

Kontrollpflichten externer
Lieferanten
Zahlungsprozess

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
Einhaltung der gesetzlichen und satzungsmäßigen Bestimmungen vor Ort	Der Lieferant stellt sicher, dass rechtliche wie regulatorische Bestimmungen, die für die vom Lieferanten verarbeiteten Zahlungen gelten, angemessen dokumentiert sind und eingehalten werden.	Damit wird sichergestellt, dass Zahlungen gemäß den im Geltungsbereich liegenden rechtlichen wie regulatorischen Bestimmungen verarbeitet werden. Die Nichteinhaltung rechtlicher und regulatorischer Bestimmungen könnte Geldbußen und Rufschädigungen nach sich ziehen.
Identifizierung von wesentlichen Risiken im Zusammenhang mit dem Zahlungsprozess	Der Lieferant muss die Liste der Zahlungsprozesse überprüfen, um sicherzustellen, dass sämtliche Risiken identifiziert, gemanagt und entsprechend überwacht werden.	Diese Bestimmung stellt sicher, dass wesentliche Risiken im Zusammenhang mit dem Zahlungsprozess proaktiv identifiziert und wichtige Kontrollen für das Management der Risiken umgesetzt werden.
Manuelle Zahlungen	Der Lieferant muss jede manuelle Zahlungsverarbeitung identifizieren, um sicherzustellen, dass sämtliche mit der manuellen Zahlungsverarbeitung verbundenen Risiken identifiziert, gemanagt und entsprechend überwacht werden.	Damit wird sichergestellt, dass Klarheit über die Definition von manuellen Zahlungen herrscht, so dass die manuelle Zahlungsverarbeitung proaktiv identifiziert und Verantwortung dafür übernommen wird, zusammen mit einem sachgerechten Risikomanagement.
Bestandsliste der manuellen Zahlungen	<p>Es muss ein Prozess dokumentiert und vorhanden sein, um eine vollständige, genaue und aktuelle Bestandsliste der manuellen Zahlungen sicherzustellen, so dass die Bestimmungen dieses Vertragsanhangs eingehalten werden.</p> <p>Zur Schaffung von Transparenz hinsichtlich des gesamten im Geltungsbereich liegenden manuellen Zahlungsprozesses für den Lieferanten und zur Erfassung der Hauptkennzeichen für die Einhaltung der Bestimmungen dieses Vertragsanhangs muss eine Bestandsliste der manuellen Zahlungen vorhanden sein. Die Bestandsliste der manuellen Zahlungen muss mindestens einmal jährlich auf Genauigkeit und Vollständigkeit überprüft werden.</p>	<p>Wird diese Bestimmung nicht umgesetzt, kann Barclays nicht sicher sein, dass der Lieferant über ausreichend dokumentierte Verfahren zur Behandlung der mit manuellen Zahlungsprozessen verbundenen Risiken verfügt.</p> <p>Die Bestimmung zur Bestandsliste der manuellen Zahlungen stellt sicher, dass der Lieferanten-Manager eine End-to-End-Überprüfung zur Identifizierung von manuellen Zahlungsprozessen und zur letztendlichen Implementierung und Überwachung von erforderlichen wesentlichen Kontrollen im Zusammenhang mit dem Risiko der Verarbeitung von manuellen Zahlungen durchgeführt hat.</p>

		Dadurch kann das Risiko von damit verbundenen Verlusten, Rufschädigung und/oder einer Geldbuße/Rüge von Aufsichtsbehörden verringert werden.
