

CITI-ANFORDERUNGEN FÜR LIEFERANTEN

VERANTWORTLICHE:
Head of Citi Procurement & Risk

AUSSTELLUNGSDATUM:
Januar 2015

ÜBERARBEITET:
September 2026

VERSION:
9

INHALTSVERZEICHNIS

1	ALLGEMEINER ÜBERBLICK	3
2	CHANCENGLEICHHEIT BEI DER BESCHÄFTIGUNG	5
3	ANTI-BESTECHUNG UND KORRUPTIONSBEKÄMPFUNG (AB&C)	6
4	GESCHENKE UND BEWIRTUNG	7
5	LIEFERANTENENGAGEMENT UND LIEFERANTENPRINZIPIEN	7
6	VERBOT DER MODERNEN SKLAVEREI	7
7	PERSONAL DES LIEFERANTEN	10
8	BETRUGSBEKÄMPFUNG	11
9	UMGANG MIT MEDIEN UND ÖFFENTLICHE AUFTRITTE	13
10	SCHRIFTLICHE ELEKTRONISCHE KOMMUNIKATION	14
11	POLITISCHE TÄTIGKEIT UND BEITRÄGE	14
12	BEKÄMPFUNG VON GELDWÄSCHE („AML“).....	15
13	UNTERLAGENVERWALTUNG	17
14	WIDERSTANDSFÄHIGKEIT DES UNTERNEHMENS/KONTINUITÄT DER GESCHÄFTSTÄTIGKEIT	19
15	 Globale Standards für Hintergrundüberprüfungen.....	26
16	Kosten	28
17	Informationssicherheit (IS).....	29
18	Richtlinien zur Sicherheit am Arbeitsplatz	70
19	Künstliche Intelligenz/Maschinelles Lernen (Einschliesslich generativer KI/Agentischer KI)	71
20	Kundenbeschwerden	72
21	Richtlinie für den privaten Handel und private Investitionen	73
22	Rechnungs- und Abrechnungsstandards.....	74
23	Richtlinie zu verpflichtenden Abwesenheiten	75
	ANHANG – DEFINITIONEN	76

1 ALLGEMEINER ÜBERBLICK

1.1. Anforderungen im Allgemeinen

Diese Citi-Anforderungen an Lieferanten („**Anforderungen**“) führen einige der Verpflichtungen auf, die Lieferanten im Rahmen ihrer Geschäftsbeziehung mit Citi erfüllen müssen. Bestimmte Anforderungen gelten für alle Lieferanten, während die Anwendbarkeit anderer Anforderungen auf einen bestimmten Lieferanten von der Art der Produkte und Dienstleistungen abhängt, die der Lieferant für Citi bereitstellt (letztere sind in Abschnitt 1.2 weiter unten zusammengefasst und werden am Anfang jeder darin aufgeführten Bestimmung angegeben). Großgeschriebene Begriffe haben die Bedeutung, die ihnen hierin, einschließlich des beigefügten Anhangs, zugeschrieben wird, es sei denn, eine solche Bedeutung ist hierin nicht angegeben. In diesem Fall haben sie die Bedeutung, die ihnen im Vertrag zugeschrieben wird, wie unten definiert.

Diese Anforderungen sind vertragliche Verpflichtungen aus Lieferantenvereinbarungen mit Citi (einschließlich, aber nicht beschränkt auf Transaktionsdokumente, z. B. Arbeitsaufträge, Lizenzpläne) (jeweils ein „**Vertrag**“) und gelten zusätzlich zu allen in einer Vereinbarung festgelegten Verpflichtungen, allen Verpflichtungen gemäß geltendem Recht (wie dieser Begriff unten definiert wird), allen Mitteilungen von Citi an den Lieferanten, in denen dieser über seine Verpflichtungen gemäß diesen Vereinbarungen informiert wird (jeweils eine „**Mitteilung**“), oder allen zusätzlichen, spezifischeren Anforderungen, die von den Geschäftsbereichen oder Funktionen von Citi umgesetzt werden. Bei Widersprüchen zwischen den vorstehenden Anforderungen und diesen Anforderungen gelten die strengereren Verpflichtungen und Anforderungen. Lieferanten müssen eine proaktive Rolle übernehmen und sich bei allen Fragen zu diesen Anforderungen, einschließlich etwaiger Änderungen daran, etwaiger beantragter Ausnahmen davon oder etwaiger wahrgenommener Konflikte darin oder mit geltendem Recht, an ihren primären Geschäftskontakt bei Citi (oder einen Beauftragten) wenden.

Der Lieferant ist verpflichtet, allen angemessenen Anfragen von Citi bezüglich der Daten, die Citi im Zusammenhang mit den Dienstleistungen oder dem Personal des Lieferanten im Rahmen seiner Verpflichtung zur Einhaltung der geltenden Gesetze benötigt, unverzüglich nachzukommen. Die Nichterfüllung dieser Verpflichtungen durch den Lieferanten gilt als wesentlicher Verstoß gegen die Bedingungen dieser Vereinbarung.

Die Nichteinhaltung dieser Anforderungen oder jeglicher zusätzlicher Anforderungen, die von einem Citi-Unternehmen festgelegt werden, mit dem der Lieferant Geschäfte abwickelt, kann zur Kündigung des Vertrags des Lieferanten mit Citi führen. Darüber hinaus können Verstöße gegen die Anforderungen zugleich Verstöße gegen geltendes Recht darstellen und zivilrechtliche Schadensersatzansprüche von Citi (oder Dritten) sowie strafrechtliche Sanktionen gegen den Lieferanten nach sich ziehen. Der Lieferant darf ohne die schriftliche Zustimmung von Citi die Einhaltung seiner eigenen Richtlinien nicht als Ersatz für seine Verpflichtung zur Einhaltung jeglicher Bestimmungen dieser Anforderungen verwenden.

1.2. Anforderungen an ausgewählte Lieferanten

In der folgenden Tabelle sind bestimmte Anforderungen aufgeführt, die für bestimmte Lieferanten gelten, die die darin genannten Anwendbarkeitskriterien erfüllen. Unten nicht aufgeführte Abschnitte gelten für ALLE Lieferanten.

Abschnitt #	Abschnittstitel	Anwendbarkeit
2	CHANCENGLEICHHEIT BEI DER BESCHÄFTIGUNG/AFFIRMATIVE-ACTION-MASSNAHMEN	Gilt für Verträge und Kaufaufträge, die für die Erfüllung eines Citi-Vertrags mit der US-Bundesregierung erforderlich sind. Bei Unsicherheit, ob der Vertrag oder die Bestellung einen Unterauftrag oder eine Bestellung der Bundesregierung darstellt, ist gegebenenfalls am Anfang oder Ende der Klausel „Sofern zutreffend“ hinzuzufügen.
12	BEKÄMPFUNG VON GELDWÄSCHE	Gilt für Lieferanten, die bestimmte kundenbezogene Dienstleistungen erbringen (d. h. Onboarding, Überprüfung von Kundenkonten und Transaktionen) oder die Lieferung von Daten/Metriken im Zusammenhang mit den vorgenannten Aktivitäten; <u>UND/ODER</u> Lieferanten, die als Vermittler in Bezug auf Bargeld oder Finanzinstrumente tätig sind (z. B. Remote Deposit Capture, Kurierdienste, Geldtransportdienste oder Lockbox-Dienstleistungen).
13	UNTERLAGENVERWALTUNG	Gilt für Lieferanten, die auf Citi-Informationen zugreifen/diese verarbeiten/speichern.
14	GESCHÄFTSKONTINUITÄT	Gilt für Lieferanten, die Dienste bereitstellen oder die von Citi genutzte Technologieinfrastruktur/Anwendungen hosten. Der Citi Business Activity Owner (BAO) ist dafür verantwortlich, dem Lieferanten die Anwendbarkeit und die COB-Anforderungen mitzuteilen.
15	GLOBALE STANDARDS FÜR HINTERGRUNDÜBERPRÜFUNGEN	Gilt für Lieferanten, die Dienstleistungen für Citi erbringen.
16	KOSTEN	Gilt für Lieferanten, die vertraglich berechtigt sind, erstattungsfähige Geschäftsausgaben geltend zu machen.
17	INFORMATIONSSICHERHEIT (IS)	Gilt für Lieferanten, einschließlich Subunternehmer, die auf Informationen von Citi zugreifen, diese verarbeiten, verwalten oder speichern; <u>UND/ODER</u> Lieferanten, die als Host für internetbasierte Anwendungen der Marke Citi verantwortlich sind; <u>UND/ODER</u> Lieferanten mit Konnektivität zu den Netzwerkressourcen von Citi;
18	RICHTLINIEN ZUR SICHERHEIT AM ARBEITSPLATZ	<u>UND/ODER</u> Lieferanten, die unbegleiteten Zugang zu den Einrichtungen von Citi benötigen.
19	KÜNSTLICHE INTELLIGENZ/MASCHINELLES LERNEN (einschließlich generativer KI/agentischer KI)	Gilt für Lieferanten, die Künstliche Intelligenz/Maschinelles Lernen (KI/ML), wie von Citi definiert, in einem beliebigen Teil des von ihnen bereitgestellten Produkts bzw. der von ihnen bereitgestellten Dienstleistung einsetzen.
20	RICHTLINIE FÜR DEN PRIVATEN HANDEL UND PRIVATE INVESTITIONEN	Gilt für Lieferanten, die im Rahmen ihrer beruflichen Aufgaben bei Citi regelmäßigen Zugriff auf MNPI benötigen.
23	RICHTLINIE ZU VERPFLICHTENDEN ABWESENHEITEN	Diese Richtlinie gilt für Nicht-Mitarbeiter („Nichtbeschäftigte“), die sensible

Abschnitt #	Abschnittstitel	Anwendbarkeit
		Positionen (wie im Glossar definiert) bekleiden („Nichtbeschäftigte in sensiblen Positionen“), sowie für die direkten Vorgesetzten und Aufsichtspersonen von Mitarbeitern in sensiblen Positionen („Manager“) und die geschäftlichen Ansprechpartner von Citi für Nichtbeschäftigte in sensiblen Positionen.

2 CHANCENGLEICHHEIT BEI DER BESCHÄFTIGUNG

2.1 Chancengleichheit bei der Beschäftigung.

Citi hat Richtlinien entwickelt, die darauf abzielen, allen qualifizierten Personen gleiche Beschäftigungschancen zu gewährleisten, unabhängig von Rasse, Hautfarbe, Religion, Geschlecht, sexueller Orientierung, Geschlechtsidentität, nationaler Herkunft, Staatsangehörigkeit, Einwanderungsstatus, Alter, Familienstand, genetischen Informationen, Behinderung, geschütztem Veteranenstatus oder anderen gesetzlich geschützten Merkmalen.

Lieferanten müssen die Anforderungen aller geltenden Nichtdiskriminierungsgesetze und -vorschriften einhalten und dafür sorgen, dass ihr Personal diese einhält, einschließlich, aber nicht beschränkt auf alle Gesetze oder Vorschriften, deren Einhaltung Citi dem Lieferanten schriftlich mitteilt.

Die Lieferanten müssen die US-Grundsatzerklärung von Citi zur Chancengleichheit bei der Beschäftigung prüfen und geeignete Maßnahmen im Einklang damit ergreifen. Diese Erklärung ist unter www.citigroup.com/global/eeo-aa-policy abrufbar.

2.2 Regierungsaufträge

Verträge und Bestellungen, die für die Erfüllung eines Citi-Vertrags mit der Bundesregierung erforderlich sind, müssen die folgende Klausel wörtlich und in Fettschrift enthalten, wie unten dargestellt. (Wenn Sie sich nicht sicher sind, ob es sich um einen Untervertrag/eine Bestellung der Bundesregierung handelt, fügen Sie am Anfang des Abschnitts „Sofern zutreffend“ hinzu.)

[Sofern zutreffend] Der Lieferant hält alle geltenden Bundesgesetze gegen Diskriminierung ein und versichert, dass er keine Programme betreibt, die gegen geltende Bundesgesetze gegen Diskriminierung verstoßen.

2.3 Anhang zu Regierungsaufträgen

Verträge und Bestellungen, die für die Erfüllung eines Citi-Vertrags mit der Bundesregierung erforderlich sind, müssen im Anhang des Untervertrags oder der Bestellung den folgenden Hinweis enthalten. (Wenn Sie sich nicht sicher sind, ob es sich um einen Unterauftrag/eine Bestellung der Bundesregierung handelt, fügen Sie am Ende des nachstehenden Hinweises eher „Sofern zutreffend“ hinzu.)

Als Auftragnehmer der Bundesregierung informiert Citigroup hiermit den unterzeichnenden Auftragnehmer oder Lieferanten schriftlich über unsere

Verpflichtungen zur Chancengleichheit am Arbeitsplatz gegenüber geschützten Veteranen und Menschen mit Behinderungen. Citigroup hält sich in vollem Umfang an Abschnitt 503 des Rehabilitation Act und des Vietnam Era Veterans' Readjustment Assistance Act sowie an die jeweils geltenden Bestimmungen gemäß 41 CFR § 60-741 und 41 CFR § 60-300. Unsere Grundsatzerklärung zur Chancengleichheit am Arbeitsplatz finden Sie unter www.citigroup.com/global/eeo-aa-policy. Fragen zu unserer Erklärung zur Gleichstellung am Arbeitsplatz können an die in unserer Erklärung angegebene Kontaktadresse gerichtet werden.

[Sofern zutreffend] Wir bitten Sie, geeignete Maßnahmen im Einklang mit unserer Grundsatzerklärung und den geltenden Vorschriften zu ergreifen.

3 ANTI-BESTECHUNG UND KORRUPTIONSBEKÄMPFUNG (AB&C)

Citi verfügt über Richtlinien, Verfahren und interne Kontrollen, die in angemessener Weise darauf ausgelegt sind, die geltenden Gesetze zu Anti-Bestechung und Korruptionsbekämpfung (AB&C) einzuhalten, und verbietet Bestechung oder Beschleunigungszahlungen in jeder Form strikt. Lieferanten (einschließlich Geschäftsvermittler), deren Personal und alle Personen, die direkt oder indirekt im Namen von Citi handeln, müssen ihre Aktivitäten im Einklang mit den höchsten ethischen Standards und in Übereinstimmung mit dem US-amerikanischen Foreign Corrupt Practices Act (FCPA), dem UK Bribery Act (UKBA) in der jeweils gültigen Fassung sowie allen anderen geltenden lokalen Anti-Korruptionsgesetzen der Länder durchführen, in denen Citi tätig ist.

Weder der Lieferant noch einer seiner Mitarbeiter, die im Auftrag von Citi oder im Zusammenhang mit einer Vereinbarung oder Beziehung des Lieferanten mit Citi tätig sind, (i) werden Zahlungen, Leistungen, Vorteile oder sonstige Wertgegenstände an eine Person leisten, gewähren, genehmigen oder anbieten; oder (ii) Zahlungen, Leistungen, Vorteile oder sonstige Wertgegenstände von einer Person erhalten oder annehmen, wobei in den Fällen (i)–(ii) jeweils ein Verstoß gegen den FCPA, den UKBA oder andere AB&C-Gesetze vorliegt. Der Lieferant und sein Personal müssen ihre Aktivitäten und Transaktionen im Namen von Citi oder in Verbindung mit einer Vereinbarung oder Beziehung des Lieferanten mit Citi in Übereinstimmung mit den Anforderungen, einschließlich dieses Abschnitts, durchführen. Der Lieferant und sein Personal müssen außerdem ein AB&C-Compliance-Programm sowie Richtlinien und Verfahren aufrechterhalten, die die Einhaltung aller geltenden AB&C-Gesetze gewährleisten sollen.

Eine Übersicht über das AB&C-Programm von Citi finden Sie unter [Citigroup's Investor Relations](#) (unter „Citi-Richtlinien“ „Programm zur Bekämpfung von Bestechung und Korruption“ (AB&C-Programm) auswählen).

4 GESCHENKE UND BEWIRTUNG

Weder Lieferanten noch ihr Personal dürfen Citi-Mitarbeitern Geschenke oder Wertgegenstände (einschließlich Bewirtung) zur Verfügung stellen, wenn dies zu einem tatsächlichen oder scheinbaren Interessenkonflikt oder einer Gegenleistung führen, die Integrität oder das Urteilsvermögen des Mitarbeiters beeinträchtigen oder auf andere Weise die Entscheidungsfindung des Mitarbeiters in unzulässiger Weise beeinflussen, den Mitarbeiter dazu veranlassen würde, gegen seine/ihre Pflichten zu handeln, oder anderweitig gegen geltende Gesetze verstoßen würde. Unbeschadet des Vorstehenden muss der Mitarbeiter den Abschnitt „Unzulässige Geschenke und Bewirtung“ des Geschenke- und Bewirtungs-Standards einhalten. Lieferanten und deren Personal dürfen keine Sachgeschenke an Citi-Mitarbeiter ausgeben, die einen Gesamtbetrag von 300 USD pro Person und Kalenderjahr übersteigen.

Gewährt ein Lieferant einem Citi-Mitarbeiter eine geschäftliche Bewirtung (z. B. eine Einladung zu einem Essen, einer sportlichen, kulturellen oder vergleichbaren Veranstaltung), muss der Lieferant bei der Veranstaltung anwesend sein und die Bewirtung muss angemessen, üblich und vernünftig, nicht verschwenderisch sein oder übermäßig häufig stattfinden. Wenn der Lieferant nicht an der Veranstaltung teilnimmt, wird die Bewirtung als Geschäftsgeschenk betrachtet und unterliegt den geltenden Meldeschwellen des Citi-Standards für Geschenke und Bewirtung. Der Lieferant darf im Namen von Citi oder vorgeblich im Namen von Citi weder direkt noch indirekt Wertgegenstände, auch nicht auf eigene Kosten oder auf Kosten eines Citi-Mitarbeiters, irgendeiner Person anbieten oder eine andere Person dazu verleiten, dasselbe zu tun, wenn dies korrupt wäre oder nach vernünftigem Ermessen als korrupt, unangemessen oder als Verstoß gegen geltendes Recht angesehen werden würde.

5 LIEFERANTENENGAGEMENT UND LIEFERANTENPRINZIPIEN

<https://www.citigroup.com/citi/suppliers/> Citi engagiert sich mit Lieferanten bei einer Reihe von Initiativen und um das Bewusstsein für das Beschaffungsprogramm von Citi mit potenziellen Lieferanten aus Gemeinschaften, in denen wir tätig sind, zu schärfen. Darüber hinaus dienen diese Engagements dazu, vielversprechende Lieferanten zu identifizieren, insbesondere solche, die innovative Lösungen zur Bewältigung neu entstehender Geschäftsprobleme vorantreiben. Weitere Informationen zu den Erwartungen von Citi an seine Lieferanten finden Sie auf der Seite [Doing Business with Citi](#) unter:

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 VERBOT DER MODERNEN SKLAVEREI

Citi hat sich dazu verpflichtet, Praktiken aufrechtzuerhalten, die darauf abzielen, das Risiko des Auftretens moderner Sklaverei und Menschenhandels innerhalb seiner

Organisation oder in seinen Lieferketten zu erkennen und zu verhindern. Die Lieferanten von Citi müssen die nachstehend aufgeführten Anforderungen einhalten und wirksame unternehmensweite Richtlinien, Verfahren und/oder Praktiken entwickeln, um das Risiko moderner Sklaverei und Menschenhandel innerhalb ihrer eigenen Betriebsabläufe und Lieferketten zu erkennen und zu verhindern. Lieferanten müssen auf Anfrage von Citi den Fragebogen zur Unternehmensverantwortung ausfüllen, einschließlich aller zusätzlichen Informationen, die erforderlich sind, um Citi in die Lage zu versetzen, das Risiko und alle potenziellen Maßnahmen zur Risikominderung zu bewerten, insbesondere bei Lieferanten in Sektoren und Regionen mit höherem Risiko. Die Subunternehmer des Lieferanten sind verpflichtet, denselben Prozess zu befolgen.

