

# 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 größeren und alle wiederholten Vorfälle, bei denen die kombinierten Auswirkungen ausreichen, um erhebliche betriebliche Auswirkungen zu verursachen, eine rechtzeitige Ursachenuntersuchung durchgeführt wird.	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 die oben beschriebenen 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.	
2. Änderungsmanagement	Durchsetzung einer rigorosen Änderungskontrolle	<p>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:</p> <ol style="list-style-type: none"> <li>1. Der Lieferant muss Barclays vor der Implementierung über alle wesentlichen Änderungen informieren, damit eine Folgenabschätzung durchgeführt werden kann und geeignete Abhilfemaßnahmen ergriffen werden können.</li> <li>2. Zwischen dem Initiator der Änderung, dem Verantwortlichen, der Person, die die Änderung genehmigt und der Person, die sie umsetzt, muss eine Aufgabentrennung vorgesehen sein.</li> <li>3. Änderungen müssen entsprechend der mit der Aufrechterhaltung des erforderlichen Mindestniveaus an Service für Barclays verbundenen Risikostufe geplant und verwaltet werden.</li> <li>4. Potenzielle Auswirkungen von Änderungen auf die Leistung und/oder Fähigkeit von betroffenen Technologie-Komponenten müssen angemessen berücksichtigt werden.</li> <li>5. Änderungen müssen vor der Umsetzung die für sie relevanten technischen und betriebswirtschaftlichen Tests durchlaufen, unter Aufbewahrung der Nachweise, sofern erforderlich</li> <li>6. Änderungen müssen nach der Umsetzung getestet werden, um</li> </ol>	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.

Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
		sicherzustellen, dass sie erfolgreich vorgenommen wurden, ohne dass es zu ungeplanten Auswirkungen gekommen ist	
3. Leistungs- und Fähigkeitsmanagement	Den Technologiebedürfnissen von Barclays auch weiterhin entsprechen	Der Lieferant muss für sämtliche wichtigen IT-Komponenten, die Barclays zur Erbringung von Services verwendet, geeignete Leistungs- und Fähigkeitsstufen definieren, pflegen und dokumentieren, die alle vertraglichen Anforderungen erfüllen. Dabei sind bekannte Geschäftsanforderungen und die aktuelle Kapazitätsauslastung zu berücksichtigen, um sicherzustellen, dass die verfügbaren Kapazitäten weiterhin den Anforderungen entsprechen. 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.
4. Entwicklung von Technologie-Anwendungen	Teststrategie und Abschluss vor der technischen und/oder geschäftlichen Umsetzung	Der Lieferant muss sicherstellen, dass die Software/der Dienst wie vom Lieferanten beschrieben funktioniert, bevor er diese Software oder softwarebasierten Dienste an Barclays verkauft oder bereitstellt, oder einen Überblick über bekannte Mängel und Auswirkungen auf die Bereitstellung der Software/Dienste geben. Vor der Bereitstellung an Barclays muss sich der gesamte Softwarecode in Versionskontrollsystemen befinden und vom Lieferanten abgezeichnet werden. Anwendungsänderungen müssen vom Lieferanten einem Softwaretest unterzogen werden, um sicherzustellen, dass die Software die erfassten Anforderungen erfüllt. Der Lieferant muss Testnachweise aufbewahren.	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 an die Technologie klar definiert sind und mit Barclays vereinbart wurden.	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 geschäftlichen 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.

## 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.
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.
Wesentliche Änderungen	Änderungen, die sich auf den effektiven Betrieb der für Barclays bereitgestellten Dienste auswirken werden – oder sich auswirken könnten – und/oder Änderungen, zu deren Umsetzung Barclays möglicherweise angemessene Maßnahmen zur Risikominderung ergreifen muss.