Unversehrtheit von Zahlungsanweisungen	Der Lieferant muss sicherstellen, dass die Unversehrtheit von Zahlungsanweisungen im Laufe des gesamten Lebenszyklus der Zahlung gewahrt bleibt. Beim Lieferanten müssen die minimalen wesentlichen Kontrollen vorhanden sein, um die Echtheit und Unversehrtheit der Anweisungen zu wahren und zu schützen. Hierzu gehört unter anderem, dass die Anweisung: nicht verändert werden kann und von der Auslösung bis zur Abrechnung in ihrem ursprünglichen Zustand verbleibt genau verarbeitet und abgerechnet wird, d. h. der ursprünglichen Aufforderung und den anwendbaren Vorschriften entsprechend nicht vervielfältigt wird	Wird diese Bestimmung nicht umgesetzt, kann Barclays möglicherweise nicht sicher sein, dass es beim Lieferanten ausreichende Kontrollen gibt, um sicherzustellen, dass die Unversehrtheit der Zahlungsanweisungen im Laufe des gesamten Zahlungszyklus gewahrt bleibt. Mögliche Folgen sind potenzielle betrügerische Zahlungen, eine fehlerhafte Zahlungsverarbeitung und eine damit verbundene Rufschädigung und/oder eine Geldbuße/Rüge von Aufsichtsbehörden.
Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
Authentifizierung des Absenders	Der Lieferant muss sicherstellen, dass die Zahlungsaufforderung echt ist. Der Lieferant sollte sich vergewissern, dass die Zahlungsaufforderung aus seriöser Quelle stammt (z. B. Identitätsprüfungen und Verifizierungen); und er sollte die Unversehrtheit der Zahlungsanweisungen feststellen.	Diese Bestimmung dient zur Feststellung der Seriosität der Zahlungsanweisung, indem sichergestellt wird, dass die Zahlungsanweisung echt ist. Durch diese Kontrolle wird das Risiko von Verlusten im Zusammenhang mit betrügerischen Zahlungen, einer damit verbundenen Rufschädigung und/oder einer Geldbuße/Rüge von Aufsichtsbehörden verringert.

Befugnis des Absenders	Der Lieferant muss sicherstellen, dass jede Zahlungsaufforderung von den vorab bestimmten und vorab zugelassenen Einzelpersonen genehmigt worden ist.	Diese Bestimmung dient zur Feststellung der Echtheit der Zahlungsanweisungen, indem sichergestellt wird, dass die Personen, die die Zahlungsanweisungen unterzeichnet haben, die Bevollmächtigung dafür haben. Durch diese Kontrolle wird das Risiko von Verlusten im Zusammenhang mit betrügerischen Zahlungen, einer damit verbundenen Rufschädigung und/oder einer Geldbuße/Rüge von Aufsichtsbehörden vermindert.
Befugnis für den gesamten Lebenszyklus von Zahlungen	Der Lieferant muss sicherstellen, dass die Person, die die Zahlung genehmigt, die Genehmigung während des gesamten Lebenszyklus der Zahlung im Rahmen des festgelegten Befugnisrahmens (Limits of Authority) erteilt (vorab definierte und vorab genehmigte Limits of Authority). Die Limits of Authority sollten mindestens einmal jährlich oder wenn erforderlich überprüft werden.	Diese Bestimmung dient zur Feststellung der Gültigkeit der Zahlungsanweisungen, indem sichergestellt wird, dass die im Zahlungsprozess eingeräumten unterschiedlichen Befugnisse im Einklang mit der im Unternehmen vorgenommenen und genehmigten Erteilung von Befugnissen steht. Durch diese Kontrolle wird das Risiko von Verlusten im Zusammenhang mit betrügerischen/fehlerhaften Zahlungen, einer damit verbundenen Rufschädigung und/oder einer Geldbuße/Rüge von Aufsichtsbehörden vermindert.
Unabhängige Ebenen während des gesamten Lebenszyklus von Zahlungen	Der Lieferant muss sicherstellen, dass die Person, die die Zahlung genehmigt, unabhängig ist und keinen Zugriff auf die Erstellung oder Änderung der Anweisung hat.	Diese Kontrolle stellt sicher, dass potenzielle Fehler oder potenzielle Probleme von einer unabhängigen Person proaktiv identifiziert werden. Durch diese Kontrolle wird das Risiko von Verlusten im Zusammenhang mit betrügerischen/fehlerhaften Zahlungen, einer damit verbundenen Rufschädigung und/oder einer Geldbuße/Rüge von Aufsichtsbehörden verringert.