6.1 Vermeidung von Kinderarbeit

Lieferanten dürfen keine Kinderarbeit einsetzen. Der Begriff „Kind“ bezeichnet jede Person unter dem Mindestalter für die Zulassung zur Beschäftigung gemäß den geltenden Gesetzen oder in Ermangelung solcher Gesetze jede Person unter 15 Jahren oder unter dem Alter, in dem die Schulpflicht endet, je nachdem, welches Alter höher ist. Vorbehaltlich des vorrangigen Verbots der Kinderarbeit ist bei der Beschäftigung von Arbeitnehmern unter 18 Jahren besonders darauf zu achten, dass die ihnen übertragenen Aufgaben und die Arbeitsbedingungen so gestaltet sind, dass sie weder durch ihre Arbeit noch durch ihre Arbeitsbedingungen unmittelbar oder mittelbar körperlichen, geistigen oder sonstigen Schaden nehmen.

6.2 Frei gewählte Beschäftigung

Der Lieferant hat sicherzustellen, dass die Arbeiter nicht gezwungen, geistig oder körperlich genötigt, in Schuldknecht- oder Leibeigenschaft genommen werden oder zu jeglicher unfreiwilligen Gefängnis- oder Sklavenarbeit, verkaufter oder erzwungener Arbeit jeder Art einschließlich erzwungener Überstunden gebracht werden. Alle Arbeiten müssen freiwillig ausgeführt werden. Die Verpflichtungen des Lieferanten umfassen unter anderem die Sicherstellung der folgenden Punkte:

1. **Verträge, Löhne und Arbeitszeiten:** Arbeitnehmern sind die Bedingungen ihrer Beschäftigung oder Beauftragung in einem schriftlichen Dokument vorzulegen, das für sie leicht verständlich ist und ihre Rechten und Pflichten klar regelt. Dieses schriftliche Dokument muss unter anderem transparente Regelungen zu Löhnen, Überstundenvergütung, Entgeltzahlungszeiträumen, Arbeitszeiten sowie zu Ansprüchen auf Ruhepausen und Urlaub enthalten. Solche schriftlichen Bedingungen müssen dem Arbeitnehmer vor Arbeitsbeginn zur Verfügung gestellt werden, müssen vom Arbeitgeber eingehalten werden und müssen den Branchenstandards sowie den Mindestanforderungen der geltenden Gesetze und Tarifverträge entsprechen, in denen die Arbeit ausgeführt wird.
2. **Recht auf freie Beendigung der Arbeit:** Arbeitnehmer müssen das Recht haben, ihre Beschäftigung frei zu beenden, gegebenenfalls nach Ablauf einer angemessenen Kündigungsfrist entsprechend einschlägigen Gesetzen und Tarifverträgen und ohne Verhängung unstatthafter Strafen.

3. **Unmenschliche Behandlung:** Arbeitnehmer, ihre Familien und nahe Angehörige dürfen keiner rauen oder unmenschlichen Behandlung, etwa körperlicher Bestrafung, körperlicher, seelischer oder sexueller Gewalt oder Nötigung, Beleidigung, Belästigung oder Einschüchterung ausgesetzt werden. Gastarbeiter, ihre Familien und nahe Angehörige dürfen aufgrund ihrer Staatsangehörigkeit keiner Diskriminierung bezüglich der Bestimmungen oder Bedingungen ihrer Arbeit ausgesetzt sein.
4. **Löhne, Zusatzleistungen und Arbeitsstunden:** Die Vergütung sollte mit allen einschlägigen Lohngesetzen übereinstimmen, einschließlich solcher, die sich auf Mindestlöhne, Überstunden und gesetzlich vorgeschriebene Zusatzleistungen beziehen. Mitarbeiter sollten ihre Vergütung vollständig, fristgerecht und mit einer transparenten Entgeltabrechnung erhalten. Vergütungen oder Zusatzleistungen dürfen weder als Disziplinarmaßnahme gekürzt noch einbehalten werden. Arbeitswochen sollten nicht die durch lokale Gesetze festgelegte Grenze überschreiten, Überstunden müssen freiwillig erfolgen, innerhalb rechtlicher Grenzen liegen, und die Ablehnung von Überstunden darf nicht bestraft werden.
5. **Keine Beschlagnahmung von Ausweisdokumenten:** Ausweis- oder Reisepapiere, Pässe oder sonstige amtliche Unterlagen oder Wertgegenstände von Arbeitnehmern dürfen nicht als Voraussetzung einer Beschäftigung beschlagnahmt oder zurückgehalten werden, auch darf die Zurückbehaltung von Eigentum weder unmittelbar noch mittelbar dazu verwendet werden, die Freiheit von Arbeitnehmern einzuschränken oder Sklaverei am Arbeitsplatz entstehen zu lassen.
6. **Keine Vermittlungsgebühren oder Schuldknechtschaft** Gebühren oder Kosten im Zusammenhang mit dem Einstellen von Mitarbeitern (darunter Gebühren für Arbeitsvisa, Reisekosten und Kosten der Bearbeitung von Unterlagen) dürfen Arbeitnehmern weder mittelbar noch unmittelbar in Rechnung gestellt werden. In ähnlicher Weise dürfen Arbeitnehmern keine Zahlungen auferlegt werden, die absichtlich oder im Ergebnis zur Schaffung von Sklaverei am Arbeitsplatz führen, darunter Sicherheitsleistungen oder erzwungene Schuldenrückzahlung durch Arbeit. Wird festgestellt, dass Arbeitnehmern Gebühren oder Kosten im Zusammenhang mit dem Einstellungsverfahren berechnet wurden oder ihnen im Verlauf des Beschäftigungsverhältnisses entstanden sind, muss der Lieferant angemessene Maßnahmen ergreifen, um sicherzustellen, dass diese Kosten unverzüglich erstattet werden. Ist die Anwerbung von Arbeitnehmern erforderlich, die über einen Dritten, beispielsweise eine Arbeitsvermittlung, beschäftigt werden, dürfen nur seriöse Arbeitsvermittlungsagenturen beauftragt werden. Wenn Arbeitnehmer direkt eingestellt werden sollen, dürfen nur seriöse Personalvermittlungsagenturen beauftragt werden. Das Verbot, Arbeitnehmern Anwerbungsgebühren aufzuerlegen, gilt für alle Personalvermittler, Vermittlungsagenturen und Untervermittler. Lieferanten müssen über

Kontrollen verfügen, um die Einhaltung der Vorschriften zu gewährleisten.

Freizügigkeit: Arbeitnehmer müssen sich ohne unzumutbare Einschränkungen frei bewegen können und dürfen nicht physisch an den Arbeitsplatz oder andere vom Arbeitgeber kontrollierte Orte (z. B. Wohnblocks) gebunden sein. Es darf Arbeitnehmern nicht vorgeschrieben werden, dass sie in vom Arbeitgeber beherrschten Räumen wohnen, es sei denn, dies ist wegen des Ortes oder der Art der zu leistenden Arbeit erforderlich.

7. **Beschwerden ohne Vergeltung:** Arbeitnehmern steht es frei, sich bei ihren Arbeitgebern über die Behandlung durch den Arbeitgeber zu beschweren, und die Arbeitnehmer dürfen keine Nachteile, Vergeltungsmaßnahmen oder Schikanen erleiden, weil sie eine Beschwerde vorgebracht haben.

7 PERSONAL DES LIEFERANTEN

7.1 Schulung, Zuweisung, Neuzuweisung und Management des Personals des Lieferanten

Der Lieferant wird eine angemessene Anzahl von Personen mit geeigneter Ausbildung, Schulung, Erfahrung und Fertigkeit einsetzen, um die Dienstleistungen auf die effektivste Weise im Einklang mit dem Vertrag zu erbringen, und wird die Qualifikationen dieser Personen auf Anfrage nachweisen. Nachdem das Personal einem Projekt zugewiesen wurde, wird der Lieferant ohne die vorherige schriftliche Zustimmung von Citi kein Personal neu zuweisen oder für andere Angelegenheiten einsetzen, die seine Verfügbarkeit für die Arbeit an dem Projekt einschränken, und er wird das Personal im Allgemeinen so für Projekte zuweisen, dass Unterbrechungen durch die Notwendigkeit einer Neuausrichtung minimiert werden. Der Lieferant stellt sicher, dass sein Personal sich weder als Mitarbeiter oder Beauftragte von Citi ausgibt noch versucht, für irgendeinen Zweck als Mitarbeiter von Citi behandelt zu werden, insbesondere nicht im Hinblick auf Ansprüche auf von Citi bereitgestellte Zusatzleistungen, Erwerbsunfähigkeitsleistungen, Sozialversicherungsabgaben oder -leistungen, Bundesarbeitslosensteuern, Arbeitslosenversicherungsleistungen der Bundesstaaten oder den Einbehalt von Bundeseinkommensteuer. Der Lieferant ist allein für alle arbeitgeberbezogenen Pflichten in Bezug auf sein Personal verantwortlich, insbesondere die Aufrechterhaltung des erforderlichen Versicherungsschutzes, die Einreichung aller anwendbaren Steuererklärungen und die Entrichtung aller erforderlichen Zahlungen und Abgaben in einer Weise, die dem Status des Lieferanten als unabhängiger Auftragnehmer entspricht.

7.2 Austausch des Personals des Lieferanten

Der Lieferant wird alle von ihm für ein Projekt zugewiesenen Mitarbeiter abziehen und ersetzen, wenn Citi dem Lieferanten mitteilt, dass diese Mitarbeiter aus nicht diskriminierenden Gründen für Citi nicht akzeptabel sind. Der Lieferant erklärt sich ferner damit einverstanden, alle einem Projekt zugewiesenen Mitarbeiter zu entfernen und zu ersetzen und sie von der Erbringung von Dienstleistungen für Citi (oder von jeglicher Verantwortung in Bezug auf die Erbringung oder Beaufsichtigung von Dienstleistungen)

unverzüglich auszuschließen, wenn sie nicht in der Lage oder bereit sind, die Dienstleistungen rechtzeitig und professionell zu erbringen.

7.3 Personalrichtlinien des Lieferanten

Der Lieferant sichert zu, gewährleistet und verpflichtet sich, dass er umfassende Richtlinien und Verfahren für die Qualifizierung seines Personals, das natürliche Personen sind und für die Erbringung von Vor-Ort-Dienstleistungen für Citi eingesetzt wird, unterhält und effektiv verwaltet, und dass diese Richtlinien und Verfahren die Überprüfung der Arbeitsberechtigung, Hintergrundüberprüfungen der Beschäftigungsgeschichte und strafrechtlicher Verurteilungen, wie hierin weiter ausgeführt, sowie Drogentests vor der Einstellung umfassen, und zwar in dem Umfang, der nach geltendem Recht und anwendbaren Tarifverträgen zulässig ist. Unbeschadet der Allgemeingültigkeit des Vorstehenden sichert der Lieferant ferner zu, gewährleistet und verpflichtet sich, über Kontrollen und Verfahren zu verfügen, die die vollständige Einhaltung aller geltenden einwanderungsrechtlichen Vorschriften durch den Lieferanten sicherstellen, einschließlich der Überprüfung, dass sämtliches dem Einsatz bei Citi zugewiesene Personal des Lieferanten während der gesamten Einsatzdauer zur Arbeitsaufnahme berechtigt ist und alle geltenden einwanderungsrechtlichen Vorschriften uneingeschränkt einhält. Auf Verlangen wird der Lieferant Citi unverzüglich einen schriftlichen Nachweis über die Arbeitsberechtigung eines oder aller dem Einsatz bei Citi zugewiesenen Mitarbeiter des Lieferanten sowie über die Einhaltung der geltenden einwanderungsrechtlichen Vorschriften vorlegen und alle Mitarbeiter, die nicht über eine den geltenden gesetzlichen Bestimmungen entsprechende Arbeitsberechtigung verfügen, durch entsprechend qualifizierte Ersatzkräfte ersetzen, einschließlich der Durchführung aller erforderlichen Schulungen und Einweisungen, um die rechtzeitige und ordnungsgemäße Erbringung der Dienstleistungen sicherzustellen, und zwar in jedem Fall ohne zusätzliche Kosten für Citi.

7.4 Eigentümerstruktur des Lieferanten

Zur Einhaltung der geltenden Gesetze und Vorschriften in den Rechtsordnungen, in denen Citi geschäftlich tätig ist, sind Lieferanten auf Verlangen von Citi verpflichtet, Angaben zu den Eigentümern, unabhängig davon, ob es sich um natürliche oder juristische Personen handelt, einschließlich der unmittelbaren Eigentümer des Lieferanten sowie des wirtschaftlich Berechtigten, der direkt oder indirekt durch Einfluss oder auf andere Weise Eigentum oder Kontrolle über den Auftrag, das Produkt oder die Dienstleistung ausübt.

8 BETRUGSBEKÄMPFUNG

Im Zusammenhang mit den Bemühungen von Citi, Betrugsrisiken zu erkennen und zu mindern („Betrugsbekämpfung“).

8.1 Alle Lieferanten müssen:

1. Mit allen Citi-Untersuchungen von vermutetem oder angeblichem Diebstahl, Betrug oder anderen potenziellen kriminellen Handlungen oder Fehlverhalten sowie mit jeder Strafverfolgung von betrügerischem oder kriminellm Verhalten im vollen Umfang des Gesetzes zusammenarbeiten.
2. Eine rechtzeitige Meldung und Weiterleitung potenzieller Betrugsfälle an Citi durch die [Ethics Hotline](#) sicherstellen. Dazu gehören unter anderem

versuchter, mutmaßlicher, angeblicher oder tatsächlicher Diebstahl, Betrug (z. B. die wissentliche Übermittlung falscher, ungenauer oder falsch dargestellter Daten in Bezug auf den Lieferanten, Abrechnungsschemata, das Verschwinden von Geldern oder Wertpapieren usw.), kriminelle Aktivitäten oder Fehlverhalten, an denen Citi, ein Citi-Mitarbeiter, ein Citi-Lieferant oder -Vertreter oder ein Nicht-Mitarbeiter von Citi (z. B. Zeitarbeiter und Auftragnehmer) beteiligt ist.

3. Die Überwachung und Beaufsichtigung durch Citi und seine Vertreter genehmigen und die von Citi – und den Strafverfolgungsbehörden – geführten Untersuchungen zu potenziell betrügerischen Aktivitäten, an denen dieser Lieferant beteiligt war, unterstützen.
4. Rechtzeitig alle Interessenkonflikte (einschließlich Interessenkonflikte zwischen Lieferanten/Mitarbeitern des Lieferanten und/oder Citi-Mitarbeitern) melden, von denen die Lieferanten Kenntnis erhalten; und
5. Die Betrugspräventionsprozesse von Citi während der Einrichtung oder Aktualisierung eines Bankkontos eines Lieferanten im Lieferantenzahlungssystem von Citi unterstützen.

8.2 Darüber hinaus sind Lieferanten, die Dienstleistungen erbringen, die von Natur aus einem höheren Betrugsrisiko ausgesetzt sind, zu Folgendem **verpflichtet**:

1. Ein Betrugsrisiko-Managementprogramm zu dokumentieren und zu befolgen, in dem die wesentlichen Betrugsrisiken für die von Citi bereitgestellten Dienste und die zur Eindämmung dieser Risiken geltenden Kontrollen und Verfahren bestimmt werden.
2. Eine Schulung zur Sensibilisierung für Betrugsrisiken (innerhalb von 90 Kalendertagen nach der Einstellung und danach jährlich) zu absolvieren und Mitarbeiter zu den spezifischen Betrugsrisiken zu schulen, die für die für Citi erbrachten Dienstleistungen relevant sind.
3. Versuche von Betrug überwachen und wirksame Kontrollen zur Minderung des Betrugsrisikos im Zusammenhang mit den für Citi erbrachten Dienstleistungen aufrechterhalten, Verfahren für diese Kontrollen dokumentieren und die Wirksamkeit der Kontrollen fortlaufend überprüfen sowie etwaige Mängel dem Business Activity Owner (BAO) melden.
4. Alle erforderlichen Informationen für die Due Diligence/laufende Überwachung/Bewertung des Betrugsrisikos an den Business Activity Owner (BAO) bereitstellen.
5. Die Due Diligence umfasst die Vorlage zur Bewertung der Auswirkungen von Betrug durch Dritte („TP-FIAT“), die dazu dient, die Fähigkeiten der Lieferanten im Hinblick auf die Minderung des Betrugsrisikos zu kontrollieren. Diese Betriebsanweisung beschreibt eine Reihe von Schritten, die vom Business Activity Owner (BAO) oder Third-Party Officer (TPO) und dem Fraud Risk Management Officer („FRMO“) durchzuführen sind, um Betrugsrisiken zu identifizieren und zu managen.

8.3 Zu den Lieferanten mit einem von Natur aus höheren Betrugsrisiko gehören unter anderem diejenigen, die:

1. Zugriff auf Daten mit der Klassifizierung „Vertraulich“ oder höher haben (wenn sie nicht unter der direkten Kontrolle oder Aufsicht von Citi stehen), die verwendet werden können, um Betrug zu ermöglichen, wie z. B. Zugriff auf interne Konten, Finanztransaktionen, Bargeldtransaktionen.
2. Konnektivität zu Citi-Netzwerken/-Systemen haben; und
3. die Bereitstellung, Unterstützung oder den Zugang zu Diensten und Funktionen bieten, die auf Betrug ausgelegt sind oder ihn ermöglichen können, einschließlich:
 - a) Identifikation, Onboarding oder Bearbeitung von Anträgen neuer Kunden.
 - b) Citi oder Kundenzahlungs-/Geldübertragungsaktivitäten und/oder die Authentifizierung von Citi-Kunden, auf diese Dienste zuzugreifen;
 - c) Vornehmen, Überprüfen und Durchführen von Änderungen an Citi-Daten oder Citi-Kundendaten (z. B. demografische) Daten;
 - d) Bereitstellung, Betreuung oder Autorisierung von Transaktionsinstrumenten (z. B. Debit-/Kreditkarten, eWallets, Scheckbücher usw.);
 - e) Bereitstellung oder Unterstützung operativer Aktivitäten zur Betrugsbekämpfung an Citi in Bezug auf die Verhinderung, Aufdeckung oder Reaktion auf Betrugsereignisse;
 - f) Bereitstellung von physischem Zugang zu Bargeld, Finanzinstrumenten und Vermögenswerten/physischen Gütern;
 - g) Unbegleiteter Zugang oder Zugang außerhalb der Öffnungszeiten in Citi-Einrichtungen;
 - h) Finanzberichte: Buchhaltungsaktivitäten, wie z. B. Buchungen in der GL/SL;
 - i) Annahme und Ausgabe von Belohnungen für Aktivitäten mit Anreiz.

9 UMGANG MIT MEDIEN UND ÖFFENTLICHE AUFTRITTE

Citi Enterprise Services and Public Affairs ist die einzige Abteilung, die befugt ist, im Namen von Citi Pressemitteilungen oder öffentliche Erklärungen herauszugeben. Lieferanten dürfen keine Pressemitteilungen herausgeben, in denen Citi, ein Vertrag oder eine Vereinbarung zwischen einem Lieferanten und Citi oder die von Citi von einem Lieferanten bezogenen Produkte und Dienstleistungen direkt oder indirekt genannt werden. Lieferanten dürfen ohne vorherige schriftliche Zustimmung ihres primären Geschäftskontakts bei Citi keinerlei PR-Aktivitäten in Bezug auf Citi mit Kunden, Mitarbeitern von Citi, anderen Lieferanten von Citi, anderen Kunden von Lieferanten oder sonstigen Drittparteien zustimmen oder sich an solchen beteiligen.

