Kontrollpflichten externer Lieferanten

Belastbarkeit

Version 9.0 April 2019

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.
„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. Belastbarkeitsanforderungen an die Konzeption von Diensten	Barclays schreibt die Resilience-Kategorie für die Dienste vor, und der Lieferant stellt sicher, dass die Dienste so konzipiert sind, dass sie den Erwartungen gemäß den entsprechenden Zielvorgaben für die Wiederherstellungszeit (Recovery Time Objectives (RTO)) wie nachstehend festgelegt gerecht werden.	Für Barclays ist es aus betriebswirtschaftlicher (und risikoorientierter) Sicht erforderlich, erhebliche Prozessstörungen 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.
2. Validierung der Belastbarkeitsanforderungen	Im Sinne dieser Beschreibung der Kontrolle umfasst eine Dienst-„Komponente“ alles, was die Bereitstellung des betreffenden Dienstes erleichtert, unter anderem Personen, Einrichtungen, Lieferanten, IT-Anwendungen und Infrastruktur. Um nachzuweisen, dass die Dienste den von Barclays vorgeschriebenen Anforderungen laut Resilience-Kategorie	Test- und Validierungsarbeiten werden durchgeführt, um Barclays die Gewissheit zu geben, dass die Konzeption der Dienste bestimmungsgemäß funktioniert und den von Barclays vorgeschriebenen Belastbarkeitsanforderungen gerecht wird.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
	entsprechen, muss der Lieferant die Dienst-Komponenten alle 12 Monate testen und validieren. Erfüllen Dienst-Komponenten die zutreffenden Anforderungen laut Resilience-Kategorie nicht, muss der Lieferant Barclays umgehend benachrichtigen und detaillierte Abhilfepläne (einschließlich der zu ergreifenden Maßnahmen und der entsprechenden Termine für die Fertigstellung) vorlegen.	
3. 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; und (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. Der Lieferant muss Test- und Validierungsarbeiten durchführen, 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.
4. 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 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
	• Ereignisse im Umfeld der Situation; • wie der Vorfall bzw. die Krise gemanagt wurde; • Analyse der Grundursachen des Vorfalls bzw. der Krise; • ob der Vorfall bzw. die Krise vom Lieferanten oder von Barclays als „Risikoereignis“ eingestuft wurde (d. h. als in ausreichendem Maße erheblich angesehen wird, dass er bzw. sie gemäß den geltenden Richtlinien, die dem Lieferanten bekannt sind, an die relevanten Stakeholder gemeldet/eskaliert werden sollte); • ob der Vorfall bzw. die Krise ein Verhaltenrisiko („Conduct Risk“) darstellt (z. B., wenn der Lieferant direkten Umgang mit Kunden von Barclays hat); • jegliche dem Lieferanten bekannte Beschwerden von Kunden von Barclays; und • etwaige Maßnahmen, die erforderlich sind, um ein Wiederauftreten ähnlicher Vorfälle/Krisen zu verhindern.	

3. Matrix der Belastbarkeitskritikalität:

Die Dienste des Lieferanten werden von Barclays einer spezifischen Belastbarkeitskategorie (0-3) 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:

Belastbarkeitskategorie	0	1	2	3
Zielvorgabe für die Wiederherstellungszeit (Recovery Time Objective, RTO)	0 Sekunden	< 4 Stunden	< 12 Stunden	24 Stunden