Verzögerungen bei der Zahlungsverarbeitung	Der Lieferant muss sicherstellen, dass jede Zahlung rechtzeitig verarbeitet und abgerechnet wird, damit die SLAs (Anforderungen des Kunden und der Systeme) eingehalten werden.	Diese Bestimmung stellt sicher, dass sämtliche vom Lieferanten verarbeitete Zahlungen im Einklang mit den Stichtagen der betreffenden Zahlungs-/Kartensysteme sowie nach Kundenanforderungen verarbeitet werden. Dies wiederum verringert das Risiko, dass Zahlungen mit Verzögerungen verarbeitet werden. Mögliche Folgen einer verzögerten Verarbeitung von Zahlungsanweisungen sind Unzufriedenheit der Kunden und Beschwerden, was zu einem potenziellen Verlust von Kunden und Rufschädigung führt.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
<p>In Frage kommende Kommunikationsmethode und Übertragungsmethoden zur Übermittlung von Zahlungsanweisungen</p>	<p>Der Lieferant muss sicherstellen, dass sämtliche in Frage kommenden Kommunikations- und Übertragungsmethoden für die Übermittlung von Zahlungsanweisungen genau geprüft werden, um sicherzustellen, dass angemessen starke Kontrollen implementiert werden.</p>	<p>Zur Verminderung der verschiedenen Risiken wie beispielsweise des Informationsrisikos (Datenschutz), des Betrugsrisikos (Datenmanipulation), des Cyber-Risikos (Cyber-Bedrohungen) usw. hat Barclays Festlegungen zu verbotenen, begrenzt zulässigen und genehmigten Methoden getroffen.</p> <p>Begrenzt zulässige Kommunikationsmethoden sollen nur eingesetzt werden, wenn ausreichende Kontrollen vorhanden sind.</p>
<p>Funktionen und Verantwortlichkeiten</p>	<p>Der Lieferant muss Funktionen und Verantwortlichkeiten für das Zahlungsprozessrisiko definieren und kommunizieren. Diese müssen nach jeder wesentlichen Änderung am Betriebsmodell oder Geschäft des Lieferanten überprüft werden.</p>	<p>Durch diese Bestimmung wird sichergestellt, dass die Funktionen und Verantwortlichkeiten der beiden Seiten festgelegt, dokumentiert und genehmigt sind. Das ist im Streitfall hilfreich.</p>
<p>Zahlungs-/Kartensystemrisiko</p>	<p>Zahlungs-/Kartensystemrisiko ist eine Kollektivbezeichnung für die drei Hauptrisikokategorien, die mit der Zugehörigkeit zu einem Zahlungs-/Kartensystem, der Struktur und dem Betrieb des Systems verbunden sind:</p> <ul style="list-style-type: none"> • Geschäftsrisiko • Erfüllungsrisiko • Operationelles Risiko <p>In Fällen, wo der Drittanbieter einem Zahlungs-/Kartensystem (direkt/indirekt) angehört, sollte der für das System Verantwortliche sicherstellen, dass speziell im Zusammenhang mit der Rechtzeitigkeit und der regelmäßigen Bewertung stehende Geschäfts-/Erfüllungsrisiken oder operationelle Risiken, die sich eingestellt haben, über festgelegte Kanäle für Geschäftskontrollen gemeldet werden.</p>	<p>Die Kontrolle liefert den Kontext dafür, was ein Zahlungs-/Kartensystemrisiko in Bezug auf Barclays bedeutet. Dadurch wird sichergestellt, dass Klarheit über die Definition des Zahlungs-/Kartensystemrisikos herrscht, damit die manuelle Zahlungsverarbeitung proaktiv identifiziert und Verantwortung dafür übernommen wird, zusammen mit einem sachgerechten Risikomanagement.</p> <p>Durch diese Bestimmung muss der Lieferant sicherstellen, dass speziell im Zusammenhang mit der Rechtzeitigkeit und der regelmäßigen Bewertung stehende Geschäfts-/Erfüllungsrisiken oder operationelle Risiken, die sich eingestellt haben, über festgelegte Kanäle für Geschäftskontrollen gemeldet werden. Dadurch wird sichergestellt, dass rechtzeitig Maßnahmen ergriffen werden, um operationelle Probleme, darunter auch rechtliche und den Ruf betreffende Risiken, zu entschärfen.</p>

	Der Lieferant muss die Liste der Zahlungs-/Kartensysteme überprüfen, um sicherzustellen, dass sämtliche Risiken identifiziert, gemanagt und entsprechend überwacht werden.	Wird diese Bestimmung nicht umgesetzt, kann Barclays nicht sicher sein, dass der Lieferant für die vollumfängliche Erfüllung der Anforderungen gesorgt hat.
Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
Zahlungs-/Kartensystemrisiko	Der Lieferant muss sicherstellen, dass sämtliche im Auftrag von Barclays verarbeiteten Zahlungen unter Einhaltung der Bestimmungen des Zahlungs-/Kartensystems verarbeitet werden.	<p>Wird diese Bestimmung nicht umgesetzt, kann Barclays nicht sicher sein, dass der Lieferant über ausreichend dokumentierte Verfahren zur Behandlung der mit einer Nichteinhaltung der Bestimmungen des Zahlungs-/Kartensystems verbundenen Risiken verfügt.</p> <p>Zahlungen, die fehlerhaft, mit Verzögerungen, mit Fehlern bei der Authentifizierung oder Fehlern im Zusammenhang mit Berechtigungen verarbeitet werden und zudem die Nichteinhaltung der anwendbaren Zahlungsvorschriften nach sich ziehen, müssen anhand der damit verbundenen Risiken auf Stufe 3 gemeldet werden. Darüber hinaus muss bei jeder Nichteinhaltung von Zahlungsvorschriften der betreffende Geschäftskontrollen-Prozess für die Meldung von regulatorischen Verstößen im Rahmen des Verhaltensrisikos befolgt werden.</p>
System-Risikobewertung	Der Lieferant muss mindestens einmal jährlich eine umfassende System-Risikobewertung für jedes Zahlungs-/Kartensystem, dem er direkt und indirekt angehört, durchführen. Die Risikobewertung muss vom Verantwortlichen für das System und von der Geschäftsleitung abgezeichnet werden.	Ziel dieser Kontrollbestimmung ist es, sicherzustellen, dass die drei mit dem Zahlungs-/Kartensystem verbundenen Hauptrisiken entsprechend gemanagt worden sind. Mögliche Folgen einer nicht sachgerechten Bewertung sind potenzielle betrügerische Zahlungen, eine fehlerhafte Zahlungsverarbeitung und eine damit verbundene Rufschädigung und/oder eine Geldbuße/Rüge von Aufsichtsbehörden.
Due Diligence	Bevor er sich einem Zahlungs-/Kartensystem neu anschließt oder es unterstützt, muss der Lieferant eine formelle Due Diligence durchführen, um sicherzustellen, dass die Mindestanforderungen erfüllt werden.	Durch diese Bestimmung wird sichergestellt, dass der Lieferant eine Due Diligence im erforderlichen Umfang durchgeführt hat, um das Risiko von Verlusten im Zusammenhang mit betrügerischen Zahlungen, einer damit verbundenen Rufschädigung und/oder einer Geldbuße/Rüge von Aufsichtsbehörden zu verringern.

Änderungen	Im Falle von erheblichen Änderungen an Prozessen oder Vorschriften muss der Lieferant eine zusätzliche, außerplanmäßige Risikobewertung durchführen, um sicherzustellen, dass das System-Risiko durchgängig gemäß dem von Barclays vorgegebenen Rahmen gemanagt wird.	Ziel dieser Kontrollbestimmung ist es, sicherzustellen, dass die drei mit den Änderungen bezüglich des Zahlungs-/Kartensystems verbundenen Hauptrisiken entsprechend gemanagt worden sind. Mögliche Folgen einer nicht sachgerechten Bewertung sind potenzielle betrügerische Zahlungen, eine fehlerhafte Zahlungsverarbeitung und eine damit verbundene Rufschädigung und/oder eine Geldbuße/Rüge von Aufsichtsbehörden.
Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
Verantwortlicher für das System	Der Lieferant muss sicherstellen, dass ein für das Zahlungs-/Kartensystem Verantwortlicher benannt wird, der die Geschäftsbeziehung insgesamt pflegt und die fortlaufende Risikoüberwachung zur Ausgestaltung des Systems sicherstellt. Darüber hinaus muss der Lieferant sicherstellen, dass der für das System Verantwortliche das System-Risiko überwacht und über die Kanäle für Geschäftskontrollen darüber berichtet.	Diese Bestimmung stellt sicher, dass es für das betreffende Zahlungs-/Kartensystem einen benannten Verantwortlichen gibt, damit die Geschäftsbeziehung besser gemanagt und für eine zeitnahe Berichterstattung gesorgt wird.
Vorfallbehandlung und Reaktionsebenen im Zusammenhang mit Fehlern bei manuellen Zahlungen	Der Lieferant muss über Fehler bei der Durchführung von manuellen Zahlungsprozessen in Verbindung mit internem oder externem Betrug, menschlichem Versagen, System-Problemen oder unzulänglichen Prozessen proaktiv Bericht erstatten.	Damit wird sichergestellt, dass betriebliche Probleme in Verbindung mit Fehlern bei manuellen Zahlungen zeitnah durch Eskalation weitergereicht und proaktiv identifiziert werden, um die Auswirkungen auf Kunden und den Betrieb zu verringern.
Vorfallberichterstattung	Es muss ein dokumentierter Prozess vorhanden sein, um sicherzustellen, dass sämtliche betrieblichen Fehler bzw. Ausfälle, darunter auch Vorfälle, die ein Zahlungsprozessrisiko darstellen, zusammen mit Angaben zu den Umfängen und zum Wert der betroffenen Zahlungen, zu den betroffenen Kunden und zur betroffenen Business Unit, zeitnah an Barclays gemeldet werden. Der Lieferant sollte Vorfälle unverzüglich behandeln und Barclays melden. Es sollte ein Vorfallbehandlungsprozess für die zeitnahe Bearbeitung und Meldung von Fehlern, die Auswirkungen auf Barclays haben, eingerichtet werden.	Mit Hilfe eines Vorfallbehandlungsprozesses wird sichergestellt, dass Vorfälle schnell in Grenzen gehalten werden und verhindert wird, dass sie sich ausweiten. Wird diese Bestimmung nicht umgesetzt, kann Barclays nicht sicher sein, dass der Lieferant über ausreichend dokumentierte, geprüfte Verfahren für die Behandlung von Zwischenfällen im Zusammenhang mit Zahlungen verfügt. Dies kann dazu führen, dass nach einem Zwischenfall unangemessene Maßnahmen getroffen werden, was die Gefahr von Verlusten oder einer damit verbundenen Rufschädigung und/oder Geldbuße/Rüge von Aufsichtsbehörden erhöht.

	Der Lieferant muss dafür sorgen, dass die festgelegten Abhilfemaßnahmen nach einem Vorfall gemäß einem Abhilfeplan (Aktion, Zuständigkeit, Frist) ausgeführt und mit Barclays abgesprochen und vereinbart werden.	Durch das Vorhandensein eines eingeführten dokumentierten und genehmigten Verfahrens für das Management und die Meldung von Fehlern bzw. Ausfällen im Betrieb wird die Vollständigkeit der Berichterstattung sowie die Identifizierung von (gegebenenfalls) gezogenen Lehren bei anderen Business Units sichergestellt.
15. Fortlaufende Überwachung	Der Lieferant muss regelmäßig (mindestens jedoch einmal in jedem Kalenderjahr) seine Einhaltung dieses Vertragsanhangs messen, auswerten und dokumentieren.	Durch fortlaufende Sicherheitskontrollen wird die Kontrollumgebung beim Lieferanten aufrechterhalten.