Lieferanten dürfen ohne vorherige schriftliche Genehmigung ihres primären Citi-Geschäftskontakts und des Senior Country Public Affairs Officer keine Materialien in schriftlicher oder elektronischer Form (einschließlich Bücher, Artikel, Podcasts, Webcasts, Blogs, Website-Beiträge, Fotos, Videos, soziale Medien oder andere Medien)

veröffentlichen oder posten, Reden halten oder Interviews geben oder öffentliche Auftritte absolvieren, in denen Citi, die Geschäftstätigkeit von Citi, Kunden, Produkte oder Dienstleistungen erwähnt werden.

Unabhängig davon, ob sie in Verbindung mit der Erbringung von Dienstleistungen oder Produkten für Citi stehen oder nicht, dürfen die Lieferanten keine geschützten Kennzeichen, Warenzeichen, Dienstleistungsmarken, Handelsnamen, Logos, Symbole oder Markennamen von Citi verwenden, ohne in jedem Fall die vorherige schriftliche Zustimmung von Citi einzuholen. Lieferanten dürfen den Namen, das Logo oder die Markenzeichen, Einrichtungen oder Beziehungen von Citi nicht zum eigenen Vorteil oder für eine Tätigkeit außerhalb von Citi (einschließlich auf Briefköpfen, privaten Websites, Blogs oder anderen sozialen Netzwerken) verwenden. Lieferanten dürfen den Namen oder die Räumlichkeiten von oder die Beziehungen zu Citi auch nicht für gemeinnützige oder ehrenamtliche Zwecke verwenden.

10 SCHRIFTLICHE ELEKTRONISCHE KOMMUNIKATION

Bei der Interaktion mit Citi-Mitarbeitern oder bei der Erfüllung ihrer Verpflichtungen für oder im Namen von Citi dürfen Lieferanten nur solche schriftlichen elektronischen Kommunikationsgeräte, -systeme und -dienste verwenden, die von Citi genehmigt wurden. Neue, erweiterte oder geänderte Citi eComm-Kanäle, ob als eigenständige Tools oder in eine umfassendere Plattform integriert, die von Citi oder Drittanbietern bereitgestellt wird, müssen gemäß den geltenden Citi-Anforderungen genehmigt werden, über die der Lieferant von seinem BAO schriftlich informiert wurde. Die Kommunikation von Citi-Geschäften mit Citi-Mitarbeitern auf nicht von Citi genehmigten Messaging-Plattformen, wie WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber und anderen interaktiven elektronischen Plattformen, ist verboten.

Darüber hinaus sollten Lieferanten keinen Anspruch auf Privatsphäre in Bezug auf schriftliche elektronische Kommunikation haben, die über von Citi zur Verfügung gestellte Kommunikationsgeräte, -systeme und -dienste erstellt, entdeckt, verwendet, abgerufen, heruntergeladen, gespeichert, übertragen, empfangen oder gelöscht wird. Citi darf elektronische Kommunikationsgeräte, -systeme und -dienste sowie die elektronische Kommunikation überwachen. Solche elektronischen Kommunikationen sind Eigentum von Citi und können in Übereinstimmung mit den geltenden Anforderungen an die Aufbewahrung von Unterlagen aufbewahrt werden (vorbehaltlich lokaler Gesetze und Vorschriften).

<https://policydirectory.citi.net/cpd/layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 POLITISCHE TÄTIGKEIT UND BEITRÄGE

Eine Vielzahl von Gesetzen, wie beispielsweise zu ausländischer Einflussnahme, Wahlkampffinanzierung, Geschenken und Bewirtungen, Lobbying auf gesetzgeberischer, gesellschaftlicher, gemeinnütziger und regulatorischer Ebene, Beschaffung, Pay-to-Play sowie Wertpapierangelegenheiten regeln politische Aktivitäten

und damit verbundene Offenlegungspflichten von Citi und seinen Lieferanten. Jegliche politische Aktivität von Lieferanten, die nicht mit den relevanten Richtlinien oder Standards, Gesetzen oder Vorschriften von Citi übereinstimmt, ist verboten.

Politische Aktivitäten umfassen unter anderem:

1. Die Leistung von politischen Beiträgen durch Unternehmen oder Einzelpersonen, das Einwerben von politischen Beiträgen, die Verwendung von Unternehmensgeldern oder -ressourcen (z. B. Einrichtungen, Ausrüstung, Software oder Personal) oder die freiwillige Erbringung von persönlichen Dienstleistungen während der Unternehmenszeit im Namen eines Kandidaten, der für ein öffentliches Amt kandidiert, eines politischen Parteikomitees oder eines politischen Komitees;
2. Lobbyarbeit oder Kontaktaufnahme zu Amtsträgern, sei es direkt oder über Dritte, einschließlich Versuchen, Amtsträger, Gesetzgebung und, je nach Rechtsordnung, auch die Regulierung durch Behörden oder die Vergabe öffentlicher Aufträge zu beeinflussen; oder
3. Das Streben, die Annahme oder das Halten eines politischen Amtes, das mit einer Regierung verbunden ist, einschließlich eines Regierungsgremiums, einer Kommission oder einer ähnlichen Organisation.

Ohne vorherige schriftliche Genehmigung der Abteilung „Government Affairs Global Operations Control“ von Citi (ggacontrol@citi.com) dürfen Lieferanten keine politischen Aktivitäten im Namen (oder angeblich im Namen) von Citi oder seinen Kunden durchführen oder betreiben. Obwohl Citi für vertraglich vereinbarte und zulässige Dienstleistungen des Lieferanten im Zusammenhang mit politischen Aktivitäten, wie z. B. Lobbyarbeit, eine Gebühr zahlen und/oder Kosten aus eigener Tasche erstatten kann, wird Citi niemals einen Lieferanten oder einen seiner Mitarbeiter für persönliche oder unternehmenspolitische Beiträge jeglicher Art entschädigen.

12 BEKÄMPFUNG VON GELDWÄSCHE („AML“)

Gilt für Lieferanten, die bestimmte kundenbezogene Dienstleistungen erbringen (d. h. Onboarding, Kundenkonto- und Transaktionsprüfungen) oder Daten/Kennzahlen im Zusammenhang mit den vorstehend genannten Aktivitäten bereitstellen; UND/ODER als Vermittler in Bezug auf Finanztransaktionen oder Finanzinstrumente tätig sind (z. B. Remote Deposit Capture, Kurierdienste, Geldtransportdienste oder Lockbox-Dienstleistungen, elektronische Überweisungen, digitale Vermögenswerte).

12.1 AML-Verpflichtungen:

1. Einhaltung der Citi-Prozesse und geltenden Gesetze:

- Aufrechterhaltung und Einhaltung der Prozesse und Verfahren von Citi, die dazu bestimmt sind, die Anforderungen der geltenden Gesetze zu erfüllen, einschließlich (i) des Gramm-Leach-Bliley Act und der darunter

erlassenen Vorschriften; (ii) des USA PATRIOT Act und der darunter erlassenen Vorschriften; (iii) aller Gesetze oder Vorschriften, die sich mit Geldwäsche befassen; und (iv) aller Gesetze oder Vorschriften, die sich auf Wirtschaftssanktionen beziehen. Diese Richtlinien und Verfahren beziehen sich auf die Aufgaben und Verantwortlichkeiten bei der Bekämpfung von Geldwäsche, einschließlich der Verpflichtung, jede beobachtete Aktivität, die im Zusammenhang mit finanziellen Aktivitäten, Transaktionen und der Annahme von Bargeld ungewöhnlich oder potenziell ungewöhnlich erscheint, unverzüglich zu melden.

2. Jährliche Schulungs- und Programmelemente für das Personal:

- Es ist sicherzustellen, dass die Mitarbeiter, die Dienstleistungen für Citi erbringen, eine jährliche Schulung in Bezug auf die Aufgaben und Verantwortlichkeiten bei der Bekämpfung von Geldwäsche erhalten, einschließlich der Verpflichtung, jede beobachtete Aktivität, die im Zusammenhang mit finanziellen Aktivitäten, Transaktionen und der Annahme von Bargeld ungewöhnlich oder potenziell ungewöhnlich erscheint, unverzüglich zu melden. Schulungen haben unter anderem folgende Elemente zu beinhalten:
 - a. Meldung und Eskalation verdächtiger Aktivitäten.
 - b. Ein „Kennen Sie Ihren Kunden“-Programm (KYC), einschließlich eines Kundenidentifizierungsprogramms (CIP), Sanktionen und Namensprüfung, Sorgfaltspflicht gegenüber Kunden (CDD), erweiterte Sorgfaltspflicht und die Identifizierung und Überprüfung von **wirtschaftlich Berechtigten (UBO)**.
 - c. Transaktionsüberwachung über alle relevanten Finanzinstrumente und Aktivitäten hinweg.
 - d. Periodisches Berichtswesen/periodische Kennzahlen, einschließlich Berichterstattung über rechtliche und regulatorische Änderungen sowie wesentliche AML-Programmänderungen.
 - e. Tests und Kontrollen der Wirksamkeit des AML-Programms, einschließlich Besuche vor Ort.

3. Einhaltung von Vertragsbestimmungen:

- Einhaltung sämtlicher Vertragsbestimmungen, die ein vom Lieferanten einzuführendes Programm festlegen.

4. Sofortige Meldung mutmaßlicher Verstöße:

- Unverzügliche schriftliche Meldung jedes mutmaßlichen Gesetzesverstoßes an Citi, einschließlich aller beobachteten Aktivitäten, die ungewöhnlich oder potenziell ungewöhnlich im Zusammenhang mit der Annahme von Bargeld, finanziellen Aktivitäten oder Transaktionen im Zusammenhang mit Citi oder seinen Kunden erscheinen.

5. Verhinderung und Meldung von Steuerhinterziehung:

- Einhaltung aller geltenden Steuergesetze und -vorschriften in den Ländern, in denen sie tätig sind.
- Unter keinen Umständen sollten Lieferanten sich an einer vorsätzlichen, illegalen Steuerhinterziehung beteiligen oder eine solche Hinterziehung im Namen anderer erleichtern, wozu auch die Beteiligung an Aktivitäten gehören kann, die dazu beitragen würden, die Zahlung fälliger Steuern zu hinterziehen oder Informationen vor den Steuerbehörden zu verbergen.
- Daher müssen die Lieferanten angemessene Verfahren zur Verhinderung von Steuerhinterziehung einführen und Citi unverzüglich schriftlich über Verstöße oder mutmaßliche Verstöße, die Citi betreffen, informieren.

12.2 Interne Richtlinien und Verfahren des Lieferanten:

Lieferanten müssen angemessene interne Richtlinien und Verfahren beibehalten, um alle bestehenden oder später in Kraft tretenden AML-Gesetze und -Vorschriften einzuhalten.

13 UNTERLAGENVERWALTUNG

Gilt für Lieferanten, die auf Citi-Informationen zugreifen/diese verarbeiten/speichern.

Citi verlangt, dass alle Lieferanten, die im Besitz oder in der Verwahrung von Citi-Informationen sind, mit ihrem Business Activity Owner („**BAO**“) oder ihrem primären Citi-Geschäftskontakt zusammenarbeiten, um (i) Informationen für die Zwecke der Unterlagenverwaltung von Citi als „Aufzeichnungen“ oder „vorübergehende Informationen“ zu klassifizieren, (ii) Aufzeichnungen gemäß dem Master Record Catalogue („**MRC**“) von Citi zu klassifizieren, (iii) Informationen entsprechend den Aufbewahrungsanforderungen von Citi aufzubewahren und (iv) vorbehaltlich bestehender Informationssperren am Ende ihres Lebenszyklus ordnungsgemäß zu entsorgen.

Der BAO oder primäre Citi-Geschäftskontakt muss mit dem Lieferanten zusammenarbeiten, um sicherzustellen, dass der Lieferant die Aufzeichnungen gemäß den Citi-Aufzeichnungs-codes im MRC identifiziert und klassifiziert hat und dass das

Inventar mindestens einmal jährlich aktualisiert wird. Der Lieferant ist verpflichtet, die vom BAO mitgeteilten Anforderungen an die Unterlagenverwaltung einzuhalten. Aufzeichnungen, die zur Entsorgung freigegeben sind, müssen so bald wie möglich, spätestens jedoch sechs Monate nach Ablauf der Aufbewahrungsfrist, ordnungsgemäß entsorgt werden, sofern sie nicht einer Informationssperren unterliegen. Transitorische Informationen müssen spätestens zwei Jahre nach ihrer letzten Verwendung vernichtet werden, es sei denn, sie unterliegen einer Informationssperre. Transitorische Informationen, die personenbezogene Daten enthalten, müssen gelöscht werden, sobald der Zweck, zu dem sie erhoben wurden, erfüllt ist, es sei denn, sie unterliegen einer Informationssperre. Der Lieferant muss die Vernichtung oder Veränderung von Citi-Informationen aussetzen, wenn er über eine Informationssperre informiert wird. Im Falle von Unklarheiten hat sich der Lieferant an seinen primären Citi-Geschäftskontakt oder den BAO zu wenden.

Die in den Länderaufbewahrungsplänen aufgeführten Aufbewahrungsregeln werden vierteljährlich von DRIM überprüft und bei Bedarf aktualisiert, um die Einhaltung regulatorischer und interner Änderungen sicherzustellen. Bei Änderungen, die Auswirkungen auf den Lieferanten haben, wird der BAO den Lieferanten informieren. Der Lieferant muss die Auswirkungen bewerten und Änderungen an den jeweiligen Systemen, Prozessen und Inventaren vornehmen. Außerdem muss er innerhalb von 90 Tagen nach Benachrichtigung durch den BAO Änderungen an den Datensatztypen vornehmen, die er besitzt und verwaltet.

Lieferanten, die im Auftrag von Citi Dokumente verwalten, sind dafür verantwortlich, alle Informationen, die als für ein rechtliches oder sonstiges Verfahren relevant eingestuft werden, innerhalb der vom BAO geforderten Frist zu sichern („zu halten“), zu sammeln und herauszugeben. Der Lieferant muss auf Anfrage Citi-Informationen gemäß den geltenden Vertragsbedingungen zurückgeben. Lieferanten dürfen keine Citi-Informationen, unabhängig von ihrer Klassifizierung (z. B. vertraulich, nicht vertraulich), ohne die Genehmigung ihres primären Citi-Geschäftskontakts oder BAO entsorgen, wobei bestätigt werden muss, dass keine aktiven Informationssperren für die zu entsorgenden Informationen bestehen. Die Anforderungen an die Verwaltung und Aufbewahrung von Unterlagen sowie alle anderen Anforderungen an den Umgang mit Informationen bleiben auch nach Beendigung oder Ablauf des Vertrags bestehen, sofern nicht ausdrücklich etwas anderes vereinbart wurde.

Lieferanten müssen eine Dokumentation führen, in der alle Mitarbeiter der Lieferanten aufgeführt sind, die für die Überwachung der Verwaltung von Citi-Informationen in der Obhut der Lieferanten verantwortlich sind, und regelmäßige Treffen mit ihrem primären Citi-Ansprechpartner oder dem Records Management Officer abhalten, um die Namen der Ansprechpartner, Verfahrensdetails, Rollen und Verantwortlichkeiten sowie den Bestand der Lieferantenunterlagen von Citi zu überprüfen und zu aktualisieren.

14 WIDERSTANDSFÄHIGKEIT DES UNTERNEHMENS/KONTINUITÄT DER GESCHÄFTSTÄTIGKEIT

Gilt für Lieferanten, die Dienste bereitstellen oder die von Citi genutzte Technologieinfrastruktur/Anwendungen hosten. Der Citi Business Activity Owner (BAO) ist dafür verantwortlich, dem Lieferanten die Anwendbarkeit und die COB-Anforderungen mitzuteilen.

14.1 Wiederherstellungsressourcen

Der Notfallwiederherstellungsplan des Lieferanten muss alternative Ressourcen vorsehen, mit denen alle Produkte und Dienstleistungen an Citi geliefert werden können, falls die Hauptstandorte des Lieferanten ausfallen. Die Wiederherstellungsressourcen müssen sich an geografisch von den primären Standorten getrennten Orten befinden, die so weit voneinander entfernt sind, dass die Gefahr, dass dasselbe Katastrophenereignis sowohl den primären als auch den Wiederherstellungsstandort betrifft, minimiert oder beseitigt wird.

1. Wiederherstellungsressourcen umfassen nicht nur Informationssysteme, sondern sämtliche für die fortgesetzte Bereitstellung von Produkten und Dienstleistungen für Citi erforderliche Ressourcen, wozu Mitarbeiter, Gebäude, Geschäftsausstattung, Rechenzentren, Daten- und Sprachnetze sowie Verkehrsdienstleistungen gehören können.
2. Anwendungsanbieter können eine Hot/Hot-Architektur implementieren, um eine Hochverfügbarkeitskonfiguration (HA) sicherzustellen. Diese Architektur erfordert mindestens zwei identisch konfigurierte Systeme, die betriebsbereit und für Clients/Benutzer verfügbar sind. Das wichtigste Merkmal dieses Modells ist, dass die alternativen Umgebungen parallel zum primären (Produktions-)Rechenzentrum laufen.

14.2 Dienstleistungsniveau im Wiederherstellungsfall

Die Geschäftskontinuität der Lieferanten muss festgelegte Servicestandards erfüllen, um für Citi effektiv zu sein. Der Notfallwiederherstellungsplan des Lieferanten muss mindestens spezifische Werte festlegen für:

1. Ziel der Wiederherstellungszeit
2. Wiederherstellungspunktziel
3. Wiederherstellungsressourcen/Technologiekapazität
4. Wiederherstellungsdauer

14.3 Notfallwiederherstellungsplan

Der Lieferant unterhält einen Notfallwiederherstellungsplan für die Fortführung des Geschäftsbetriebs (und legt auf Verlangen von Citi einen Nachweis über dessen Aktualität und regelmäßige Tests vor), so dass der Lieferant trotz einer Unterbrechung seiner Fähigkeit, die Produkte/Dienstleistungen zu erbringen oder seine sonstigen Verpflichtungen aus diesem Vertrag von einem bestimmten Standort aus oder durch den Einsatz bestimmter Personen zu erfüllen, unverzüglich in der Lage ist, die Produkte/Dienstleistungen zu erbringen und seine Verpflichtungen von einem anderen

Standort aus oder mit Ersatzpersonal zu erfüllen. Eine Kopie des Notfallwiederherstellungsplans muss Citi innerhalb von zehn (10) Kalendertagen nach dem Datum des Inkrafttretens eines jeden zwischen Citi und dem Lieferanten abgeschlossenen Arbeitsauftrags und danach jährlich vorgelegt werden, solange der Arbeitsauftrag in Kraft ist. Der Lieferant stellt Citi alle Anweisungen oder sonstigen Informationen zur Verfügung, die Citi erforderlich sind, um weiterhin Produkte/Dienstleistungen vom Lieferanten zu erhalten, wenn der Lieferant seinen Notfallplan in Kraft setzt. Der Lieferant sichert zu, dass sein Notfallwiederherstellungsplan mindestens Folgendes umfasst:

1. Wiederherstellungsverfahren und -strategien, einschließlich Umzug, Arbeitsübertragung und/oder Fernzugriff, um die Auswirkungen von Störungen zu mindern, darunter die Nichtverfügbarkeit von Technologie (Denial of Service/DoS), die Nichtverfügbarkeit des primären Arbeitsortes (Denial of Access/DoA) und die Nichtverfügbarkeit von Mitarbeitern (einschließlich Subunternehmern);
2. Unterhaltung eines zweiten, von den Produkt-/Dienstleistungsstandorten getrennten Standorts für die Notfallwiederherstellung durch den Lieferanten (einschließlich, aber nicht beschränkt auf), die Aufbewahrung von Backup-Medien an einem von den Produkt-/Dienstleistungsstandorten getrennten Ort, die Verwendung redundanter Kommunikationsleitungen und Server;
3. Verfahren zur Sicherung/Wiederherstellung des Betriebs und der Anwendung der Produkte/Dienste, einschließlich eines detaillierten, dokumentierten Plans für die Reaktion auf eine längere Unterbrechung der Produkte/Dienste aufgrund eines Stromausfalls, eines Systemfehlers, einer Naturkatastrophe oder anderer unvorhergesehener Umstände, der Prozesse und Verfahren zur Wiederaufnahme des Betriebs innerhalb eines einvernehmlich festgelegten Zeitraums umfasst;
4. Verfahren zum Schutz aller Inhalte;
5. Verfahren und Vereinbarungen mit Dritten für Ersatzgeräte (z. B. Computerausstattung);
6. Verfahren für alle Produktionsanlagen außerhalb des Standorts; und
7. Der Notfallwiederherstellungsplan des Lieferanten, der Folgendes gewährleistet:
 - a. Der Lieferant wird Citi unverzüglich über alle Katastrophen informieren, die sich negativ auf die Produkte/Dienstleistungen auswirken könnten;
 - b. Der Lieferant wird Citi innerhalb von 24 Stunden nach dieser Benachrichtigung einen Plan vorlegen, wie die Produkte/Dienstleistungen weiterhin in einer alternativen Bearbeitungseinrichtung erbracht werden können;
 - c. Die Produkte/Dienstleistungen müssen innerhalb des erforderlichen Wiederherstellungszeitziels (RTO) vollständig betriebsbereit sein, das – sofern im anwendbaren Vertrag nicht anderweitig festgelegt – für Prozesse, die von Citi mit einem

Kritikalitätsgrad „Unternehmenskritisch“ oder „HOCH“ bewertet werden, 4 Stunden oder weniger beträgt, für Prozesse mit einem von Citi bewerteten Kritikalitätsgrad „MITTEL“ 24 Stunden oder weniger und für Prozesse mit einem von Citi bewerteten Kritikalitätsgrad „NIEDRIG“ 72 Stunden oder weniger; und

- d. Wenn Teile der Einrichtungen des Lieferanten nicht betriebsbereit sind, wird der Lieferant Citi nicht schlechter behandeln als seine anderen gewerblichen Kunden.

