

Kontrollpflichten externer Lieferanten

Technologierisiko – Technische Kontrollen

Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Problemmanagement	Problemerkennung und -Aufzeichnung	Der Lieferant muss sicherstellen, dass für alle einzigen größeren Vorfälle eine rechtzeitige Ursachenuntersuchung durchgeführt wird, und Vorfälle wiederholen, bei denen die kombinierten Auswirkungen ausreichen, um erhebliche betriebliche Auswirkungen zu verursachen.	Wenn die Grundursache wichtiger Vorfälle nicht rechtzeitig erkannt und behoben wird, besteht weiterhin das Risiko wiederholter und vermeidbarer Ausfälle, die zu System-/Serviceunterbrechungen, Rufschäden und/oder Datenbeschädigung/-verlust führen.
	Problem-Management und Lösung	Der Lieferant muss sicherstellen, dass die Grundursache für signifikante Vorfälle zeitnah behoben wird oder – sofern dies nicht möglich ist – von Barclays eine Risikoakzeptanz zur Verfügung gestellt wird und geeignete mildernde Kontrollen angewendet werden, um die Wahrscheinlichkeit eines Wiederauftretens zu begrenzen.	
Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
2. Änderungsmanagement	Durchsetzung einer rigorosen Änderungskontrolle	Der Lieferant muss sicherstellen, dass sämtliche zum Erbringen von Services für Barclays verwendeten IT-Komponenten mit einer rigorosen Änderungskontrolle verwaltet werden, die folgende Anforderungen einschließt: <ul style="list-style-type: none"> 1. Ohne entsprechende Genehmigung von Barclays dürfen vor der Implementierung keine Änderungen vorgenommen werden. 2. Zwischen dem Initiator der Änderung, dem Verantwortlichen, der Person, die die Änderung genehmigt und der Person, die sie umsetzt, 	Unzulängliche Änderungsprozesse, mit denen unbefugte, unzureichend verwaltete oder unangemessene Änderungen an Technologien verhindert werden können zu Störungen des Dienstes, zur Beschädigung von Daten, zu Datenverlust, Verarbeitungsfehlern oder Betrug führen.

		<p>muss eine Aufgabentrennung vorgesehen sein.</p> <p>3. Änderungen müssen entsprechend der mit der Aufrechterhaltung des erforderlichen Mindestniveaus an Service für Barclays verbundenen Risikostufe geplant und verwaltet werden.</p> <p>4. Potenzielle Auswirkungen von Änderungen auf die Leistung und/oder Fähigkeit von betroffenen Technologie-Komponenten müssen angemessen berücksichtigt werden.</p> <p>5. Änderungen müssen vor der Umsetzung die für sie relevanten technischen und betriebswirtschaftlichen Tests durchlaufen, unter Aufbewahrung der Nachweise, sofern erforderlich</p> <p>6. Änderungen müssen nach der Umsetzung getestet werden, um sicherzustellen, dass sie erfolgreich vorgenommen wurden, ohne dass es zu ungeplanten Auswirkungen gekommen ist</p>	
3. Leistungs- und Fähigkeitsmanagement	Den Technologiebedürfnissen von Barclays auch weiterhin entsprechen	Der Lieferant muss für sämtliche zur Erbringung von Services für Barclays verwendeten wichtigen IT-Komponenten geeigneten Leistungs- und Fähigkeitsstufen definieren, pflegen und dokumentieren, die alle vertraglichen Anforderungen erfüllen. Der Lieferant 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 Erbringung von Services allen vertraglichen Anforderungen und den Bedürfnissen von Barclays entspricht.	Unzureichende Maßnahmen, mit denen die Leistung und/oder Fähigkeit von IT-Ressourcen definiert, dokumentiert und überwacht und dafür gesorgt wird, dass sie auch weiterhin den aktuellen und künftigen Anforderungen entsprechen, können zu einem nicht hinnehmbaren Abbau und/oder nicht hinnehmbaren Unterbrechungen von Technologie-Diensten und zu Geschäftsverlusten führen.
Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
4. Entwicklung von Technologie-Anwendungen	Teststrategie und Abschluss vor der technischen und/oder geschäftlichen Umsetzung	Der Lieferant muss die Qualität aller Software kennen, bevor er diese Software an Barclays verkauft oder liefert. Vor der Bereitstellung an Barclays muss sich der gesamte Softwarecode in dem/den Versionskontrollsystem(en) befinden und vom Dienstleister des Lieferanten abgezeichnet werden. Anwendungsänderungen müssen vom Lieferanten einem Softwaretest unterzogen werden, um sicherzustellen, dass die Software die erfassten Anforderungen erfüllt. Prüfnachweise müssen aufbewahrt werden.	Infolge von unzureichend getesteten und qualitätsgesicherten Systemen und Diensten kann es zu unvorhersehbaren kritischen Verlusten von Funktionalität bei Technologie-Diensten und Geschäftsprozessen kommen.

