BARCLAYS

Kontrollpflichten externer Lieferanten

Technologierisiko

Version 9.0, April 2019

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 zu minimieren. Der Lieferant sollte zudem sicherstellen,	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.

		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	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: 1. Keine Änderung ohne entsprechende Autorisierung - Genehmigung muss vor der Umsetzung erfolgen 2. Aufgabentrennung zwischen dem Initiator der Änderung, dem Verantwortlichen, der Person, die die Änderung genehmigt und der Person, die sie umsetzt 3. Planung und Verwaltung von Änderungen je nach Stufe des damit verbundenen Risikos 4. Hinreichende Berücksichtigung der potenziellen Auswirkungen von Änderungen auf die Leistung und/oder Fähigkeit von betroffenen Technologie-Komponenten 5. Änderungen durchlaufen vor der Umsetzung die für sie relevanten technischen und betriebswirtschaftlichen Tests, unter Aufbewahrung der Nachweise, sofern erforderlich 6. Änderungen müssen nach der Umsetzung getestet werden, um sicherzustellen, dass sie erfolgreich vorgenommen wurden, ohne dass es zu ungeplanten Auswirkungen gekommen ist	Unzureichende Maßnahmen, mit denen die Leistung und/oder Fähigkeit von IT-Ressourcen überwacht wird 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. Darüber hinaus kann es infolge von unzulänglichen Änderungsprozessen, mit denen unbefugte oder unangemessene Änderungen an Technologie-Diensten verhindert werden, zu Störungen des Dienstes, zur Beschädigung von Daten, zu Datenverlust, Verarbeitungsfehlern oder Betrug kommen.
5. Dienstkontinuität	Schaffen und Validieren von geeigneten Maßnahmen für die Resilience/Wiederherstellung	Der Lieferant muss die Bedürfnisse von Barclays in Bezug auf die Belastbarkeit/Wiederherstellung für jedes IT-System und jeden von ihm für Barclays erbrachten Dienst verstehen und abstimmen. Belastbarkeits- und Wiederherstellungspläne sollten gepflegt und ihre Genauigkeit sollte bestätigt werden,	Eine fehlende oder unzulängliche Planung der Dienstkontinuität kann zu nicht hinnehmbaren Ausfällen von Technologie-Diensten für das Unternehmen oder zum Verlust von Kunden nach einem Vorfall führen. Wenn die Dokumentation zur Belastbarkeit auf dem aktuellen Stand gehalten wird und Übungen dazu durchgeführt werden, entsprechen

		und die Maßnahmen im Zusammenhang mit der Dienstkontinuität sollten hinreichend dokumentiert werden, es sollten Übungen dazu durchgeführt werden bzw. sie sollten nachweislich zuverlässig sein und den geschäftlichen Bedürfnissen entsprechen.	die Wiederherstellungspläne auch weiterhin den geschäftlichen Bedürfnissen.
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 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.	Die unzureichende Definition von Geschäfts-/Kundenbedürfnissen und/oder die unzureichende Dokumentation dieser 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 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. 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.	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.
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 unzuverlässige Bereitstellung von Diensten vermeiden lässt.	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 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 die Genauigkeit und Vollständigkeit der Daten wahren.	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 vollständige und genaue Verzeichniseintragungen in Bezug auf sämtliche im Umfang enthaltenen IT-Hardware-Ressourcen pflegen, die bei der Erbringung von Diensten für Barclays verwendet werden (einschließlich der Zuständigkeiten und Kennzeichnungen, sofern erforderlich). Der Lieferant muss die Genauigkeit und Vollständigkeit der Daten während des gesamten Lebenszyklus der Ressource von der Beschaffung bis zur Entsorgung wahren. Sämtliche entsorgten	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.

		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.	
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-Hardware-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.