14.4 Anforderungen an Notfallwiederherstellungspläne für gehostete Dienste

Soweit der Lieferant einen gehosteten Service für Citi verwaltet und bereitstellt, gelten auch die folgenden Bestimmungen. Der Notfallwiederherstellungsplan umfasst mindestens Folgendes:

1. Verfahren zur Sicherung/Wiederherstellung des Betriebs und der Anwendung der gehosteten Dienste, einschließlich eines detaillierten, dokumentierten Plans für die Reaktion auf eine längere Unterbrechung der Dienste aufgrund eines Stromausfalls, eines Systemausfalls, einer Naturkatastrophe oder anderer unvorhergesehener Umstände, der Prozesse und Verfahren für die Wiederaufnahme des Betriebs innerhalb eines einvernehmlich festgelegten Zeitraums enthält;
2. Darüber hinaus sieht der Notfallwiederherstellungsplan des Lieferanten Folgendes vor: (a) Der Lieferant benachrichtigt Citi schriftlich innerhalb von zwei (2) Stunden über jede Katastrophe, die sich negativ auf die gehosteten Dienste auswirken könnte; (b) der Lieferant legt Citi innerhalb von 24 Stunden nach einer solchen Benachrichtigung einen Plan vor, wie die gehosteten Dienste in einer alternativen Verarbeitungseinrichtung weiter erbracht werden können, und (c) die gehosteten Dienste müssen innerhalb von 48 Stunden nach der ersten Benachrichtigung wieder vollständig betriebsbereit sein;
3. Der Lieferant erklärt sich damit einverstanden, auf Anfrage die Informationen freizugeben, die erforderlich sind, damit Citi einen Notfallplan und einen Plan zur Aufrechterhaltung des Geschäftsbetriebs entwickeln kann, der mit dem Notfallwiederherstellungsplan und dem Plan zur Aufrechterhaltung des Geschäftsbetriebs des Lieferanten zusammenarbeitet; und
4. Wenn Teile der Einrichtungen des Lieferanten nicht betriebsbereit sind, wird der Lieferant Citi nicht schlechter behandeln als seine anderen gewerblichen Kunden.

14.5 Änderungen am Notfallwiederherstellungsplan

Der Lieferant kann seinen Notfallwiederherstellungsplan ändern, solange die Änderungen den Notfallwiederherstellungsplan nicht in einer Weise verschlechtern, die sich nachteilig auf die Services auswirkt (z. B. Verlängerung der RTOs). Der Lieferant wird Citi unverzüglich alle Änderungen an seinem Notfallwiederherstellungsplan mitteilen

und auf Anfrage von Citi die Änderungen erläutern, damit Citi die Änderungen vollständig versteht und auf sie reagieren kann.

14.6 Notfallwiederherstellungsplan der Subunternehmer

Der Lieferant stellt sicher, dass jeder Subunternehmer des Lieferanten einen Notfallwiederherstellungsplan sowie Maßnahmen zur Sicherstellung der Geschäftskontinuität unterhält, die vollständig mit den Anforderungen von Citi an Lieferanten übereinstimmen. Der Lieferant muss die Subunternehmer angemessen überwachen, einschließlich der regelmäßigen Überprüfung solcher Kontrollen und Testergebnisse, und die zeitnahe Behebung festgestellter Mängel sicherstellen.

14.7 Anrufung des Notfallwiederherstellungsplans und Krisenbenachrichtigung

Der Lieferant benachrichtigt unverzüglich den primären Geschäftskontakt von Citi:

1. Wenn der Lieferant seinen Notfallwiederherstellungsplan aufruft; und
2. Bei jeder Krise, Bedrohung, Warnung oder jedem Cyber-Ereignis, das sich gegen den Lieferanten oder seine Subunternehmer richtet und bei dem es hinreichend wahrscheinlich ist, dass es sich negativ auf die für Citi erbrachten Dienstleistungen oder Produkte auswirkt.

14.8 Testen

Alle Wiederherstellungsressourcen und -pläne des Lieferanten müssen innerhalb von 120 Tagen nach der Produktionsimplementierung (90 Tage bei Anwendungen, die von Citi als unternehmenskritisch eingestuft wurden) getestet und mindestens einmal jährlich (alle 12 Monate) überprüft werden. Die Tests müssen belegen, dass der Lieferant die Wiederherstellungs-Dienstleistungsniveaus für alle an Citi gelieferten Produkte und erbrachten Dienstleistungen einhalten kann. Diese Tests müssen umfassend sein und den gesamten Umfang der für Citi bereitgestellten Dienste umfassen. Lieferanten müssen Citi mindestens 30 Kalendertage im Voraus darüber informieren, dass sie die Wiederherstellung der für Citi erbrachten Produkte/Dienstleistungen testen. Citi kann an Wiederherstellungstests des Lieferanten für Anwendungen, die von Citi zur Validierung der Geschäftsfunktionalität der Anwendung in der Wiederherstellungsumgebung verwendet werden, teilnehmen oder diese beobachten. Wenn Citi teilnehmen möchte, stellt der Lieferant Citi die Testziele, den Testplan und die Verfahren für die Verbindung zum Teststandort zur Verfügung, bevor er den Test durchführt. Innerhalb von zehn (10) Werktagen nach Abschluss jedes Tests stellt der Lieferant Citi eine Zusammenfassung der Testziele, des Testplans und der Testergebnisse zur Verfügung, einschließlich der für die Wiederherstellung erforderlichen Zeiträume und Nachweise für die Testergebnisse (z. B. Screenshots).

14.9 Volumenvvalidierung

Ein Lieferant, der von Citi als unternehmenskritisch eingestufte Anwendungen hostet, muss nachweisen, dass Produktionsvolumina in seiner COB-/Notfallwiederherstellungsumgebung verarbeitet werden können. Citi und der Lieferant müssen sich auf die Methodik einigen, die für die Validierung verwendet werden soll.

14.10 Nutzung von Citi-Systemen zur Bereitstellung von Diensten

Auf Anfrage von Citi oder den verbundenen Unternehmen von Citi nehmen Lieferanten, die Citi-Systeme verwenden, kostenlos oder gebührenpflichtig an den Notfallwiederherstellungsübungen von Citi teil.

14.11 Umgang mit Testergebnissen

Wenn die Testergebnisse des Lieferanten zeigen, dass die Testziele oder geltende RTO nicht erfüllt wurden, führt der Lieferant eine Ursachenanalyse durch und behebt unverzüglich alle festgestellten Mängel. Nach der Umsetzung dieser Abhilfemaßnahmen führt der Lieferant spätestens einhundertzwanzig (120) Kalendertage (90 Kalendertage bei Anwendungen, die von Citi als unternehmenskritisch eingestuft wurden) nach dem ersten Testfehler (oder innerhalb des in dem entsprechenden Arbeitsauftrag angegebenen Zeitraums) einen erneuten Test durch.

14.12 Krisenmanagement

Im Zusammenhang mit dem Geschäftsfortführungsplan muss der Lieferant einen Krisenmanagementplan für die Steuerung und Koordinierung der Wiederherstellungsmaßnahmen unterhalten. Der Krisenmanagementplan des Lieferanten muss bestimmte Personen benennen, die über die für das Ingangsetzen einer Wiederherstellungsoperation nötige Autorität verfügen, Kommunikations- und Eskalationsprotokolle für die Erhebung und Verteilung von Kriseninformationen definieren sowie Benachrichtigungs- und Eskalationsprotokolle für die Kommunikation mit Citi im Fall einer Krise umfassen.

14.13 Beurteilungen der Geschäftskontinuität

Lieferanten unterliegen dem Bewertungsverfahren von Citi zur Informationssicherheit bei Dritten (Third Party Information Security Assessment Process, TPISA) zur Bewertung der Richtlinien, Verfahren und Kontrollen des Lieferanten im Hinblick auf die Einhaltung der Anforderungen von Citi und aller gesetzlichen und/oder behördlichen Anforderungen (die entweder für Citi oder den Lieferanten gelten), die die Geschäftskontinuität betreffen. Die Bewertung besteht aus Fragebögen, die vom Lieferanten mit entsprechenden Nachweisen beantwortet werden müssen, und kann Besuche an den Standorten des Lieferanten umfassen. Sollten die Ergebnisse einer Bewertung Probleme oder Bedenken aufzeigen, wird Citi die Ergebnisse dokumentieren und gemeinsam mit dem Lieferanten eine Möglichkeit zur Behebung der Probleme finden. Lieferanten müssen unverzüglich die erforderlichen Korrekturen vornehmen und/oder Ausgleichsmaßnahmen ergreifen, um die Bedenken von Citi zur angemessenen Zufriedenheit von Citi auszuräumen.

14.14 Betriebliche Widerstandsfähigkeit

Kritische Geschäftsdienste sind Dienste, deren Unterbrechung erhebliche negative Auswirkungen auf Citi, seine Kunden oder das Finanzsystem haben könnte. Der Lieferant stellt sicher, dass eine Unterbrechung der Erbringung von Elementen der Dienstleistungen, die entweder kritische Geschäftsdienstleistungen darstellen oder die Erbringung wichtiger/kritischer Geschäftsdienstleistungen durch Citi unterstützen, wie von Citi von Zeit zu Zeit festgelegt („kritische Geschäftsdienstleistungen“), nicht die von Citi festgelegte Dauer überschreitet oder anderweitig gegen eine von Citi festgelegte relevante Metrik („Ausfalltoleranzen“) verstößt, die dem Lieferanten von Zeit zu Zeit mitgeteilt wird. Ausfalltoleranzen werden als klare, zeitgebundene Kennzahlen ausgedrückt, die der Dauer entsprechen, für die die Leistungserbringung unterbrochen

werden darf. Citi und der Lieferant überprüfen die Ausfalltoleranzen jährlich im Rahmen des laufenden Vertragsverwaltungsprozesses. Wenn Citi aufgrund der Anforderungen mehrerer Aufsichtsbehörden für einen einzelnen kritischen Geschäftsdienst mehr als eine Ausfalltoleranz festlegen muss, kann Citi für diesen kritischen Geschäftsdienst separate Ausfalltoleranzen festlegen. Der Lieferant ist verpflichtet:

1. Citi unverzüglich zu benachrichtigen, sobald bekannt wird, dass sie eine Dienstleistung nicht innerhalb der von Citi festgelegten Ausfalltoleranz(en) erbringen kann (oder dass dies mit hinreichender Wahrscheinlichkeit zu erwarten ist), zusammen mit einer Erläuterung der Gründe für den voraussichtlichen oder tatsächlichen Ausfall und den Maßnahmen, die zur Minderung der Auswirkungen dieses Ausfalls ergriffen werden;
2. Auf Anfrage Citi in angemessener Weise dabei zu unterstützen, die Personen, Prozesse, Technologien, Einrichtungen und Informationen zu identifizieren, die für die Erbringung der Dienstleistungen zur Unterstützung kritischer Geschäftsprozesse durch den Lieferanten erforderlich sind;
3. Citi angemessene Unterstützung zu gewähren, damit Citi Folgendes durchführen kann:
 - a. interne Szenariotests über die Fähigkeit des Lieferanten, im Falle einer schwerwiegenden, aber plausiblen Unterbrechung seines oder des Betriebs des Lieferanten innerhalb der Ausfalltoleranz(en) für jeden kritischen Geschäftsdienst zu verbleiben, durchzuführen; und
 - b. alle Erfahrungen, die nach einem Szenario-Test gemacht wurden, um Citi in die Lage zu versetzen, Schwachstellen und notwendige Maßnahmen zu identifizieren, um die Fähigkeit des Lieferanten zu verbessern, effektiv auf künftige Unterbrechungen zu reagieren und seine Systeme wiederherzustellen.

Wenn interne Szenariotests von Citi Schwachstellen oder Einschränkungen hinsichtlich der Fähigkeit des Lieferanten zur Erbringung von Dienstleistungen innerhalb der von Citi festgelegten Ausfalltoleranz(en) aufdecken und wenn der Lieferant eine Dienstleistung nicht innerhalb der von Citi festgelegten Ausfalltoleranz(en) erbringt, vereinbaren die Parteien einen Plan (einschließlich eines Zeitplans für die Umsetzung des Plans), um sicherzustellen, dass der Lieferant die erforderlichen Maßnahmen ergreift, um diese Schwachstellen oder Einschränkungen zu beheben oder zu mindern oder die Ursache für die Nichteinhaltung der Ausfalltoleranz(en) (sofern zutreffend) so schnell wie möglich zu beseitigen.

14.15 Treuhandvereinbarung

Auf Wunsch von Citi müssen Lieferanten, die (i) Software für den Betrieb innerhalb der Citi-Umgebung an Citi lizenzieren oder (ii) Citi einen gehosteten Dienst bereitstellen, sicherstellen, dass Hinterlegungsmaterialien bei dem von Citi benannten Treuhänder hinterlegt werden, und einen Hinterlegerregistrierungsplan oder andere vom Treuhänder geforderte Formulare in Bezug auf die Hinterlegungsmaterialien gemäß der geltenden

Treuhandvereinbarung ausfüllen. Danach wird der Lieferant während der gesamten Restlaufzeit der geltenden Vereinbarung über die Lizenz oder den gehosteten Dienst aktualisierte Versionen der hinterlegten Materialien beim Treuhänder hinterlegen, um sicherzustellen, dass der hinterlegte Quellcode und andere hinterlegte Materialien auf dem neuesten Stand der Software sind, die für die von Citi verwendete Version der Software oder der gehosteten Dienste gilt. Aktualisierungen des Quellcodes oder anderer hinterlegter Materialien sind innerhalb von dreißig (30) Tagen nach dem Datum der Aktualisierung(en) der an Citi lizenzierten Software oder der Änderungen an den von Citi genutzten gehosteten Diensten an den Treuhänder zu übermitteln. Der Lieferant wird alle Verpflichtungen und Anforderungen eines Hinterlegers gemäß der Treuhandvereinbarung vollständig erfüllen. Der Lieferant ist allein verantwortlich für alle Treuhandkosten und -gebühren, einschließlich, aber nicht beschränkt auf Einrichtungsgebühren, Jahresgebühren, Einzahlungsgebühren, Servicegebühren und alle anderen Treuhandgebühren und -kosten. Im Falle eines Freigabeereignisses gibt der Treuhänder die Hinterlegungsunterlagen gemäß den Bedingungen der zugrunde liegenden Vereinbarung und der Treuhandvereinbarung an Citi oder einen von Citi benannten Empfänger frei.

Wenn der Quellcode (oder andere hinterlegte Materialien) an Citi oder einen von Citi benannten Empfänger geliefert wird (entweder direkt durch den Lieferanten oder durch den Treuhänder in Erfüllung seiner Verpflichtungen aus einer geltenden Treuhandvereinbarung), unterliegen der Quellcode und die hinterlegten Materialien der bestehenden Lizenz gemäß der entsprechenden Vereinbarung zwischen dem Lieferanten und Citi; vorausgesetzt, dass jede Lizenz Citi berechtigt, den Quellcode und andere hinterlegte Materialien in angemessenem Umfang zu nutzen und zu ändern, um: (i) die Software und andere hinterlegte Materialien in die Systeme von Citi zu integrieren und deren Kompatibilität sicherzustellen, (ii) dafür zu sorgen, dass die Software oder andere hinterlegte Materialien den geltenden Gesetzen, Industriestandards oder Marktgepflogenheiten entsprechen, (iii) dafür zu sorgen, dass die Software oder andere hinterlegte Materialien mit technologischen Innovationen Schritt halten, und (iv) dafür zu sorgen, dass die Software und andere hinterlegte Materialien den Geschäftszwecken von Citi und ihren verbundenen Unternehmen im Rahmen der bestehenden Lizenz entsprechen. Alle Versionen der Software, die eine von oder im Auftrag von Citi unter Verwendung des Quellcodes entwickelte Änderung enthalten, unterliegen allen Bestimmungen dieses Abschnitts und der zugrunde liegenden Vereinbarung, vorausgesetzt jedoch, dass der Lieferant keine Rechte, Titel oder Ansprüche an den Änderungen hat und alle geistigen Eigentumsrechte an den Änderungen ausschließlich Citi zustehen.

Der Lieferant wird sich in angemessener Weise gegenüber Dritten, die in der Software verwendete Software bereitgestellt haben, bemühen, dass der Lieferant den Quellcode dieser Software von Dritten in die Quellcode-Hinterlegung aufnehmen kann. Für den Fall, dass der Dritte dem Lieferanten dieses Recht verweigert, unternimmt der Lieferant wirtschaftlich angemessene Anstrengungen, um die Übertragung der entsprechenden Softwarelizenzvereinbarung des Dritten auf Citi bei Eintritt eines Freigabeereignisses zu erreichen.

Der gemäß diesem Abschnitt an Citi gelieferte Quellcode unterliegt der bestehenden Lizenz für die entsprechende lizenzierte Software oder die gehosteten Dienste, vorausgesetzt, dass Citi den Quellcode und die Software im Zusammenhang mit ihren

geschäftlichen und betrieblichen Anforderungen nutzen und ändern darf, um die Software auf dem neuesten Stand der technischen Innovationen zu halten und die geltenden Gesetze einzuhalten. Alle Versionen der Software, die eine von oder im Auftrag von Citi unter Verwendung des Quellcodes entwickelte Änderung enthalten, unterliegen allen Bestimmungen der geltenden Vereinbarung, vorausgesetzt jedoch, dass der Lieferant keine Rechte, Titel oder Ansprüche an den Änderungen hat und alle geistigen Eigentumsrechte an den Änderungen ausschließlich Citi zustehen.

15 GLOBALE STANDARDS FÜR HINTERGRUNDÜBERPRÜFUNGEN

Anwendbar auf alle Lieferanten, die als Drittanbieter Dienstleistungen für Citi erbringen.