Abkürzungen und andere Begriffe	Definitionen
Zahlungsprozessrisiko	Als Zahlungsprozessrisiko wird das Risiko eines Ausfalls beim Betreiben von Zahlungsprozessen bezeichnet.
Manuell	Alles, was mit Eingriffen durch den Menschen an irgendeiner Stelle der End-to-End-Transaktion / des Zahlungsprozess-Lebenszyklus verbunden ist.
Manuelle Zahlungen	Eine manuelle Zahlung ist die eingehende, ausgehende oder interne Übertragung von Mitteln von einem Beteiligten an einen anderen, die über ein externes System oder eine Korrespondenzbank-Beziehung abgerechnet wird, wobei jeglicher Teil des Zahlungsprozesses von der Auslösung bis hin zur Abrechnung, einschließlich etwaiger Nachbesserungen oder Änderungen, manuell erfolgt.
Risiko im Zusammenhang mit manuellen Zahlungen	Das Risiko im Zusammenhang mit manuellen Zahlungen betrifft einen Ausfall bzw. Fehler beim Betrieb von manuellen Zahlungsprozessen infolge von internem oder externem Betrug, menschlichem Versagen, System-Problemen oder unzulänglichen Prozessen.
In Frage kommende Kommunikationsmethode und Übertragungsmethoden zur Übermittlung von Zahlungsanweisungen	Folgende Methoden sind verboten: Externe Laufwerke / USB / Floppy Disks / CDs/Diskette Begrenzt zulässige Methoden: Filiale / Persönlich / Telefax / E-Mail*

	<p>Folgende Methoden kommen in Frage: Online-Banking, Mobile-Banking, sonstige definierte und vereinbarte Methoden im hinsichtlich der Risikoneigung genehmigten Rahmen</p> <p>*Anmerkung zu begrenzt zulässigen Methoden: Diese Kanäle können genutzt werden, solange angemessene Kontrollen gemäß der Richtlinie vorhanden sind.</p>
Zahlungs-Lebenszyklus	<p>Beginnt bei der Auslösung und Erfassung der Zahlung im Zahlungskanal und endet bei Abrechnung der Zahlung mit der Gegenpartei über ein externes Abrechnungssystem.</p>
Absender	<p>Eine Einzelperson, die eine Zahlungsaufforderung (mehrere Zahlungsaufforderungen) vorlegt.</p>
Zahlungs- /Kartensystemrisiko	<p>Zahlungs-/Kartensystemrisiko ist eine Kollektivbezeichnung für die drei Hauptrisikokategorien, die mit der Zugehörigkeit zu einem Zahlungs-/Kartensystem, der Struktur und dem Betrieb des Systems verbunden sind:</p> <ul style="list-style-type: none"> • Geschäftsrisiko: Risiko, dass das Zahlungssystem-/ Kartensystem / System oder jegliche von dessen Komponenten, z. B. ein dafür eingesetzter Infrastrukturservers, aufgrund von Beeinträchtigungen durch Finanzschocks nicht nach dem Prinzip der Unternehmensfortführung aufrechterhalten werden kann • Erfüllungsrisiko: Risiko, dass ein anderer Teilnehmer in einem System seinen finanziellen Verpflichtungen zum Zeitpunkt ihrer Fälligkeit nach den Regelungen des Systems nicht nachkommen kann oder nicht nachkommt; oder dass eine andere Institution, die die Erfüllung dieser Verpflichtungen ermöglicht, beispielsweise die Abrechnungsstelle, insolvent wird • Operationelles Risiko Risiko, dass ein Systembetreiber oder wichtiger Dienstleister für das System aufgrund von unzulänglichen, ausgefallenen oder fehlerhaften internen Prozessen, Mitarbeitern oder Systemen operativ nicht in der Lage ist, Zahlungen wie vorgesehen zu verarbeiten oder abzurechnen.