenn Technologie-Dienste abhängig von veralteter Hardware oder Software werden, kann das zu einer inakzeptablen Leistung, zu Instabilität, Sicherheitsschwachstellen, Geschäftsverlusten und übermäßig hohen Migrationskosten führen.
2. Umgang mit Vorfällen	Erfassung, Einstufung und Klärung von Vorfällen	Der Lieferant muss ein System für den Umgang mit Vorfällen in Bezug auf den Betrieb seiner IT-Systeme und Dienste betreiben, mit dem sichergestellt wird, dass alle diese Vorfälle im Zusammenhang mit dem Betrieb angemessen identifiziert, erfasst, vorrangig behandelt, eingestuft und sofort geklärt werden, entweder beim ersten Kontakt oder durch zeitnahe und angemessene Eskalation. Dazu muss auch ein robuster Prozess für den sofortigen und effektiven Umgang mit bedeutenden Vorfällen gehören.	Infolge von Technologie-Vorfällen, die nicht rechtzeitig oder ohne hinreichende Detailangaben gemeldet werden oder bei denen die erforderlichen Korrekturmaßnahmen nicht ergriffen werden, kann es zu vermeidbaren Störungen von Systemen/Diensten oder zur Beschädigung oder zum Verlust von Daten kommen. Bedeutende Vorfälle erfordern eine intensivere und dringliche Reaktion, denn diese Vorfälle bergen ein erhebliches Risiko für das Geschäft und können ernste Folgen nach sich ziehen, unter anderem schwerwiegende Ausfälle, Reputationsverluste, finanzielle Auswirkungen und Auswirkungen auf zentrale Geschäftsprozesse.
3. Problemmanagement	Identifizierung, Bewertung/Analyse und Klärung von Technologie-Problemen	Der Lieferant muss ein System zur rechtzeitigen Untersuchung der zugrundeliegenden Probleme von erheblichen Technologie-Vorfällen betreiben, das für die Identifizierung und Erfassung dieser Probleme durch eine Analyse der Grundursachen und die effektive Klärung dieser Probleme sorgt, um die Wahrscheinlichkeit und die Auswirkungen eines wiederholten Auftretens dieser Vorfälle	Werden zugrundeliegende Probleme, durch die Vorfälle mit Auswirkungen auf die Bereitstellung von Technologie-Diensten verursacht werden, nicht zeitnah identifiziert und geklärt, können sie zu vermeidbaren Störungen von Systemen/Diensten oder zur Beschädigung oder zum Verlust von Daten führen.

		zu minimieren. Der Lieferant sollte zudem sicherstellen, dass eine proaktive Analyse routinemäßiger Vorfälle stattfindet, um die Ursache von häufigen, in großer Zahl auftretenden wiederholten Vorfällen zu identifizieren und zu klären.	
4. Änderungsmanagement	Durchsetzung einer rigorosen Änderungskontrolle	<p>Der Lieferant muss sicherstellen, dass sämtliche zum Erbringen von Diensten für Barclays verwendeten IT-Komponenten mit einer rigorosen Änderungskontrolle verwaltet werden, bei der folgende Ziele vollumfänglich berücksichtigt werden:</p> <ol style="list-style-type: none"> <li>1. Keine Änderung ohne entsprechende Autorisierung - Genehmigung muss vor der Umsetzung erfolgen</li> <li>2. Aufgabentrennung zwischen dem Initiator der Änderung, dem Verantwortlichen, der Person, die die Änderung genehmigt und der Person, die sie umsetzt</li> <li>3. Planung und Verwaltung von Änderungen je nach Stufe des damit verbundenen Risikos</li> <li>4. Hinreichende Berücksichtigung der potenziellen Auswirkungen von Änderungen auf die Leistung und/oder Fähigkeit von betroffenen Technologie-Komponenten</li> <li>5. Änderungen durchlaufen vor der Umsetzung die für sie relevanten technischen und betriebswirtschaftlichen Tests, unter Aufbewahrung der Nachweise, sofern erforderlich</li> <li>6. Änderungen müssen nach der Umsetzung getestet werden, um sicherzustellen, dass sie erfolgreich vorgenommen wurden, ohne dass es zu ungeplanten Auswirkungen gekommen ist</li> </ol>	Infolge von unzulänglichen Änderungsprozessen, mit denen unbefugte, unzureichend verwaltete oder unangemessene Änderungen an Technologie-Diensten verhindert werden, kann es zu Störungen des Dienstes, zur Beschädigung von Daten, zu Datenverlust, Verarbeitungsfehlern oder Betrug kommen.
5a. Technologie-Belastbarkeit	Systemwiederherstellungsplan (SRP)	Der Lieferant muss für alle benötigten Technologie-Systeme/-Dienste, die zur Unterstützung der Bereitstellung von Diensten der Barclays-Belastbarkeitskategorie	Fehlende oder unzulängliche Systemwiederherstellungspläne können zu nicht hinnehmbaren Ausfällen von Technologie-Diensten für das Unternehmen oder zum Verlust von Kunden nach einem Vorfall führen. Wenn die Dokumentation