15.1 Überblick – Hintergrundüberprüfungen

Die Hintergrundüberprüfung muss in Übereinstimmung mit allen geltenden örtlichen Gesetzen und Vorschriften durchgeführt werden. Alle in diesem Dokument beschriebenen Informationen und Selbstoffenlegungen müssen, soweit zutreffend, von den Vertretern des Lieferanten, dem Personal des Lieferanten und den Subunternehmern bereitgestellt werden. Falschdarstellungen oder Auslassungen ob in einem Lebenslauf, während eines Vorstellungsgesprächs, auf einem Einstellungsfragebogen oder während des Einstellungsverfahrens können unabhängig vom Zeitpunkt ihrer Entdeckung Grund für eine Ablehnung oder die Beendigung der Beschäftigung durch Citi entsprechend den örtlichen Gesetzen sein. Unerwünschte Ergebnisse bei einer durchgeführten Überprüfung können gleichfalls unabhängig vom Zeitpunkt ihrer Entdeckung Grund für eine Ablehnung oder die Beendigung der Beschäftigung durch Citi entsprechend örtlichen Gesetzen sein.

Weitere Informationen zum Abschluss der Hintergrundüberprüfung finden Sie unter https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

15.2 Erfassung grundlegender Informationen und Identitätsüberprüfung

Bevor Mitarbeiter eines Lieferanten einen Auftrag für Citi ausführen, müssen Lieferanten den Vor- und Nachnamen, die Postanschrift und die ständige Anschrift (falls abweichend), die Telefonnummer und die E-Mail-Adresse (falls zutreffend) der betreffenden Personen erfassen. Das Personal des Lieferanten muss zudem Dokumente vorlegen, die seine Identität verifizieren. Dies kann die Bereitstellung von Informationen und/oder Dokumenten einer nationalen ID-Nummer, eines von der Regierung ausgestellten Personalausweises mit Bild oder eines Reisepasses umfassen.

15.3 Sanktionsprüfung

Das gesamte Personal des Lieferanten, das im Auftrag von Citi tätig ist, sowie Eigentümer mit einer Beteiligung von mindestens 25 % an einem Citi-Lieferanten, einschließlich Subauftragnehmern, müssen unabhängig davon, ob sie Zugang zu Citi-Daten, -Systemen und -Netzwerken UND/ODER Zugang zu Citi-Räumlichkeiten haben,

Citi-Anforderungen an Lieferanten

gegen die vom Office of Foreign Assets Control („OFAC“) des US-Finanzministeriums geführte Liste der Specially Designated Nationals and Blocked Persons („SDN-Liste“), gegen die Liste der Regionen und Rechtsgebiete, die US-Sanktionen unterliegen, sowie gegen von Behörden außerhalb der Vereinigten Staaten herausgegebene Sanktionslisten geprüft werden, einschließlich der konsolidierten Finanzsanktionsliste der Europäischen Union („EU“), der konsolidierten Liste des Sicherheitsrats der Vereinten Nationen („UN“), der Sanktionsliste des Vereinigten Königreichs („UK“) sowie der Listen gemäß den im jeweiligen Rechtsgebiet geltenden Gesetzen und Vorschriften („Nicht-US-Sanktionen“).

OFAC-Listen sind auf dieser Website öffentlich zugänglich:
<https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Einhaltung der Einwanderungsbestimmungen

Der Lieferant muss nachweisen, dass er Protokolle unterhält und implementiert, um zu überprüfen, ob alle Mitarbeiter zur Arbeit in den Einsatzländern berechtigt sind. Darüber hinaus muss der Lieferant: (1) sicherstellen, dass das gesamte Personal zur Arbeit berechtigt ist; und (2) die Einhaltung aller geltenden Gesetze, Vorschriften und Richtlinien (einschließlich der Anforderungen an die Arbeitsberechtigung und Überprüfung) gewährleisten. Der Lieferant muss ferner nachweisen und sicherstellen, dass er Verfahren unterhält, um zu gewährleisten, dass sein Personal alle geltenden Einwanderungsgesetze und -vorschriften einhält und dass sein Personal über den für die jeweiligen Einsätze und Tätigkeiten erforderlichen Visastatus bzw. die erforderliche Visakategorie verfügt.

15.5 Beschäftigungshistorie

Lieferanten müssen die Beschäftigungshistorie ihrer Mitarbeiter für die letzten sieben (7) Jahre oder, falls gemäß den lokalen Vorschriften erforderlich, für die letzten zehn (10) Jahre überprüfen. Die Angaben einer Person zu ihrer beruflichen Laufbahn sind daraufhin zu überprüfen, ob die Arbeitgeber, Positionen, Daten und Aufgaben zutreffend wiedergegeben wurden. Mitarbeiter eines Lieferanten müssen darüber hinaus eine Beschäftigung oder eine Beauftragung als Berater oder befristeter Mitarbeiter bei Citi oder einem seiner Rechtsvorgänger angeben (einschließlich, aber nicht beschränkt auf: Citibank, Citicorp, Travelers, Salomon Brothers und/oder Smith Barney).

15.6 Bildungsverlauf

Lieferanten müssen den höchsten Bildungsabschluss ihres Personals nachweisen. Zu den zu erhebenden Angaben zählen die Datumsangaben, Name(n) der Einrichtung(en), Anschrift(en) und erworbene Abschlüsse.

15.7 Krimineller Hintergrund

Soweit rechtlich zulässig, müssen die Mitarbeiter der Lieferanten und Subunternehmer Citi offenlegen, wenn sie verhaftet, vorgeladen, angeklagt oder wegen einer Straftat verurteilt werden, einschließlich eines Schuldbekenntnisses oder eines Bekenntnisses zu unbestrittenen Tatsachen und jeder Teilnahme an einem Programm zur Abwendung des Strafverfahrens oder einem ähnlichen Programm. Die administrative Überprüfung

von Strafregistern und/oder Fingerabdruckkontrollen müssen, soweit rechtlich zulässig und verfügbar, vor Beginn des Einsatzes abgeschlossen sein. Strafrechtliche Verurteilungen wegen Straftaten im Zusammenhang mit Diebstahl, Betrug, Unehhrlichkeit oder Vertrauensbruch oder ähnlichen Straftaten, die nach lokalem Recht anders definiert sind, können, sofern nicht gesetzlich anders vorgeschrieben, zur Ablehnung einer Einstellung bei Citi und/oder zur Unzulässigkeit für eine Einstellung bei Citi führen. Andere Verurteilungen können gemäß den geltenden örtlichen Gesetzen und Vorschriften zur Ablehnung und/oder Nichtberechtigung des Einsatzes führen.

15.8 Erneute Überprüfung

Mitarbeiter des Lieferanten, deren Auftrag beendet wird, müssen erneut überprüft werden, wenn sie erneut bei Citi zum Einsatz kommen. Weitere Informationen zu den Anforderungen für erneute Überprüfungen finden Sie unter https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Internationale Versetzungen

Alle Überprüfungen müssen gemäß den Bestimmungen des Landes durchgeführt werden, in dem der Einsatzort liegt. Wenn Mitarbeiter des Lieferanten in ein neues Land versetzt werden, müssen sie gemäß den Anforderungen des neuen Landes erneut überprüft werden.

16 KOSTEN

Lieferanten, die vertraglich berechtigt sind, erstattungsfähige Geschäftsausgaben geltend zu machen.

16.1 Übersicht

Citi erstattet nur angemessene geschäftliche Ausgaben, die zuvor schriftlich von Citi genehmigt wurden und dem Lieferanten im Zusammenhang mit der Bereitstellung von Produkten und Dienstleistungen für Citi entstanden sind, den Bestimmungen des geltenden Vertrags oder der Richtlinie zur Verwaltung der Betriebsausgaben von Citi und gegebenenfalls den entsprechenden Standards und Verfahren entsprechen und durch Belege, Rechnungen, Reisepläne oder andere von Citi als akzeptabel erachtete Unterlagen ausreichend belegt sind.

16.2 Rückerstattungen

Diese Ausgaben müssen ordnungsgemäß dokumentiert und Citi in Übereinstimmung mit den Citi-Rechnungsstellungsanforderungen in Rechnung gestellt werden. Ausgaben des Lieferanten dürfen nicht von einem Citi-Mitarbeiter im Namen des Lieferanten getätigt werden. Jede Ausgabe, die bei Citi zur Rückerstattung von (einer) gültigen und

genehmigten Ausgabeposition(en) eingereicht wird, muss (zusätzlich zu allen anderen Anforderungen an die Rechnungsstellung) Folgendes enthalten:

1. Den geschäftlichen Zweck der Auslage;
2. Den Betrag und die Beschreibung der Auslage;
3. Ort und Datum der Auslage;
4. Name/Beschreibung des Projekts, für das der Lieferant Dienstleistungen erbringt;
5. Die Namen und Geschäftsbeziehung des Citi-Vertreters, der die Dienstleistungen angefordert hat, für die die Auslagen angefallen sind; und
6. Die Bestellnummer, wo zutreffend.

Näheres zu genehmigten, erstattbaren geschäftlichen Auslagen erfahren Sie bei Ihrem geschäftlichen Hauptkontakt bei Citi. Belege, Rechnungen, Reiserouten oder andere Formen der Dokumentation, die von Citi als akzeptabel erachtet werden, müssen zusammen mit dem Erstattungsantrag eingereicht werden. Erstattungsanträge müssen den Bestimmungen des geltenden Vertrags oder gegebenenfalls der Richtlinie zur Verwaltung von Betriebsausgaben von Citi und den entsprechenden Standards und Verfahren entsprechen und vom zuständigen Geschäftspartner und/oder dem primären Ansprechpartner bei Citi genehmigt sowie von einer ordnungsgemäß bevollmächtigten Person mit ausreichender Verfügbarkeit für die entsprechende Ware genehmigt werden. Nicht ordnungsmäßige Anträge werden nicht erstattet.

17 INFORMATIONSSICHERHEIT (IS)

Gilt für Lieferanten, einschließlich Subunternehmer, die auf Citi-Informationen gemäß der Klassifizierung und Definition im Anhang zugreifen, diese verarbeiten, speichern oder verwalten, oder internetbasierte Anwendungen mit der Marke Citi hosten, oder über eine Verbindung zu den Netzwerkressourcen von Citi verfügen, oder unbegleiteten Zugang zu den Einrichtungen von Citi benötigen.

17.1 Überblick

Dieser Abschnitt enthält Mindestanforderungen für Lieferanten von Citi, einschließlich Unterauftragnehmern oder Subunternehmern, die Citi-Informationen speichern, verarbeiten, verwalten oder darauf zugreifen oder Citi-Anwendungen hosten oder über eine Netzwerkverbindung zu Citi verfügen, hinsichtlich der von Citi erwarteten Kontrollen zum Schutz von Informationen. Diese Anforderungen stellen sicher, dass Informationen an den Standorten, an denen Citi und seine Lieferanten geschäftlich tätig sind, gemäß den geltenden gesetzlichen und behördlichen Anforderungen und den höchsten Industriestandards (z. B. ISO/IEC 27001/2) geschützt werden. Wenn lokale Gesetze, Vorschriften oder relevante Industriestandards höhere Standards festlegen als hier angegeben, müssen die Lieferanten diese Gesetze, Vorschriften oder Standards einhalten. Außerdem können Lieferanten im Rahmen ihrer Einhaltung anderer Citi-Richtlinien und Vertragsbedingungen verpflichtet sein, zusätzliche Informationssicherheitspraktiken und -verfahren anzuwenden. Entscheidet sich ein Lieferant dafür, zusätzliche Sicherheitspraktiken oder Verfahren zur Informationssicherheit anzuwenden, hat der Lieferant dafür zu sorgen, dass diese

Praktiken und Verfahren nicht im Widerspruch zu den Mindestkontrollen stehen, die in diesem Abschnitt definiert sind.

17.2 Richtlinie und Umsetzung der Informationssicherheit

Lieferanten müssen über dokumentierte Richtlinien und Standards zur Informationssicherheit verfügen. Die Richtlinienverwaltung muss klar definierte Rollen und Verantwortlichkeiten sowie eine jährliche Überprüfung/Aktualisierung der Richtlinien und Standards umfassen, um sicherzustellen, dass sie dem aktuellen Stand der Technik, den Branchenstandards sowie den gesetzlichen und behördlichen Anforderungen entsprechen.

17.3 Aufgabentrennung

Lieferanten müssen Abläufe eingeführt haben, die sicherstellen, dass keine Einzelperson zwei Geschäftsfunktionen oder zwei IT-Funktionen gleichzeitig innehat. Gleiches gilt für zwei Funktionen im kontrollierten Informationssystem mit ständigem Zugang zur gleichen Tätigkeit, Änderung, zum Informationssystem oder zu Transaktionen ohne Autorisierung oder Nachweis, außer ausreichende Ausgleichskontrollen zur Minderung des Risikos sind eingesetzt.

Tabelle A

Funktionen	Beschreibung der Funktion
Entwicklung/Engineering	Entwurf, Entwicklung oder Veränderung von Software, Hardware und Konfigurationen, zum Beispiel: – Entwurf und Entwicklung neuer Anwendungscodes sowie zugehörigen Datenbankschemata – Engineering-Infrastrukturprodukte und Anwendungskomponenten – Anpassung von Technologieprodukten zur Integration in Software und Dienstleistungen
Genehmigung	Genehmigung der umzusetzenden Codeänderungen
Implementierung/Verwaltung von Systemen	Installation, Implementierung oder Verwaltung von Software, Hardware und Änderungen an Konfigurationen. Zum Beispiel: – Durchführung einer automatisierten oder manuellen Codefreigabe in die Produktionsinfrastruktur – Installation eines Technologieprodukts oder -geräts – Starten oder Stoppen von Dienstleistungen zur Unterstützung der Fehlerbehebung und Behebung von

	Problemen bei Systemen mit Produktionsdaten
Überprüfung der Aktivitäten privilegierter IDs	Überprüfung von Aktivitäten des Änderungsmanagements oder sicherheitsbezogener Systemereignisse (z. B. Prüfprotokollen)
Verwaltung von IDs	Hinzufügen, Ändern und Löschen von IDs (Benutzer, FIDs und Bots), Berechtigungen oder Passwörtern
Geschäftsfunktion	Beschreibung der Funktion
Initiierung einer Geschäftstransaktion	Initiieren von Geschäftstransaktionen (auch als Erfassen, Anlegen oder Erstellen bezeichnet) sowie Ändern von Kundeninformationen
Genehmigung von Geschäftstransaktionen	Genehmigen von Geschäftstransaktionen (auch als Autorisieren, Prüfen oder Freigeben bezeichnet)
IT-Funktion	Beschreibung der Funktion
Netzwerkbetrieb	Gerätemanagement und operative Unterstützung von Produkten, die Dienstleistungen der Netzinfrastruktur bereitstellen. Netzwerkrouter, Switches, Firewalls, Domain Name Services (DNS) usw.
Nicht-Netzwerkbetrieb	Gerätemanagement und operative Unterstützung von Produkten, die keine Dienstleistungen der Netzinfrastruktur bereitstellen. Server, Telefone, Computer usw.

17.4 Verpflichtung der Geschäftsführung zu Informationssicherheit

Lieferanten, die eine internetbasierte Anwendung der Marke Citi hosten und/oder Zugang zu Citi-Informationen mit der Einstufung „vertraulich“ oder höher haben, unterliegen dem Prozess zur Bewertung der Informationssicherheit von Dritten (Third-Party Information Security Assessment Process, TPISA) von Citi, bei dem die Richtlinien, Verfahren und Kontrollen des Lieferanten hinsichtlich der Einhaltung der Anforderungen von Citi und aller gesetzlichen und/oder regulatorischen Anforderungen (die entweder für Citi oder den Lieferanten gelten) in Bezug auf die Informationssicherheit bewertet werden.

Die Bewertung besteht aus Sicherheitsfragebögen, die vom Lieferanten mit entsprechenden Nachweisen zu beantworten sind, und kann Besuche an Standorten des Lieferanten umfassen, an denen vertrauliche Informationen von Citi oder höher eingestufte Informationen gespeichert, verarbeitet, verwaltet oder von Dritten abgerufen werden. Darüber hinaus kann das TPISA-Team für die kontinuierliche Überwachung durch Dritte den Lieferanten mithilfe von Cybersicherheits-Überwachungstools überwachen, die öffentlich zugängliche Informationen nutzen, um anfällige, mit dem Internet verbundene Systeme, Hosts, Anwendungen und Server zu identifizieren, beispielsweise Software, deren Lebensdauer abgelaufen ist, ausgenutzte offene Ports, Schwachstellen oder andere Sicherheitsrisiken. Sollten die Ergebnisse einer TPISA Sicherheitsmängel aufdecken oder darauf hinweisen, wird Citi die Ergebnisse in einer Mitteilung an den Lieferanten dokumentieren und gemeinsam mit dem Lieferanten Maßnahmen zur Behebung dieser Mängel erarbeiten. Lieferanten müssen unverzüglich die erforderlichen Korrekturen und/oder Ausgleichsmaßnahmen vornehmen, um die Bedenken von Citi nach alleinigem Ermessen von Citi auszuräumen und die erforderlichen Fristen von 180 Kalendertagen für Probleme mit hohem Risiko, 240 Kalendertagen für Probleme mit mittlerem Risiko und vor dem nächsten Compliance-Termin für Probleme mit geringem Risiko einzuhalten, da diese Probleme von Citi einer Risikobewertung unterzogen werden.

1. Der Lieferant muss seine Geschäftsabläufe und die damit verbundenen Kontrollen regelmäßig anhand seiner eigenen Informationssicherheitsstandards, Richtlinien und Verfahren bewerten. Zu diesen periodischen Überprüfungen gehört mindestens das Folgende:
 - a) Bewertung der Verfahren, die der Lieferant einsetzt, um die Einhaltung der eigenen IS-Richtlinien und -Standards zu gewährleisten;
 - b) Bewertung der unterstützenden Ressourcen, wie z. B. der vom Lieferanten genutzten Anwendungen und Infrastruktur und der von den Subunternehmern des Lieferanten genutzten IS-Prozesse (falls zutreffend), die deren Geschäftsbetrieb unterstützen oder Citi die Durchführung solcher Bewertungen ermöglichen. Die Einhaltung der Vorschriften ist erforderlich, wenn ein Dritter einen neuen Vertrag mit einem Subunternehmer unterzeichnet oder einen bestehenden Vertrag mit einem Subunternehmer erneuert, der auf Citi-Informationen, die von Citi als vertraulich oder höher eingestuft werden, zugreift, sie verarbeitet, verwaltet oder entsorgt.
2. Probleme, die als Ergebnis einer Informationssicherheits-Risikobewertung (z. B. TPISA) identifiziert wurden, müssen dokumentiert und bis zum Abschluss verfolgt werden, wobei Citi ein Nachweis über die Behebung der Probleme vorzulegen ist.
3. Wenn das Informationssicherheitsmanagement des Lieferanten über Ländergrenzen hinweg verlagert wird, muss der Lieferant vor einer solchen Verlagerung die dokumentierte Genehmigung von Citi einholen.
4. Wenn der Lieferant einen neuen Betrieb erwirbt, muss er eine Bewertung des erworbenen Betriebs hinsichtlich der Einhaltung dieser Standards durchführen.
5. Der Lieferant darf keine Sicherheitsmanagementfunktionen auslagern, einschließlich, aber nicht beschränkt auf Firewall-Management, Sicherheitskonfigurationsmanagement, Patch-Management oder Funktionen der Informationssicherheitsverwaltung (ISA) für Systeme, die zur Speicherung,

Verarbeitung und/oder Übertragung von Citi-Informationen verwendet werden, es sei denn, Citi hat dies im Voraus schriftlich genehmigt.