	Bestätigen der Systemanforderungen	Bei der Lieferung von Software nach Barclays-Spezifikationen muss der Lieferant sicherstellen, dass die geschäftlichen Anforderungen klar definiert sind und mit Barclays vereinbart werden.	Unzureichend definierte Geschäftsanforderungen können zu einem falschen Systemverhalten führen, was zu Risiken für Geschäfts- und Betriebsprozesse führt.
	Geschäftliche Akzeptanz vor dem Einsatz	Bei der Lieferung von Software nach Barclays-Spezifikationen muss der Lieferant einen mit Barclays vereinbarten Qualitäts-/Abnahmeprozess vereinbaren und befolgen.	Eine unzureichende geschäftliche Akzeptanz vor dem Einsatz kann zu einem falschen Systemverhalten führen, was zu Risiken für Geschäfts- und Betriebsprozesse führt.
5. 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.	Sichere und zuverlässige Sicherungsmedien sind erforderlich, um System-/Serviceunterbrechungen, Datenverlust oder unangemessene Offenlegung von Daten zu vermeiden.
Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
6. 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 unzuverlässige Bereitstellung von Diensten vermeiden lässt.	Werden produktionsfremde Komponenten 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 Konfigurationselementen	Der Lieferant muss vollständige und genaue Verzeichniseintragen in Bezug auf sämtliche im Umfang enthaltenen Konfigurationselemente pflegen, die bei der Erbringung von Diensten für Barclays verwendet werden (einschließlich der Zuständigkeiten und der	Unangemessene oder unvollständige Verzeichniseintragen (zusammen mit den damit verbundenen Abhängigkeiten/Zuordnungen von bzw. zu anderen Konfigurationselementen) können dazu führen,

		vorgelagerten/nachgelagerten Abhängigkeiten/Zuordnungen). Der Lieferant muss Kontrollmechanismen bereithalten, welche die fortlaufende Pflege der Genauigkeit und Vollständigkeit der Daten sicherstellen.	dass Dienste und Daten bedingt durch ineffektive Folgenabschätzungen von Vorfällen und Änderungen unsicher oder instabil werden.
7. Service-Level-Management	Definieren und Überwachen der Service-Performance	Der Lieferant muss sicherstellen, dass der Service den vereinbarten Service-Levels entspricht, einschließlich der Überwachung und Berichterstattung der Service-Level.	Die Service-Level stellen sicher, dass die IT-Services gemäß den vereinbarten IT-Serviceverpflichtungen erbracht werden

Technologiedefinitionen:

Konfigurationselement	Jede Komponente, die für die Erbringung eines IT-Services gemanagt werden muss. Konfigurationselemente können physisch (z. B. ein Computer oder Router), virtuell (z. B. ein virtueller Server) oder logisch (z. B. ein Service) sein. Änderungen (Ergänzungen, Änderungen oder Einstellung) müssen unter der Kontrolle des Änderungsmanagements vorgenommen werden.
Vorfall	Eine ungeplante Unterbrechung eines IT-Services oder eine Qualitätsminderung eines IT-Services, wie unter anderem der Ausfall eines Konfigurationselements, der noch keinen Service beeinträchtigt hat.
IT-Service	Ein Service, der einem oder mehreren Kunden von einem IT-Dienstleister zur Verfügung gestellt wird. Ein IT-Service besteht aus einer Kombination aus Mitarbeitern, Prozessen und IT und wird den Kunden zur Unterstützung ihrer Geschäftsprozesse erbracht.
Schwerer Vorfall	Ein Vorfall, der ein erhebliches Risiko/Auswirkungen auf Barclays darstellt und zu schwerwiegenden Folgen wie einem schweren Produktivitätsverlust, einem Schaden für den Ruf / die aufsichtsbehördlichen Vorschriften und Auswirkungen auf die wichtigsten Geschäftsprozesse, wichtigen Kontrollen oder Systeme führen kann.
Problem	Die unbekannte Ursache eines oder mehrerer Vorfälle.