		<p>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.</p> <p><b>Hinweis:</b> 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).</p>	zur Belastbarkeit auf dem aktuellen Stand gehalten wird und Übungen dazu durchgeführt werden, entsprechen die Wiederherstellungspläne auch weiterhin den geschäftlichen Bedürfnissen.
5b. Technologie-Belastbarkeit	Datenintegritätswiederherstellungsplan (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 Genauigkeit überprüft werden.	Datenverlust zählt zu den größten Bedrohungen, denen wir ausgesetzt sind, denn er kann durch böswillige Aktivitäten oder Systemausfälle geschehen. Ein entsprechender Plan für solche Szenarien ist wichtig und hilft, Datenquellen und Abhängigkeiten zu ermitteln und zu verstehen.
5c. Technologie-Belastbarkeit	Vielfalt der Datenzentren	Der Lieferant muss sicherstellen, dass alle Technologie-Systeme/-Dienste, die zur Unterstützung der Bereitstellung von Diensten der Barclays-Belastbarkeitskategorie	Die Datenzentren sollten über alternative Stromquellen, Netzwerkverbindungen usw. verfügen und weit genug voneinander entfernt sein, um das Risiko zu verringern, dass mehrere Datenzentren

		<p>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.</p>	<p>gleichzeitig von einem einzelnen Vorfall betroffen sind.</p>
<p>5d. Technologie-Belastbarkeit</p>	<p>SRP-Validierung</p>	<p>Um nachzuweisen, dass die Technologie-Systeme/-Dienste 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.</p> <p>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.</p> <p>Die Validierungshäufigkeitsanforderungen müssen von der zugehörigen Belastbarkeitskategorie unterstützt werden, d. h.:</p> <ul style="list-style-type: none"> <li>- Belastbarkeitskategorie 0: die SRP-Validierung muss alle 12 Monate und für PCO alle 3 Monate durchgeführt werden</li> <li>- Belastbarkeitskategorie 1: die SRP- und</li> </ul>	<p>Vom Lieferanten bereitgestellte Technologie-Systeme können sich auf die Barclays-Kundenbetreuung auswirken. Die Gewährleistung, dass Lieferanten, 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.</p> <p>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 <u>Abhängigkeit von vorgelagerten oder nachgelagerten Systemen</u> weiter wie erwartet funktioniert.</p>

		<p>PCO-Validierung muss alle 12 Monate durchgeführt werden</p> <p>- Belastbarkeitskategorie 2–3: die SRP-Validierung muss alle 24 Monate durchgeführt werden</p> <p>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.</p>	
5e. Technologie-Belastbarkeit	DIRP-Validierung	<p>Um die Integrität der Daten während der Wiederherstellung nachzuweisen, muss der Lieferant den/die Datenintegritätswiederherstellungspläne/-pläne (DIRP) für alle Technologie-Systeme/-Dienste, die zur Unterstützung der Bereitstellung von Diensten der Barclays-Belastbarkeitskategorie 0–1 benötigt werden, testen und validieren. Diese Validierung sollte alle 12 Monate erfolgen.</p> <p>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.</p>	Daten sind ein kritisches Element, das auf vielerlei Weise beeinträchtigt werden kann. Der dokumentierte Plan zur Zurückgewinnung, Wiederherstellung oder Neuerstellung von Daten muss geübt werden, um seine Genauigkeit und Tragfähigkeit zu bestätigen.
6. Leistungs- und Fähigkeitsmanagement	Den Technologiebedürfnissen von Barclays auch weiterhin entsprechen	Der Lieferant muss für sämtliche zum Erbringen von Diensten für Barclays verwendeten wichtigen IT-Komponenten geeignete Leistungs- und Fähigkeitsstufen definieren, die den erklärten geschäftlichen	Unzureichende oder versäumte Maßnahmen, mit denen die Leistung und/oder Fähigkeit von IT-Ressourcen überwacht und dafür gesorgt wird, dass sie auch weiterhin den aktuellen und künftigen Anforderungen entsprechen, können zu einem nicht