6. Wenn der Lieferant Software oder eine Website hostet, die Citi-Informationen enthält oder die Marke Citi trägt, müssen regelmäßige Schwachstellenbewertungen gemäß Citis Standard für System-Sicherheitstests (SSTS) durchgeführt werden, und alle wesentlichen Probleme, die während der Bewertung identifiziert werden, müssen innerhalb des in diesem Standard festgelegten Zeitrahmens behoben werden. Da das SSTS nicht für die externe Verbreitung zugelassen ist, müssen Lieferanten mit ihrem Citi Relationship Manager zusammenarbeiten, um die Einhaltung der Referenzdokumentation sicherzustellen. Darüber hinaus muss der Lieferant die einschlägigen Informationssicherheits-Managementnormen ISO/IEC 27001 (oder Nachfolgenormen für Informationssicherheits-Management, die strengere Standards und Protokolle festlegen) einhalten und die in diesem Abschnitt (17) enthaltenen Bestimmungen zur Informationssicherheit befolgen.
7. Wenn eine Verbindung zu Servern und/oder Informationssystemen im internen Netzwerk von Citi erforderlich ist, muss der Lieferant seinen Hauptansprechpartner bei Citi benachrichtigen, damit das aktuelle Verfahren zur Bereitstellung der Verbindung befolgt werden kann.
8. Der Lieferant muss die zuständige Citi-Kontaktperson (Business Activity Owner, BAO) unverzüglich über jeden unbefugten Zugriff, Erwerb, Verlust, Beschädigung oder Löschung von Citi-Informationen oder jede andere Beeinträchtigung von Informationssystemen, die zur Speicherung, Verarbeitung oder Übertragung von Citi-Informationen verwendet werden, informieren.
9. Der Lieferant muss sicherstellen, dass alle risikobehafteten Aktivitäten oder Änderungen an sensiblen Daten über Prüfpfade verfügen, die eine Zuordnung dieser Handlungen zu den Personen ermöglichen, die sie durchgeführt haben.
10. Der Lieferant muss sicherstellen, dass vertrauliche oder höherwertige Daten auf dem Bildschirm und auf Papier unkenntlich gemacht werden, darunter beispielsweise Überwachungs-, Ausnahme-, Regulierungs- und andere Berichte.
11. Der Lieferant muss das Drucken, Aufzeichnen oder Kopieren von sensiblen Daten, auch mit seinen eigenen Geräten, einschränken. Der Lieferant muss alle Informationen von Citi zu einem vereinbarten Zeitpunkt während oder am Ende der Vereinbarung zurückgeben oder vernichten, sofern dies nicht durch gesetzliche oder behördliche Vorschriften untersagt ist.
12. Der Lieferant muss sicherstellen, dass sämtliches Personal des Lieferanten (Mitarbeiter, Auftragnehmer, Zeitarbeiter, Subunternehmer) mit Zugang zu Citi-Informationen eine Geheimhaltungs- oder Vertraulichkeitsvereinbarung unterzeichnen.
13. Den Mitarbeitern des Lieferanten muss ein Mitarbeiterhandbuch oder ein ähnliches Dokument zur Verfügung gestellt werden, das Disziplinarmaßnahmen bei Verstößen gegen den Verhaltenskodex und die Personalrichtlinien des Lieferanten enthält, die im Rahmen des Onboarding-Prozesses zur Kenntnis genommen werden müssen.
14. Der Lieferant hat einen Prozess eingerichtet, um alle Vermögenswerte abzurufen, wenn ein Mitarbeiter oder Nichtmitarbeiter gekündigt wird oder zurücktritt.
15. Wenn vertrauliche Informationen aufbewahrt oder in irgendeiner Weise auf einer Website oder einem über das Internet zugänglichen System gespeichert werden, muss der Lieferant diese Informationen Citi offenlegen. Diese Offenlegung kann

in der Beschreibung der Dienste enthalten sein. Wenn der Lieferant vertrauliche Informationen von Citi verwaltet oder speichert, wird er während der Laufzeit dieser Vereinbarung einmal jährlich ein SSAE 18-Audit (oder eine nachfolgende, von Citi genehmigte maßgebliche Bewertung) durchführen lassen und Citi mindestens einmal jährlich eine Kopie der Berichte vorlegen, die die Ergebnisse eines solchen SSAE 18-Audits oder einer nachfolgenden, von Citi genehmigten maßgeblichen Bewertung dokumentieren.

16. Wenn der Lieferant im Rahmen einer Fusion, Übernahme oder ähnlichen Transaktion von einem anderen Unternehmen übernommen wird oder ein anderes Unternehmen übernimmt und diese Transaktion Auswirkungen auf die Dienstleistungen haben könnte, muss der Lieferant Citi unverzüglich schriftlich darüber informieren und eine Bewertung der Informationssicherheit des daraus hervorgehenden Unternehmens gemäß diesen Anforderungen durchführen, um sicherzustellen, dass die Übernahme oder Fusion die Einhaltung dieser Anforderungen nicht beeinträchtigt.

17.5 Informationssicherheitsrisiko für Subunternehmer

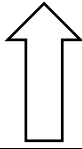
Der Lieferant muss verlangen, dass Subunternehmer, die Zugang zu vertraulichen Daten von Citi oder höher eingestuft Daten haben, vor Vertragsabschluss und regelmäßig nach Vertragsabschluss einer Bewertung der Informationssicherheit (IS) durch qualifiziertes Personal für Informationssicherheit unterzogen werden. Diese Bewertungen sollten gemäß einem vom Management genehmigten Prozess durchgeführt werden, der alle Phasen des Bewertungsprozesses von der Einleitung bis zum Problemmanagement abdeckt. Die IS-Bewertung des Subunternehmers sollte einen Fragebogen oder ein gleichwertiges Instrument nutzen, mit dem die Haltung des Subunternehmers in IS-Bereichen bewertet wird, die mit denen im Fragebogen zur IS-Bewertung von Dritten (TPAQ) von Citi übereinstimmen, und sollte eine logische Methode zur Berechnung des mit der Beauftragung des Subunternehmers verbundenen IS-Risikos enthalten. Der Lieferant muss den Abschluss der Bewertung verfolgen und festgestellte Probleme sowie Korrekturmaßnahmen bis zum Abschluss verwalten.

17.6 Verantwortung für Informationswerte

1. Der Lieferant muss sicherstellen, dass eine Inventarliste aller Anwendungen und Hardware unter seiner Kontrolle geführt wird, die zur Speicherung, Verarbeitung und/oder Übertragung von Citi-Informationen verwendet werden.
2. Der Lieferant hat ein Verzeichnis der Citi-Informationswerte gemäß einem Prozess unter seiner Kontrolle zu führen, der dazu verwendet wird, die Genauigkeit und Vollständigkeit dieses Inventars angemessen aufrechtzuerhalten.
3. Der Lieferant hat die Verantwortung für den Schutz sämtlicher Citi-Informationen unter seiner Kontrolle.
4. Der Lieferant hat dafür zu sorgen, dass die Aktivität seiner Benutzer in einer Weise verfolgt werden kann, die der Branchenpraxis entspricht.
5. Der Benutzerzugriff auf persönliche externe Internet-E-Mail-Speicher und Cloud-Speicherkonten muss vom globalen Netzwerk des Lieferanten, in dem Citi-Informationen gespeichert sind, eingeschränkt werden.

17.7 Klassifizierung und Umgang mit Informationen.

Citi klassifiziert Informationen gemäß der nachstehenden Tabelle zur Informationsklassifizierung. Im Anhang finden Sie Definitionen und Beispiele für jede der unten aufgeführten Informationsklassifikationen.

EINGESCHRÄNKT	Am sensibelsten
SENSIBLE PII	
VERTRAULICHE PII	
VERTRAULICH	
INTERNE PII	
INTERN	
ÖFFENTLICH	Am wenigsten sensibel

1. Auf der Grundlage der Klassifizierung von Citi-Informationen muss Citi mit dem Lieferanten zusammenarbeiten, um das zum Schutz dieser Informationen erforderliche Sicherheitsniveau festzulegen, und der Lieferant muss sicherstellen, dass ausreichende Kontrollen sowie alle erhöhten oder geänderten Niveaus, die Citi möglicherweise verlangt, vorhanden sind.
2. Interne oder höher eingestufte Informationen müssen auf Geräten gespeichert werden, die von Dritten verwaltet werden und einem Vertrag zwischen dem Dritten und Citi unterliegen, der Vertraulichkeitsbestimmungen enthält, die mit den Richtlinien und Standards von Citi im Einklang stehen.
3. Wenn der Lieferant die Verwendung von Geräten erlaubt, die nicht dem Unternehmen gehören, um Citi-Daten zu speichern (d. h. Geräte, die von einer Viertpartei verwaltet werden), muss der Lieferant über eine Richtlinie verfügen, die eine spezifische Genehmigung durch das Management erfordert, und Richtlinien und Überwachungsverfahren für die Verwendung festgelegt haben und Entsorgung von Citi-Informationen.
4. Der Lieferant muss Citi-Informationen stets vor unbefugtem Zugriff, Änderung oder Löschung schützen.
5. Als vertraulich oder höher eingestufte Citi-Informationen, die über elektronisch transportierbare Medien (ETM) übertragen werden, müssen mit einem zugelassenen kryptografischen Algorithmus verschlüsselt und die Zustellung bestätigt werden. Der Lieferant muss bestätigen, dass das ETM beim Empfänger eingegangen ist. Wenn bis zum voraussichtlichen Liefertermin keine Empfangsbestätigung eingeht, muss der Lieferant Citi benachrichtigen.

17.8 Sichere Konfiguration.

1. Der Lieferant ist verpflichtet, einen dokumentierten sicheren Konfigurationsstandard für alle Anlagen aufrechtzuerhalten, die das Potenzial haben, Citi-Informationen zu speichern, zu verarbeiten, darauf zuzugreifen oder sie zu übertragen.
2. Der Lieferant muss Informationssicherheitskontrollen in seine Prozesse und Verfahren für die Auswahl, Entwicklung und Implementierung von Anwendungen, Produkten und Dienstleistungen integrieren.

3. Der Lieferant muss für alle Systeme, in denen Citi-Informationen gespeichert, verarbeitet und/oder übertragen werden, über ein Verfahren zur sicheren Systembereitstellung verfügen.
4. Der Lieferant muss für alle Systeme ein sicheres Systemabbild oder eine sichere Vorlage vorhalten.
5. Alle Standard-Benutzerkonten und -Kennwörter müssen von hersteller-unterstützten Systemen, Netzwerkgeräten und Anwendungen entfernt und/oder geändert werden.
6. Jedes kompromittierte System oder jeder kompromittierte Service muss unter Verwendung eines Systemabbilds oder einer Vorlage mit nachgewiesener Integrität neu aufgebaut und konfiguriert werden.
7. Jede Änderung, die an einer sicheren Konfiguration vorgenommen werden soll, muss von der Geschäftsleitung über den Änderungsmanagementprozess des Lieferanten genehmigt werden.
8. Der Lieferant muss Citi über alle Änderungen an der sicheren Konfiguration informieren.
9. Das Verfahren zur sicheren Systembereitstellung muss Tools umfassen, die bei der Bereitstellung in der Produktionsumgebung automatisierte Konfigurationsprüfungen der Sicherheits- und Standardkonfigurationen ermöglichen sowie die fortlaufende Überwachung der Einhaltung der Basiskonfiguration und die Erkennung von Abweichungen davon sicherstellen.

17.9 Verschlüsselungsanforderungen

Der Lieferant darf als vertraulich oder höher eingestufte Informationen nicht unverschlüsselt übertragen. Als vertraulich oder höher eingestufte Informationen müssen **durchgängig** mit von Citi genehmigten Tools oder Lösungen verschlüsselt werden. Die genehmigten Protokolle und die jeweiligen Versionsnummern für die verschlüsselte Datenübertragung lauten wie folgt:

1. Beim Austausch von Authentifizierungs- und Autorisierungsinformationen: SAML v2.0, OAuth v2.0 (nur Autorisierung),
2. Zum Schutz der Kommunikationskanäle und des damit verbundenen Austauschs von Schlüsseln sind nur die folgenden Netzwerksicherheitsprotokolle zulässig:
 - a) TLS v1.3 (bevorzugt) und alle TLS v1.3-Suiten sind zulässig. Wenn TLS v1.3 das einzige aktivierte Protokoll ist, ist keine zusätzliche Überprüfung erforderlich.
 - b) Ist TLS v1.3 technisch nicht umsetzbar und wird stattdessen TLS 1.2 verwendet, ist derzeit eine Bewertung von B oder höher durch SSL Labs akzeptabel; eine zusätzliche Überprüfung ist nicht erforderlich.

Daten, die dauerhaft in der Umgebung von Citi-Drittanbietern gespeichert oder ausgetauscht werden, müssen mit von Citi zugelassenen Tools oder Lösungen vollständig verschlüsselt werden. Zugelassene Algorithmen und Schlüssellängen zum Verschlüsseln von Daten lauten wie folgt:

1. **Erweiterter Verschlüsselungsstandard (AES):** Zugelassene Schlüssellängen: 256 oder mehr Bits. Eingeschränkter Modus: Der Modus des

elektronischen Codebuchs (ECB) ist verboten, außer wenn die Klartextmenge kleiner oder gleich der Blocklänge ist. Festplattenverschlüsselung: AES mit 256-Bit-Schlüssel wird empfohlen. AES mit einer Schlüssellänge von 128 Bit ist als TLS-Chiffre zulässig. Diese wird jedoch ab dem 31. Dezember 2028 zugunsten einer Schlüssellänge von 256 Bit oder höher nicht mehr zulässig sein, um die Angleichung von Citi an internationale Zeitvorgaben zu unterstützen (siehe NIST 8547 IPD).

2. **ChaCha20 (eine Strom-Chiffre für zugehörige Anwendungsfälle):** Zugelassene Schlüssellängen: 128 oder 256 Bit, mit 96-Bit-Nonce und 32-Bit-Blockanzahl oder 64-Bit-Nonce und 64-Bit-Blockanzahl. Maximale Datengröße: 16 Petabyte.

Zulässige Public-Key-Kryptosysteme, Schlüsselaustausch, Vereinbarungsmechanismen, Message-Digest- und Schlüsselableitungsfunktionen sind wie folgt:

Hinweis zur Quantenbereitschaft des Lieferanten: Lieferanten sind verpflichtet, dem Citi Quantum Readiness Program Team über den ([survey link](#)) ihren Plan zur Umsetzung der Anforderungen aus Tabelle 2 und Tabelle 4 des NIST IR 8547 (IPD) vorzulegen.

1. **Kryptosysteme mit öffentlichen Schlüsseln und Mindestschlüssellängen:**
 - a) Rivest–Shamir–Adleman (RSA): 2048 Bit.
 - b) Digitaler Signaturalgorithmus (DSA): 2048 Bit. DSA darf nicht zur Sicherung von Citi-Daten verwendet werden, die außerhalb von Citi verarbeitet oder gespeichert werden.
 - c) Algorithmus für digitale Signaturen mit elliptischen Kurven (ECDSA): 256 Bit und wie in ANSI X9.62 mit von NIST empfohlenen Kurven angegeben.
2. **Schlüsselaustausch- und Vereinbarungsmechanismen und Mindestschlüssellängen:**
 - a) Diffie-Hellman (DH)/Ephemeral Diffie-Hellman (DHE): 2048 Bit.
 - b) Elliptic-curve Diffie-Hellman (ECDH)/Ephemeral Elliptic-curve Diffie-Hellman (ECDHE): 256 Bit und wie in ANSI X9.63 mit von NIST empfohlenen Kurven angegeben¹.
3. **Message-Digest-Funktionen:** Das Erstellen eines Verschlüsselungsschlüssels mit einer Länge, die größer ist als die Anzahl der zufälligen Bits in dem Material, das zum Generieren des Hashs verwendet wird, ist verboten.
 - a) SHA-1 ist nur für Anwendungen zulässig, die keine digitalen Signaturen verwenden. SHA-2-Familie, SHA-3-Familie und POLY-1305: Akzeptabel für alle kryptografischen Hash-Funktionsanwendungen.
4. **Passwortbasierte Schlüsselableitungsfunktionen und Mindestanforderungen:**
 - a) PBKDF2: Minimale Iterationsanzahl von 10000 mit einem Salt von mindestens 16 Bytes.
 - b) HKDF: Muss mit einem Salt versehen sein, und der Info-Eingabewert muss einbezogen werden.
 - c) SKRYPT: Mindesttrundenzahl/Kostenfaktor 10.

¹ ECDHE wird bevorzugt.

- d) Die Verwendung der NIST SP800-108 KDF für die Stromverschlüsselung ist unzulässig. Die NIST SP 800-108 KDF-Modi, nämlich die Counter-, Feedback- und Double-Pipeline-Iterationsmodi, sind zulässig.
- e) Argon2 wird empfohlen.

5. Passwort-Hash-Funktionen und Mindestanforderungen:

- a) Bcrypt (zur lokalen Speicherung von Authentifizierungsmaterial): Mindestrundenzahl/Kostenfaktor von mindestens 10.
- b) Argon2 oder PBKDF2 werden für die Passwort-Hash-Funktion empfohlen, wenn Passwörter lokal auf Produkten oder Systemen des Lieferanten gespeichert werden.

17.10 Externe E-Mail

Die Verschlüsselungsanforderung für einzelne E-Mails, die Informationen von Citi mit der Klassifizierung „Vertraulich“ oder höher enthalten, wenn der Lieferant nicht berechtigt ist, von Citi genehmigte Ende-zu-Ende-Verschlüsselungssoftware oder -Tools gemäß den Vorschriften und/oder Richtlinien des Lieferanten zu verwenden, kann vollständig erfüllt werden durch Transportverschlüsselung (z. B. Gateway-zu-Gateway-Verschlüsselung über Transport Layer Security (TLS)). Die genehmigten sicheren E-Mail-Protokolle sind:

1. **Identitätsbasierte Verschlüsselung (Identify-Based Encryption, IBE)** umfasst verschlüsselte E-Mails und kann nur innerhalb von Citi-Kundenlösungen und sicheren E-Mail- und E-Delivery-Systemen verwendet werden.
2. **Mandatory TLS (MTLS)** bietet Sitzungsverschlüsselung (verschlüsselt nicht die E-Mail-Nutzdaten) und kann mit Anbietern, Partnern und Kunden verwendet werden, mit denen zuvor Vereinbarungen über die Nutzung getroffen wurden.
3. **Domain Keys Identified Mail (DKIM)** bietet Quellenauthentifizierung und Schlüsselverwaltung und kann mit Anbietern, Partnern und Kunden verwendet werden.

17.11 Private Netzwerke

Private Netzwerke, die von einer anerkannten Behörde unabhängig reguliert werden und die Standards der Finanzdienstleistungsbranche für Transaktionen zwischen lizenzierten oder akkreditierten Gegenparteien (z. B. SWIFT oder eine Zentralbank) erfüllen, können von der Anforderung zur Verschlüsselung vertraulicher personenbezogener Daten während der Übertragung ausgenommen werden, bis diese Netzwerke die erforderliche Infrastruktur zur vollständigen Unterstützung verschlüsselter Übertragungen bereitstellen.

17.12 Sprache und Fax

Informationen mit der Citi-Klassifizierung „Vertraulich“ oder höher, die per Fax gesendet oder über Sprachanrufe (einschließlich Voice over IP, VOIP) besprochen werden, können unverschlüsselt gesendet werden. Bei Bedarf muss der Lieferant spezielle Verfahren und Richtlinien entwickeln, um vertrauliche oder höherwertige Informationen zu schützen, die über diese Kanäle gesendet werden.

17.13 Verwaltung kryptografischer Schlüssel und Zertifikate

Der in diesem Abschnitt verwendete Begriff „Sichere Grenze“ bezieht sich auf eine vom Cryptographic Module Validation Program (CMVP) validierte Grenze, wie etwa den Federal Information Protection Standard (FIPS) (FIPS 140-2/3 Level 2 ist die minimal akzeptable Sicherheitsstufe). (Vertrauliche Rechenenklaven wie AWS Nitro Enclaves sind zulässig. Andere einzigartige Fälle von Sicherheitsgrenzen müssen von Citi genehmigt werden).