		Bedürfnissen entsprechen. Er muss zudem sicherstellen, dass bei wichtigen Komponenten angemessene Warnungen und Grenzwerte vorhanden sind, um auf potenzielle Überschreitungen von Grenzwerten hinzuweisen, und er muss dafür sorgen, dass sie regelmäßig überprüft werden, damit die Bereitstellung des Dienstes den Bedürfnissen von Barclays entspricht.	hinnehmbaren Abbau und/oder nicht hinnehmbaren Unterbrechungen von Technologie-Diensten und zu Geschäftsverlusten führen.  Die unzureichende Definition und/oder Dokumentation von Geschäfts-/Kundenbedürfnissen kann dazu führen, dass die Leistung von Technologie-Diensten nicht hinnehmbar wird und Geschäftsverluste eintreten.
Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
7. Entwicklung von Technologie-Anwendungen	Durchsetzung einer wiederholbaren Qualitätssicherung	Der Lieferant muss sicherstellen, dass sämtliche zur Bereitstellung von Diensten für Barclays verwendeten IT-Systeme und Dienste nachweislich rigorose, gründliche und wiederholbare Qualitätssicherungsprozesse durchlaufen haben, unter anderem Funktionstests und nicht funktionsbezogene Tests, statische Tests der Anwendungssicherheit sowie Code-Qualitätssicherung entweder durch Begutachtung (Peer Review) oder automatisierte Werkzeuge.	Infolge von unzureichend getesteten und qualitätsgesicherten Systemen und Diensten kann es zu unvorhersehbaren kritischen Verlusten von Funktionalität bei Technologie-Diensten und Geschäftsprozessen kommen.
	Akzeptanz des geschäftlichen Ergebnisses	Der Lieferant muss entweder einmalig oder laufend für beide Seiten akzeptable Festlegungen zum geschäftlichen Ergebnis vereinbaren, nach denen neue oder aktualisierte Versionen von IT-Systemen und Diensten an Barclays bereitgestellt und von Barclays akzeptiert werden.  Diese Festlegungen müssen in einer solchen Form getroffen werden, dass unter anderem ausreichend funktionsbezogene und nicht funktionsbezogene Aspekte der Systeme und	Werden unzureichende Vereinbarungen zum Funktionsverhalten und zum nicht funktionsbezogenen Verhalten von Systemen getroffen, kann es zu Abweichungen vom erwarteten Verhalten bei Barclays-Systemen kommen und in der Folge entsteht ein Risiko für Geschäfts- und Betriebsprozesse.

		<p>Dienste darin enthalten sind, und sie können jegliche angemessene und von beiden Seiten vereinbarte Form aufweisen, z. B. bestehende Systemhandbücher, detaillierte von beiden Seiten vereinbarte Anforderungsdokumente, Software-Anforderungen aus Anwendersicht (User Stories), Anwendungsfälle oder jegliche andere angemessene Form.</p> <p>Der Lieferant muss in Zusammenarbeit mit Barclays sicherstellen, dass geschäftliche Ergebnisse entweder ganz oder in von beiden Seiten vereinbarten Teilen einmalig oder laufend auf Grundlage der von Barclays erklärten geschäftlichen Akzeptanz dieser zuvor vereinbarten Festlegungen angenommen werden.</p>	
8. Backup-Maßnahmen für Systeme und Daten	Durchführung von angemessenen und effektiven Backup- und Wiederherstellungsprozessen	Der Lieferant muss sicherstellen, dass bei sämtlichen zum Erbringen von Leistungen für Barclays verwendeten IT-Systemen und Diensten hinreichende Backup- und Wiederherstellungsprozesse vorhanden sind, die entsprechend den Bedürfnissen von Barclays ablaufen und deren Effektivität in regelmäßigen Abständen nachgewiesen wird.	Infolge fehlender oder schlecht kontrollierter Backups von Geschäftsdaten kann es zu Störungen von Systemen/Diensten, Datenverlust oder unangemessener Offenlegung von Daten kommen.
	Gewährleistung des Schutzes, der Sicherheit und Zuverlässigkeit von Backup-Speichermedien	Der Lieferant muss sicherstellen, dass sämtliche im Zusammenhang mit der Erbringung von Leistungen für Barclays stehenden Backup-Speichermedien sowie die Maßnahmen für die Handhabung und Aufbewahrung dieser Speichermedien immer sicher und zuverlässig sind und bleiben.	Infolge fehlender oder schlecht kontrollierter Backups von Geschäftsdaten kann es zu Störungen von Systemen/Diensten, Datenverlust oder unangemessener Offenlegung von Daten kommen.
9. Konfigurationsmanagement	Isolierung der Produktionsumgebung	Der Lieferant muss sicherstellen, dass bei Produktionsdiensten, die für Barclays erbracht werden, keine Abhängigkeiten von produktionsfremden Komponenten bestehen, so dass sich eine unsichere oder	Unangemessene Verzeichniseintragungen zu Technologie-Komponenten (Hardware und Software), einschließlich Festlegungen für Zuständigkeiten und Abhängigkeiten von Dritten, können dazu führen, dass Dienste und Daten unsicher oder unzuverlässig werden. Werden produktionsfremde Komponenten

		unzuverlässige Bereitstellung von Diensten vermeiden lässt.	bei der Bereitstellung von Produktionsdiensten verwendet, entsteht ein Risiko dahingehend, dass sie möglicherweise nicht nach den Produktionsstandards erstellt oder verwaltet werden.
	Erfassung und Pflege von Konfigurationsdetails	Der Lieferant muss vollständige und genaue Verzeichniseintragungen in Bezug auf sämtliche im Umfang enthaltenen Konfigurationselemente pflegen, die bei der Erbringung von Diensten für Barclays verwendet werden (einschließlich der Zuständigkeiten und der vorgelagerten/nachgelagerten Abhängigkeiten/Zuordnungen). Der Lieferant muss Kontrollmechanismen bereithalten, welche die fortlaufende Pflege der Genauigkeit und Vollständigkeit der Daten sicherstellen.	Unangemessene oder unvollständige Verzeichniseintragungen (zusammen mit den damit verbundenen Abhängigkeiten/Zuordnungen von bzw. zu anderen Konfigurationselementen) können dazu führen, dass Dienste und Daten bedingt durch ineffektive Folgenabschätzungen von Vorfällen und Änderungen unsicher oder instabil werden.
10. Hardware-Ressourcenmanagement	Erfassung und Pflege von Details zu Hardware-Ressourcen	Der Lieferant muss Kontrollmechanismen bereithalten, welche die Erfassung und fortlaufende Pflege von Hardware-Ressourcen während ihres gesamten Lebenszyklus sicherstellen.  Der Lieferant muss vollständige und genaue Verzeichniseintragungen in Bezug auf sämtliche IT-Hardware-Ressourcen pflegen, die bei der Erbringung von Diensten für Barclays verwendet werden.	Unangemessene Verzeichniseintragungen zu Technologie-Hardware-Ressourcen, einschließlich Festlegungen für Zuständigkeiten und Abhängigkeiten von Dritten, können dazu führen, dass Dienste und Daten unsicher oder unzuverlässig werden. Werden Hardware-Ressourcen nicht sicher bereinigt und entsorgt, können finanzielle, die Reputation betreffende und behördliche Schäden entstehen.
	Ressourcenentsorgung	Sämtliche entsorgten Ressourcen müssen vollumfänglich von allen Barclays-Daten bereinigt sein und ihre Entsorgung muss über einen formellen Entsorgungsprozess erfolgen, der im Einklang mit den Anforderungen der relevanten Sicherheitsstandards von Barclays steht.	Wichtig ist, dass der Lieferant eine formelle Bestätigung einholt, dass die Ressourcen ordnungsgemäß entsorgt wurden (einschließlich der sicheren Vernichtung von Bankdaten). Werden Hardware-Ressourcen nicht sicher bereinigt und entsorgt, können finanzielle, die Reputation betreffende und behördliche Schäden entstehen.