1. Der Lieferant muss aktuelle, dem Industriestandard entsprechende kryptografische Algorithmen und Mindestschlüssellängen für die Verschlüsselung und Signierung einsetzen (einschließlich SSH-Schlüssel). Der Lieferant muss über seinen Änderungsmanagementprozess die Gewähr bieten, dass solche Algorithmen und Schlüssellängen aktualisiert werden, um sie an die Industriestandards anzupassen.
2. Der Lieferant muss über einen formell dokumentierten Prozess für den Lebenszyklus von Schlüsseln, Geheimnissen und Zertifikaten verfügen, der Kontrollen zum Schutz sensibler Materialien vor unbefugter Nutzung oder Offenlegung umfasst. Alle kryptografischen Geheimnisse und Ereignisse im Schlüssellebenszyklus dürfen ausschließlich innerhalb einer Sicherheitsgrenze stattfinden. Der gesamte Zugriff auf privilegierte und gesicherte Bereiche muss dokumentiert werden. Der Lieferant muss für alle wichtigen Lebenszyklusereignisse ein Sequenzdiagramm bereitstellen, in dem die beteiligten Akteure, Einheiten und Grenzen hervorgehoben werden.
3. Kryptografische Schlüssel müssen einen eindeutigen Zweck haben und dürfen nie für andere Zwecke verwendet werden, wie z. B. die Verwendung des gleichen Verschlüsselungsschlüssels für die Festplattenverschlüsselung und die Datenverschlüsselung oder des gleichen Verschlüsselungsschlüssels für die Nutzdatenverschlüsselung und die Datenbankverschlüsselung. Die Wiederverwendung kryptografischer Schlüssel über mehrere Mandanten durch einen SaaS-Anbieter ist standardmäßig verboten und kann nur für nicht kritische, risikoreiche Anwendungsfälle zugelassen werden, in denen Citi-Informationen als „vertrauliche PII“, „Sensible PII“ und „Eingeschränkt“ klassifiziert sind, vorbehaltlich der ausdrücklichen Genehmigung des Security Architecture Council.
4. Bei allen kryptografischen Schlüsseln (symmetrisch oder asymmetrisch) darf der private Schlüssel oder das private Schlüsselmaterial (z. B. Seeds oder Teile eines privaten Schlüssels) zu keinem Zeitpunkt im Klartext angezeigt werden. Private Schlüssel oder privates Schlüsselmaterial (wie ein Seed oder ein Teil eines privaten Schlüssels) dürfen niemals die sicheren Grenzen verlassen, mit Ausnahme von kurzlebigen Schlüsseln wie dynamischen Sitzungsschlüsseln. Wenn das Design die Übertragung eines symmetrischen Schlüssels oder eines privaten Schlüssels oder eines privaten Schlüsselmaterials zwischen sicheren Enklaven/privilegierten Zugriffsgrenzen erfordert, muss diese Übertragung ausschließlich in verschlüsselter Form unter Verwendung eines symmetrischen Schlüsselverpackungsschlüssels oder eines öffentlichen Schlüsselübertragungsschlüssels über gegenseitig TLS-verschlüsselte Tunnel erfolgen, und eine solche Übertragung muss von Citi schriftlich genehmigt werden. Der private Transportschlüssel darf in

diesen Fällen niemals die sichere Grenze des privilegierten Zugriffs verlassen, in der er generiert wurde.

5. Ein symmetrischer Key-Wrapping-Schlüssel muss in zwei oder mehr Schlüsselkomponenten aufgeteilt und vor der Verteilung sowie vor der manuellen Schlüsseingabe bzw. dem manuellen Laden mittels XOR kombiniert werden. Der symmetrische Key-Wrapping-Schlüssel muss innerhalb der sicheren Sicherheitsgrenze über angemessene Zugriffssteuerungslisten (ACLs) verfügen, beispielsweise in CMVP-validierten Modulen, und darf nicht außerhalb der Sicherheitsgrenze gespeichert werden.
6. Der Zugriff von Personen, Diensten oder automatisierten Agenten auf Keystores oder sichere Bereiche, die private Schlüssel oder Geheimnisse oder privates Schlüsselmaterial (wie Seeds oder Teile eines privaten Schlüssels) enthalten, muss ordnungsgemäß getrennt werden, wobei der Zugriff auf autorisiertes Personal oder autorisierte Systeme beschränkt werden muss.
7. Jede Anfrage zum Zugriff auf die Keystores, die private oder symmetrische Schlüssel enthalten, muss protokolliert und mit Details wie wer, wann und Zweck des Zugriffs für Prüfzwecke dokumentiert werden.
8. Der Lieferant darf keine selbstsignierten und Platzhalterzertifikate oder Standard-SSL-Zertifikate verwenden.
9. Alle kryptografischen Schlüssel müssen über eine definierte Kryptoperiode verfügen, wie in NIST SP800-57 Teil 1, Revision 6 empfohlen. Schlüssel müssen vor Ablauf ihrer Gültigkeitsdauer erneuert oder rotiert werden, um Zeiträume für Änderungen, Planungskonflikte und System-Freeze-Phasen zu berücksichtigen.
 - a) Beim Ersetzen eines abgelaufenen Zertifikats ist die Wiederverwendung des alten asymmetrischen Schlüsselpaars verboten.
10. Kryptografische Schlüssel müssen als kompromittiert behandelt werden, sobald der Verdacht besteht, dass die Integrität des Schlüssels, des Mediums, auf dem der Schlüssel gespeichert oder weitergegeben wird, oder die Vertraulichkeit des symmetrischen oder privaten Schlüssels kompromittiert ist. Alle kompromittierten Schlüssel müssen aus dem Betrieb entfernt und alle zugehörigen Zertifikate widerrufen werden.
11. Drahtlose Netzwerke sind mit Verschlüsselungsalgorithmen nach Branchenstandard zu verschlüsseln.
12. Lieferanten, die jegliche kryptographische Mechanismen einsetzen, müssen Schlüsselmanagementtools und -techniken gemäß Branchenstandard verwenden. Die Schlüsselrolle im Management muss vom operativen Management getrennt werden.
13. Lieferanten dürfen Cloud-native KMS- und PKI-Dienste nur dann nutzen, wenn die Interoperabilität mit den von Citi Data Security Services bereitgestellten PKI- und KMS-Diensten gewährleistet ist und kryptografische Kontrollen nicht außerhalb der kryptografischen Governance von Citi delegiert werden.

17.14 Verantwortung für die Zugriffskontrolle

Um alle kontrollierten Informationssysteme, die zum Speichern, Zugreifen, Verwalten, Verarbeiten oder Übertragen vertraulicher oder höherwertiger Informationen von Citi verwendet werden, vor unbefugtem Zugriff zu schützen, ist der Lieferant für die Durchsetzung des Grundsatzes der geringsten Privilegien verantwortlich, indem er die Benutzerberechtigungen auf das für die jeweilige Arbeitsfunktion erforderliche Mindestzugriffsniveau beschränkt und die Bereitstellung des logischen Zugriffs auf alle Systeme und Anwendungen verwaltet. Kontrollen müssen vollständig dokumentiert und überprüfbar sein. Die Bereitstellung und Entziehung von Zugriffsberechtigungen, einschließlich Passwortzurücksetzungen und Aktivierungen, müssen nach Möglichkeit über einen automatisierten Prozess erfolgen, um das Risiko potenzieller menschlicher Fehler zu mindern, die zu übermäßigen Berechtigungen führen können, und um die Ausrichtung an Branchenstandards sicherzustellen.

1. Der Lieferant ist für die Zugriffsrechte aller Benutzer in seiner Organisation verantwortlich.
2. Der Lieferant muss Zugriffskontrollen einrichten, die sicherstellen, dass den Benutzern nur die für die Ausübung ihrer Funktion unbedingt erforderlichen Rechte und Berechtigungen gewährt werden.
3. Der Lieferant hat ein Verfahren zu implementieren, so dass alle voreingestellten Zugriffsrechte entfernt, deaktiviert oder geschützt werden, um unerlaubte Verwendung zu verhindern.

17.15 Benutzerzugriffsverwaltung

Der Lieferant muss die Bereitstellung des logischen Zugriffs auf Systeme und Anwendungen verwalten, die Informationen von Citi mit der Klassifizierung „Vertraulich“ oder höher verarbeiten, speichern und/oder übertragen. Dazu gehören:

1. Identifikation und Inventarisierung von zugelassenen Authentifizierungssystemen.
2. Die Anforderung, dass jeder Zugriff auf Citi-Daten die Genehmigung eines Managers oder eines von ihm Beauftragten und des Systembesitzers erfordert. Der Lieferant muss sicherstellen, dass seinem gesamten Personal mit Zugriff auf Citi-Daten dieser Zugriff nur nach dem Need-to-know-Prinzip gewährt wird.
3. Eine Anforderung, dass keine Kombination aus Berechtigungen/Funktionen für einen einzelnen Benutzer bereitgestellt werden darf, wenn dies einen Interessenkonflikt oder einen Verstoß gegen die Maker-Checker-Regeln darstellt.
4. Ein Überwachungsprozess zur Überwachung und Verwaltung der Zugriffsrechte, die jedem Benutzer auf dem System gewährt/entzogen wurden.
5. Zugriffsanfragen dürfen nicht auf der Spiegelung/Klonung der Berechtigungen eines anderen Benutzers basieren; Anfragen müssen explizite Rollen/Berechtigungen mit einer geschäftlichen Begründung enthalten, um eine schleichende Ausweitung von Berechtigungen zu verhindern und das Prinzip der geringsten Privilegien durchzusetzen.

17.16 Benutzeridentifizierung und -authentifizierung

Alle vom Lieferanten kontrollierten Informationssysteme müssen die Identität der Benutzer oder der Systeme prüfen, die auf diese Plattform zugreifen, ehe eine Sitzung oder Transaktion eingeleitet wird, bei der ein Zugriff auf Citi-Informationen stattfinden kann.

1. Die Benutzer müssen eindeutig identifiziert oder durch eine Benutzer-ID der Technologieplattform zugeordnet werden.
2. Benutzer müssen gegenüber der Technologieplattform mithilfe einer genehmigten Authentifizierungsmethode authentifiziert werden. Der Lieferant sollte sich an seinen primären Geschäftsansprechpartner (BAO) wenden, um die aktuell genehmigten Methoden zu erfahren.
3. Der Gebrauch einer gemeinsamen Authentifizierungsinfrastruktur (z. B. Single Sign-On, Reduced Sign-On und andere gemeinsame Authentifizierungsdienste) muss in Übereinstimmung mit den Authentifizierungsanforderungen von Citi erfolgen. Der Lieferant sollte sich bezüglich der aktuell genehmigten Methoden an seinen primären BAO wenden.
4. Identitätsprüfdaten (IVD), die zur Authentifizierung eines Benutzers gegenüber einem Informationssystem verwendet werden, müssen bei der Übertragung und Speicherung verschlüsselt werden. Informationen zu den Verschlüsselungsanforderungen finden Sie in Abschnitt 17.9.
5. Jedes Konto, das vom Personal des Lieferanten für den Zugriff auf Citi-Systeme verwendet wird, muss einer einzigartigen von Citi zugewiesenen Kennung (z. B. GEID) zugeordnet werden; generische/gemeinsam verwendete Benutzerkennungen für menschliche Benutzer sind verboten, um die Rückverfolgbarkeit, die Durchsetzung von SOD und eine ordnungsgemäße Vorbereitung auf Prüfungen zu gewährleisten.

17.17 Identifizierung von privilegiertem Zugriff und temporär privilegiertem Zugriff

Der Lieferant muss ein Inventar aller Identitäten führen und Identitäten identifizieren, die privilegierten Zugriff oder Zugriff auf elektronische Speicher (Datensätze oder Datenbanken zur Unterstützung von Geschäftsanwendungen) haben, die Informationen enthalten, die als vertrauliche PII oder höher eingestuft sind. Der Lieferant muss Kontrollen implementieren, die vor der unbefugten Nutzung dieser Identitäten schützen. Wenn ein Arbeitnehmer Zugriff auf eine privilegierte ID oder auf die zuvor genannten elektronischen Repositorien benötigt, muss der Zugriff über einen temporären Zugriffsverwaltungsprozess gewährt werden, der:

1. Der Anforderer muss auf einer vorab genehmigten Liste autorisierter Benutzer stehen oder zum Zeitpunkt der Nutzung eine Genehmigung einholen.
2. Es ist eine dokumentierte Begründung in einem Änderungs-/Problemticket erforderlich, bevor der Zugang gewährt wird.
3. Eine unabhängige Überprüfung der mithilfe des Zugangs vorgenommenen Aktivität ist inbegriffen.

4. Ein Verfahren zur Initiierung des Widerrufs/der Löschung des Zugriffs am Ende des vorübergehenden Zugriffs ist inbegriffen.
5. Ermöglicht die Verlängerung des Zugriffs auf Produktionsumgebungen sowie des Zugriffs zur Stabilisierung nach der Implementierung – etwa nach einem größeren Upgrade oder einer Fehlerbehebung – auf bis zu sieben (7) Kalendertage.

17.18 Überprüfung von Benutzerzugriffsrechten

1. Der Lieferant muss einen dokumentierten Prozess implementieren, um unnötige Benutzerberechtigungen für kontrollierte Informationssysteme, die zur Speicherung, Verarbeitung, Verwaltung und/oder Übertragung von Citi-Informationen verwendet werden, mindestens halbjährlich zu überprüfen, zu verifizieren und zu löschen.
2. Benutzer dürfen ihre eigenen Berechtigungen oder die einer Person, die ihnen Überprüfungsverantwortung übertragen hat, nicht selbst überprüfen oder genehmigen.
3. Nach einem Funktionswechsel eines Mitarbeiters des Lieferanten innerhalb von Citi hat der Lieferant 14 Kalendertage Zeit, um eine Überprüfung des Zugriffs und der Berechtigungen vorzunehmen und den Zugriff auf Citi-Daten zu entfernen, wenn er für die neue Funktion des Mitarbeiters nicht mehr erforderlich ist.

17.19 Sichere Anmeldeverfahren

1. Gespernte Benutzerzugangskennungen sind über einen Zurücksetzungsdienst nach Branchenstandard oder eine andere zulässige Funktion wieder freizuschalten. Ein Bannertext muss, sofern er vom Betriebssystem oder der Anwendung unterstützt wird, an allen Netzwerkeintrittspunkten angezeigt werden, an denen sich ein Benutzer erstmals anmeldet oder er authentifiziert wird.

17.20 Passwortverwaltungssystem

1. Statische Benutzerpasswörter dürfen niemals in Klarschrift auf dem Bildschirm angezeigt werden. Die Funktionalität zum Umschalten der Passwortsichtbarkeit ist von dieser Anforderung ausgenommen, sofern:
 - (1) die Passworteingabe standardmäßig maskiert ist,
 - (2) die Sichtbarkeit des Passworts nur durch eine explizite Benutzeraktion initiiert werden kann, (3) das Passwort innerhalb von maximal 15 Sekunden nach Beendigung der Benutzeraktion automatisch erneut maskiert wird.
2. Passwörter privilegierter Funktions-IDs dürfen nicht als Klartext hartcodiert werden.
3. Statische Passwörter müssen mindestens zehn (10) Zeichen umfassen, sowohl Buchstaben als auch Zahlen enthalten und die Groß-/Kleinschreibung berücksichtigen. Die Groß-/Kleinschreibung bei statischen Passwörtern muss an jeder Authentifizierungsstelle validiert werden. Statische Passwörter von Funktions-IDs (FID) müssen mindestens 15 Zeichen auf Anwendungen enthalten, die nach dem 31. August 2026 eingeführt wurden.

4. PINs dürfen nur dann als alleinige Methode zur Authentifizierung beim Zugriff auf Informationssysteme dienen, wenn die PINs wegen baulichen Beschränkungen der Geräte nötig sind (z. B. Zifferntastatur, Telefon, Smartcard).
5. Alle feststehenden Passwörter sind mindestens alle 90 Kalendertage zu ändern.
6. Alle statischen Passwörter müssen nach höchstens sechs (6) aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen oder sechs (6) aufeinanderfolgenden Versuchen, das Passwort zurückzusetzen, gesperrt werden. Die Entsperrung von Passwörtern muss über eine ID-Administrator-Funktion erfolgen oder erfolgt automatisch nach frühestmöglichen 30 Minuten.
7. Alle Authentifizierungssysteme müssen eine Kontrolle der Inaktivität/Nichtbenutzung der Anmeldung erzwingen, die 100 Kalendertage nicht überschreiten darf. Sofern technisch möglich, können deaktivierte Anmeldungen durch den Benutzer oder eine andere autorisierte Funktion wieder aktiviert werden.
8. Das Überprüfungsverfahren muss sicherstellen, dass dasselbe Passwort nicht bei einer der letzten sechs (6) Änderungen verwendet wurde.

17.21 Verwendung von Systemdienstprogrammen

Der Lieferant muss sicherstellen, dass die Verwendung von Dienstprogrammen, die System- und Anwendungssteuerungen außer Kraft setzen können (z. B. Hochfahren von Peripheriegeräten), eingeschränkt und kontrolliert wird.

17.22 Sitzungs-Timeout

1. Alle Benutzer eines kontrollierten Informationssystems, das zur Speicherung, Verarbeitung und/oder Übertragung von Citi-Informationen verwendet wird, müssen sich anmelden und erneut authentifizieren.
2. Benutzern ist vorzuschreiben, dass sie sich nach einem Inaktivitätszeitraum von weniger als 30 Minuten neu anmelden. Aktivität umfasst dabei jede Eingabe am Endpunkt (Maus, Tastatur, Touchscreen usw.). Wird die Regel durch den passwortgeschützten Bildschirmschoner erzwungen, ist die Durchsetzung in der Anwendung oder über Single Sign-On nicht erforderlich.

17.23 Beendigung des Benutzerzugriffs

1. Bei Kündigung oder Austritt müssen Benutzerzugänge oder Berechtigungen, die den Zugriff auf vertrauliche oder höherwertige Daten von Citi ermöglichen könnten, einschließlich Benutzeranmeldung bei Desktop/Active Directory, Single Sign-on (SSO), E-Mail, One-Time-Password-Token (OTP) und Fernzugriff, sofort entfernt werden.
2. Wenn ein Mitarbeiter Zugriff auf Systeme hat, die Eigentum von Citi sind und von Citi verwaltet werden, muss der Citi Business Relationship Manager, BAO oder der BAO-Support bei einem Funktionswechsel oder der Kündigung dieses Mitarbeiters umgehend benachrichtigt werden, um sicherzustellen, dass der Citi Business Manager die Zugriffssperre für entlassene Mitarbeiter bis zum Ende ihres Kündigungsdatums einleitet.

3. Der Lieferant muss über einen dokumentierten Prozess verfügen, um bei Beendigung des Arbeitsverhältnisses oder Ausscheiden eines Mitarbeiters oder Nicht-Mitarbeiters innerhalb der in Abschnitt 17.23.2 festgelegten Fristen die Zugriffsrechte auf alle Informationswerte zu entziehen.
4. Wenn der Lieferant eine Anomalie in Bezug auf 17.23.1-17.23.3 feststellt, muss er unverzüglich den Citi Business Relationship Manager, BAO oder den BAO-Support informieren und eine fundierte Begründung sowie Kontrollmaßnahmen vorlegen.