	Vermisste Ressourcen	Jeder Verlust oder Diebstahl von Ressourcen muss ordnungsgemäß untersucht und Barclays zur Risikofreizeichnung bei Nichtwiederfinden gemeldet werden.	Wichtig ist, dass der Lieferant Kontrollmechanismen bereithält, um sicherzustellen, dass vermisste Ressourcen gründlich untersucht und – falls nicht wiedergefunden – Barclays zur Risikofreizeichnung gemeldet werden. Gehen Hardware-Ressourcen verloren und werden sie folglich nicht sicher bereinigt und entsorgt, können finanzielle, die Reputation betreffende und behördliche Schäden entstehen.
Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
11. Software-Ressourcenmanagement	Erfassung und Pflege von Details zu Software-Ressourcen/-Installationen Lizenzierung von Software-Ressourcen	Der Lieferant muss vollständige und genaue Verzeichniseintragungen in Bezug auf sämtliche im Umfang enthaltenen Software-Ressourcen und deren Installationen pflegen, die bei der Erbringung von Diensten für Barclays verwendet werden (einschließlich der Zuständigkeiten). Der Lieferant muss die Genauigkeit und Vollständigkeit der Daten von der Beschaffung bis zur Entsorgung (und der Installation bis zur Deinstallation) wahren. Der Lieferant muss zudem sicherstellen, dass bei der Verwendung von Software die Bedingungen der definierten Lizenz konsequent eingehalten werden.	Unangemessene Verzeichniseintragungen zu Technologie-Software-Ressourcen, einschließlich Festlegungen für Zuständigkeiten, können dazu führen, dass Dienste und Daten unsicher oder unzuverlässig werden. Wird kein entsprechendes Berechtigungsmanagement zur Verwendung von Software vorgenommen, können finanzielle, die Reputation betreffende und behördliche Schäden entstehen.

## Technologie-Belastbarkeit – Definitionen:

Zielvorgabe für die Wiederherstellungszeit (Recovery Time Objective, RTO)	RTO ist die Zeit zwischen einem unerwarteten Ausfall oder einer unerwarteten Unterbrechung von Diensten und der Wiederaufnahme des Betriebs.
Zielvorgabe für den Wiederherstellungspunkt (Recovery Point Objective, RPO)	RPO bezeichnet den angestrebten Stand der Datenverfügbarkeit zu Beginn des Wiederherstellungsprozesses. Sie ist ein Maß für den in einem Wiederherstellungsfall maximal hinnehmbaren Datenverlust.
Produktionsübergang (Production Crossover, PCO)	Bei PCO handelt es sich um die Aktivierung der alternativen (DR-)Instanz für Systeme, die auf eine aktive-passive Konfiguration ausgelegt sind, und deren Nutzung als Produktionsinstanz über einen längeren Zeitraum, um die volle Funktionalität und Kapazität zu validieren.
Systemwiederherstellungsplan (System Recovery Plan, SRP)	Bei einem Systemwiederherstellungsplan handelt es sich um ein Dokument, welches die technischen Elemente und Einzelheiten darlegt, wie ein System oder eine ausgefallene Komponente wieder zurück in den Betriebsmodus gesetzt werden kann.
Datenintegritätswiederherstellungsplan (Data Integrity and Recovery Plan, DIRP)	Bei einem Datenintegritätswiederherstellungsplan handelt es sich um ein Dokument, welches die notwendigen Schritte darlegt, um aufgrund eines Systemausfalls oder in böswilliger Absicht verloren gegangene Daten wiederherzustellen. Der Plan sollte Szenarien mit sachdienlichen Optionen aufgreifen (z. B. Datenabruf aus anderen Systemen, Datenwiederherstellung über Bandarchive oder Neuerstellung der Daten).

## Die Belastbarkeitsanforderungen von Barclays nach Belastbarkeitskategorienmatrix

Belastbarkeitskategorie	0	1	2	3
Zielvorgabe für die Wiederherstellungszeit (Recovery Time Objective, RTO)	bis zu 5 Minuten	bis zu 4 Stunden	bis zu 12 Stunden	bis zu 24 Stunden
Zielvorgabe für den Wiederherstellungspunkt (Recovery Point Objective, RPO)	bis zu 5 Minuten	bis zu 15 Minuten	bis zu 30 Minuten	bis zu 24 Stunden