17.24 Fernzugriff

Der Lieferant muss über Fernzugriffskontrollen verfügen, um den Zugriff auf Netzwerke zu schützen, die Daten von Citi mit der Klassifizierung „Vertraulich“ oder höher speichern, verarbeiten oder übertragen können:

1. Der Fernzugriff auf Informationssysteme, die zur Speicherung, Verwaltung, Verarbeitung und/oder Übertragung von Citi-Informationen dienen, muss vor unerlaubtem Gebrauch geschützt werden.
2. Alle vom Lieferanten verwalteten Laptops und alle vom Lieferanten verwalteten Desktop-Computer, die zum Speichern, Verarbeiten und/oder Übertragen von Citi-Informationen verwendet werden, müssen mit einem Verschlüsselungsprogramm verschlüsselt werden, das den Industriestandards entspricht, wenn es eine lokale Speicherung/Verarbeitung von Informationen mit einer Citi-Informationsklassifizierung von Vertraulich oder höher gibt.
3. Fernverbindungen dürfen nur über zugelassene Fernzugriffslösungen hergestellt werden, die eine mehrstufige Authentifizierung (MFA) verwenden.
4. Wenn vom Lieferanten verwaltete Geräte direkt mit dem Internet verbunden sind, muss auf ihnen eine persönliche Firewall aktiv sein (d. h. nicht eine vom Lieferanten verwaltete Firewall bzw. Proxy).
5. Vom Lieferanten verwaltete Geräte müssen regelmäßig mit dem Lieferantennetzwerk verbunden werden, um erforderliche Software- und/oder Antiviren-Tool-Updates zu empfangen und zu installieren. Die Installation dieser Updates ist Voraussetzung für den vollständigen Zugriff auf das Netzwerk. Für den ausdrücklichen Zweck der Aktualisierung des Geräts kann ein eingeschränkter Zugriff gestattet werden.
6. Wenn nicht firmeneigene und verwaltete Geräte verwendet werden, um auf vertrauliche oder höhere Informationen von Citi zuzugreifen, müssen sie eine autorisierte Lösung verwenden, die das Herunterladen auf den lokalen Rechner nicht zulässt. Die folgenden Kontrollen müssen vorhanden sein:
 - a) Das Herunterladen von Citi-Daten auf ein Gerät außerhalb einer vom Unternehmen verwalteten Lösung muss verhindert werden.
 - b) Der Lieferant muss sicherstellen, dass ein solcher Zugriff entweder durch eine tokenbasierte oder zertifikatsbasierte Authentifizierung unter Verwendung standardmäßiger Fernzugriffstechnologien (z. B. Virtual Desktop Interface (VDI)) abgesichert ist.
 - c) Fernzugriffslösungen wie Terminal Services und VMware Horizon müssen so konfiguriert sein, dass die Zwischenablagefreigabe und die Laufwerkszuordnung über Blast und PCoIP deaktiviert sind und die Protokolle RDP und SSH deaktiviert werden.

7. Wenn Soft-Token für die Multi-Faktor-Authentifizierung (MFA) verwendet werden, beispielsweise für den Zugriff auf eine Softwareanwendung auf einem mobilen Gerät, muss die Soft-Token-Authentifizierungssoftware den Benutzer authentifizieren (z. B. durch Passwort, biometrische Merkmale usw.) und die Verwendung verhindern, wenn das Mobiltelefon einen Jailbreak aufweist oder gerootet ist (d. h. ein anderes Betriebssystem als das vom Hersteller des mobilen Geräts zertifizierte und bereitgestellte Betriebssystem verwendet).
8. Alle Mitarbeiter des Lieferanten, einschließlich, aber nicht beschränkt auf festangestellte/befristete Mitarbeiter, Auftragnehmer und Subunternehmer, die besonderen, privilegierten und/oder administrativen Zugriff auf Systeme, Datenspeicher, Anwendungen und/oder Infrastruktur benötigen, einschließlich, aber nicht beschränkt auf Systemadministratoren, Datenbankadministratoren, Zugriffskontrolladministratoren, Firewall-Administratoren, Website-Administratoren usw., die direkt oder indirekt mit den für Citi erbrachten Dienstleistungen in Verbindung stehen, dürfen nur über MFA authentifiziert werden, und dieser Zugriff wird vom Lieferanten unabhängig protokolliert und gemäß diesen Anforderungen auf verdächtige Aktivitäten und/oder unbefugten Zugriff überwacht.
9. Für Geräte, die sich im persönlichen Besitz befinden oder Eigentum Dritter sind, muss der Lieferant über eine wirksame Lösung verfügen, um sicherzustellen, dass diese Geräte über eine zugelassene Betriebssystemversion, Patch-Levels, Antiviren- und Anti-Malware-Lösungen verfügen, bevor sie sich im Netzwerk anmelden dürfen.
10. Der Lieferant muss sicherstellen, dass alle seine Mitarbeiter:
 - a) Einen privaten, dedizierten Remote-Arbeitsbereich unterhalten, der keine Sprachassistentengeräte (z. B. Siri, Alexa), Videoaufnahmegeräte und/oder andere Foto-, Video- oder Audioabhör-/Aufnahmegeräte enthält. Unbefugten Personen ist es nicht gestattet, Daten, Systeme und Anwendungen einzusehen, die auf den Bildschirmen der Remote-Computersysteme erscheinen.
 - b) Das Computergerät sperren werden, wenn es unbeaufsichtigt bleibt, um sicherzustellen, dass der unbefugte Zugriff auf den Bildschirm angemessen verhindert wird.

17.25 Clean-Desk-Richtlinie

Lieferantenmitarbeiter haben Citi-Informationen in jeder Gestalt zu schützen, einschließlich physischer Informationen, die an ihrem Arbeitsplatz verwendet oder aufbewahrt werden. Lieferanten sind verpflichtet, diese Anforderung mindestens einmal jährlich über IS-Schulungen oder andere Kanäle an alle Mitarbeiter weiterzugeben.

17.26 Brandschutz

1. Der Lieferant hat die einschlägigen gesetzlichen und aufsichtsrechtlichen Vorschriften zur physischen Sicherheit einzuhalten und eine sichere

Arbeitsumgebung einschließlich unter Berücksichtigung der örtlichen Brandschutzvorschriften sicherzustellen.

2. Der Lieferant muss ein oder mehrere Feuererkennungs-, Alarm- und Unterdrückungssysteme verwenden. Das/die System(e) müssen halbjährlich geprüft und jährlich getestet werden.

17.27 Physische Sicherheit

1. Citi-Informationen sind in sicheren Bereichen aufzubewahren, die nur für befugte Mitarbeiter zugänglich sind.
2. Der Lieferant muss über ein dokumentiertes und überprüfbares System zur physischen Zugangskontrolle verfügen.
3. Der Lieferant muss eine Kombination aus Sicherheitsalarm-/Einbruchmeldesystemen einsetzen, die einen von einem Dritten überwachten Sicherheitsalarm, Sicherheitspersonal und Videoüberwachung umfassen, die der Umgebung und den erbrachten Dienstleistungen angemessen sind.
4. Der Lieferant hat eine belegte Besucherregelung vorzuhalten, zu der die Maßgabe gehört, dass alle Besucher sich bei Ankunft überprüfbar ausweisen und sich ein- und austragen.

17.28 Betriebssicherheitsverfahren und Verantwortlichkeit

1. Der Prozess zum Lieferantenwechsel muss wichtige Kontrollpunkte für die Registrierung, Überprüfung, Prüfung, Genehmigung, Umsetzung und den Abschluss von Änderungen umfassen. Der Lieferant muss außerdem über einen Notfalländerungsprozess verfügen, der alle oben aufgeführten Schritte einschließlich einer Hierarchie der vorgeschriebenen Genehmigungen erfordert.
2. Der Lieferant muss über einen überprüfbaren Prozess zum Kapazitätsmanagement verfügen, der unter anderem Kennzahlen/Indikatoren zu Verfügbarkeit, Kapazität und Leistung, eine Beurteilung der geschäftlichen Auswirkungen sowie die proaktive Verfolgung, Untersuchung und Behebung von Leistungs- und Kapazitätsproblemen umfasst.
3. Gegebenenfalls muss der Lieferant sicherstellen, dass die Umgebungen Labor, Entwicklung, Test und Produktion physisch und/oder logisch voneinander getrennt sind.

17.29 Anforderungen an die Softwareentwicklung

Gilt für Lieferanten, die Software bereitstellen, die ausschließlich für die Nutzung durch Citi entwickelt wurde. Lieferanten müssen diese Anforderungen einhalten oder einen dokumentierten und genehmigten Softwareentwicklungslebenszyklus-Prozess („SDLC“) nachweisen, der einen gleichwertigen Ansatz mit gleicher Qualität verfolgt.

17.30 Initiierung und Planung

Der Lieferant muss den Umfang und die Ziele der Lösung in Übereinstimmung mit den Anforderungen von Citi und den vertraglichen Verpflichtungen festlegen. Dazu gehören:

1. Dokumentierung funktionaler und nicht funktionaler Anforderungen;
2. Bereitstellung von Aufwands- und Zeitschätzungen; und

3. Identifizierung aller Komponenten oder Abhängigkeiten von Drittanbietern.

Compliance-Aktivitäten, einschließlich Sicherheitsrisikobewertungen, müssen zu Projektbeginn initiiert werden. Rollen, Verantwortlichkeiten und Genehmigungsprüfpunkte müssen klar kommuniziert werden.

Alle Umgebungen müssen als Entwicklung (DEV), Prüfung (TEST) oder Produktion (PROD) klassifiziert sein und müssen während des gesamten Lebenszyklus streng getrennt bleiben. Die Umweltklassifizierung bestimmt die Zugriffsrechte und die Art der Daten, die verarbeitet werden können. Der Lieferant muss den Zugriff auf der Grundlage der Umweltklassifizierung einschränken und die Bereitstellung mit dem entsprechenden SDLC-Phasenabschluss in Einklang bringen, um unbefugten Zugriff oder die Datenoffenlegung zu verhindern.

17.31 Design

Der Lieferant muss einen Designansatz dokumentieren, der sicherstellt, dass die gelieferte Lösung alle aufgeführten Anforderungen erfüllt (einen „Testplan“). Ein Testplan muss mindestens Folgendes enthalten und beschreiben:

1. Alle vom Entwicklungsteam durchzuführenden Tests, einschließlich Unit-Tests, funktionaler und nicht funktionaler Tests sowie Leistungstests, müssen eine Rückverfolgbarkeit zu den Anforderungen aufweisen;
2. Identifizierung der genehmigenden Person(en), der/die den Abschluss bestätigen wird/werden;
3. Anforderungen an Sicherheitstests, wie Schwachstellenbewertungen und Bedrohungsmodellierung; und
4. Die Testumgebung, den Ansatz, den Prozess und den Bereitstellungspfad.

Es muss eine Freigabestrategie erstellt werden, in der die Voraussetzungen und der Prozess für die Freigabe in TEST- und PROD-Umgebungen einschließlich der Kriterien für die Freigabebereitschaft, des Inhalts und der Lieferkaden über die Projektlebensdauer dargelegt werden.

Sofern im Vertrag festgelegt, müssen Softwareverteilungen in einem von Citi genehmigten Format unter Verwendung von von Citi genehmigten Tools und Workflows bereitgestellt werden.

17.32 Testen

Tests müssen in einer kontrollierten Umgebung geplant und durchgeführt werden, um sicherzustellen, dass die Lösung definierte Anforderungen und Erfolgskriterien erfüllt. Testfälle müssen zu den Anforderungen und Code-Commits rückverfolgbar sein.

Der Lieferant sollte einen Bericht erstellen, in dem die Ergebnisse des bestandenen/nicht bestandenen Tests, zusätzliche, während der Entwicklung durchgeführte Tests und alle nicht abgeschlossenen Tests (mit Begründung) zusammengefasst sind (ein „Test-Abschlussbericht“). Fehler und zurückgestellte Funktionalitäten müssen dokumentiert werden, zusammen mit Maßnahmenplänen zur Behandlung ungelöster Probleme.

Auf Anfrage von Citi muss der Lieferant Folgendes nachweisen:

1. Einen detaillierten Testplan;
2. Einen Testabschluss und Ergebnisse, die in einem Test-Abschlussbericht aufgeführt sind; und

3. Rückverfolgbarkeit der Testergebnisse auf Anforderungen und Code-Commits.

17.33 Bereitstellung

Vor der Bereitstellung muss der Lieferant alle erforderlichen Sicherheitstests durchführen, einschließlich Schwachstellenscans und Bedrohungsmodellierung. Der Freigabeprozess muss dokumentierte Änderungsaufzeichnungen, Rollback-Strategien und erforderliche Genehmigungen umfassen. Bereitstellungspläne und eine detaillierte Anleitung zur Bereitstellung müssen Überwachungs- und Eskalationsprotokolle enthalten.

Nach der Bereitstellung muss der Lieferant die Systemkennungen abschließend festlegen und alle zugehörigen Dokumentationen und Artefakte aktualisieren, um die Auditfähigkeit sicherzustellen.

17.34 Sicherheit

1. Eine strukturierte Bewertung während der Designphase des SDLC zur Identifizierung und Behandlung potenzieller Sicherheitsrisiken, Schwachstellen und architektonischer Schwächen vor der Codeerstellung („Überprüfung des Sicherheitsdesigns“) muss Bestandteil des SDLC sein. Dabei sind präventive und detektive Kontrollen gemäß Branchenstandards wie OWASP zu berücksichtigen.
2. Sichere Codierungspraktiken müssen durchgesetzt werden.
3. Der Lieferant muss Informationssicherheitskontrollen in seine Prozesse und Verfahren für die Auswahl, Entwicklung und Implementierung von Anwendungen, Produkten und Dienstleistungen integrieren.
4. Der Lieferant muss über ein Verfahren zur sicheren Systembereitstellung für alle Systeme verfügen, auf denen Citi-Informationen gespeichert, verarbeitet und/oder übertragen werden, und muss für alle Systeme ein sicheres Systemabbild oder eine sichere Vorlage pflegen

17.35 Schutzvorkehrungen gegen Malware

Der Lieferant muss Kontrollen implementieren, um die Einschleusung von Schadcode (z. B. Viren, Würmer, Trojaner, Adware, Spyware, Ransomware oder ähnliche Cyberangriffe, bei denen Daten kompromittiert werden können) zu verhindern und zu erkennen. Der Lieferant muss:

1. Anti-Virus- und Anti-Spyware-Technologien auf allen PCs und Technologien auf allen LAN-Servern (Local Area Network), Mail-Servern und anderen Geräten, die Citi-Daten speichern, verarbeiten und/oder übertragen, implementieren, aktualisieren und warten.
2. Sicherheitseinstellungen bereitstellen, um zu verhindern, dass Endbenutzer die Antiviren-/Antimalware-Tools und geplanten Scans deaktivieren.
3. Über zentral verwaltete, automatisierte Verfahren zur Konfiguration und Aktualisierung von Antivirus- und Anti-Malware-Software verfügen.
4. Sicherstellen, dass Prozesse implementiert werden, um nicht konforme Computer mit veralteten Antiviren-Signaturen oder Scan-Engines zu identifizieren und entsprechende Maßnahmen zur Behebung einzuleiten.

5. Den Zugriff auf Kommunikationsanschlüsse/-schnittstellen, die eine Verbindung mit externen Geräten ermöglichen, einschließlich, aber nicht beschränkt auf Speichermedien, kontrollieren.

17.36 Schutzvorkehrungen gegen mobilen Code

Lieferanten müssen die Umsetzung von Kontrollen zur sicheren Verwendung mobiler Codes sicherstellen. Wo mobiler Code erlaubt ist, muss die Konfiguration mindestens sämtliche relevante Branchenstandards und vertraglichen Verpflichtungen gegenüber Citi entsprechen und der Lieferant muss sicherstellen, dass der autorisierte mobile Code entsprechend einer klar definierten und dokumentierten Sicherheitsrichtlinie arbeitet und unautorisierter mobiler Code an der Ausführung gehindert wird.

Für mobilen Code, der das zugrunde liegende Betriebssystem oder die Plattform beeinflussen kann (d. h. außerhalb der „Sandbox“ ausgeführt wird), muss der Lieferant Folgendes sicherstellen:

1. Vom Lieferanten veröffentlichter mobiler Code muss von einer von Citi zugelassenen Zertifizierungsstelle abgezeichnet und der Lebenszyklus des Zertifikats vom Lieferanten so gesteuert werden, dass es rechtzeitig erneuert oder geändert wird.
2. Signierter mobiler Code, dessen Zertifikate abgelaufen sind, muss aus der Produktionsumgebung entfernt werden.

17.37 Audit-Protokollierung

Der Lieferant muss sicherstellen, dass alle kontrollierten Informationssysteme, die für den Zugriff, die Speicherung, die Verarbeitung, die Verwaltung und/oder die Übertragung von Citi-Daten verwendet werden, Prüfpfade auf Infrastruktur- oder Anwendungsebene unterhalten, um die folgenden Punkte zu protokollieren:

1. Infrastruktursicherheitsrelevante Aktionen für die zugehörige Plattform
2. Alle Systemalarme, die von einer Firewall oder infolge eines IDS-/IPS-erzeugten Sicherheitsereignisses ausgelöst werden
3. Alle versuchten Verletzungen der Systemsicherheit (z. B. fehlgeschlagene Benutzeranmeldeversuche)
4. Unbefugte Zugriffsversuche auf Ressourcen (Software, Daten, Prozesse usw.)
5. Administratoraktionen
6. Informationen über den Erhalt bestimmter Informationen von einem Benutzer oder einem anderen System
7. Alle wichtigen Ereignisse im Zusammenhang mit Finanzgeschäftsvorgängen und Citi-Informationen, die ausdrücklich die folgenden Positionen einschließen:
 - a. Aktualisierungen von Finanzgeschäftsvorgängen
 - b. Aktualisierungen von vertraulichen oder sensiblen PII-Daten
 - c. Aktualisierung von geheimen Daten
 - d. Aktualisierungen von Authentifizierungsdaten
8. Alle eingerichteten Sitzungen

9. Sitzungsdaten, wie z. B. die eindeutige Geräte-ID, müssen, wenn technisch möglich, erfasst und für Citi-Anwendungen (d. h. Websites und mobile Anwendungen) protokolliert werden, um Betrugsuntersuchungen zu unterstützen. Diese Artefakte müssen mindestens IP-Adressen enthalten. Diese Daten müssen für Citi-Geschäftsvorgänge und Kontoeröffnungen bei Citi erfasst werden. Informationen müssen erfasst werden, damit die Sitzungsdaten mit der Transaktion oder Kontoeröffnung verknüpft werden können.
10. Prüfpfade müssen die Zuordnung bestimmter Aktivitäten zu einer bestimmten Person dokumentieren, um eine Ablehnung zu verhindern.
11. Wichtige ISA-Ereignisse (Information Security Administration) müssen speziell protokolliert werden, einschließlich der folgenden Punkte:
 - a) Benutzererstellung
 - b) Änderung der Benutzerzugriffsrechte
 - c) Streichung, Schaffung und Änderung von Profilen auf kontrollierten Informationssystemen
 - d) Passwortzurücksetzungen
 - e) Änderungen der Konfiguration der Systemsicherheit
 - f) Alle interaktiven Aktivitäten von privilegierten Funktions-IDs
 - g) Unabhängig von dem System, das das Protokoll erstellt, müssen Sicherheitsprotokolle mindestens die folgenden Informationen enthalten, es sei denn, eine solche Aufnahme ist technisch nicht möglich:
 - I. Datum und Uhrzeit des Ereignisses (Uhrzeit im UTC-Format)
 - II. Benutzer-ID der Person, die die Aktion ausführt
 - III. Ereignisart
 - IV. Betroffener Gegenstand oder betroffene Ressource
 - V. Zugriffsart (löschen, ändern usw.)
 - VI. Erfolg oder Misserfolg des Ereignisses
 - VII. Quelle (Terminal, Port, Standort, IP, Hostname usw.)

17.38 Schutz von Protokollinformationen

Der Lieferant muss die Implementierung von Zugriffskontrollen sicherstellen, um die Integrität der Prüfpfade während der Initiierung, beim Herunterfahren, während der Speicherung und bei der Übertragung zu gewährleisten.

1. Um unbefugte Änderungen an den Revisionsprotokollen zu verhindern, muss der Lieferant dafür sorgen, dass die Protokolle nicht von den Systemnutzern, deren Tätigkeit sie verfolgen, überschrieben oder verändert werden können.
2. Der Lieferant muss Citi ein Verfahren zur Aufbewahrung von Unterlagen für Protokolldaten zur Verfügung stellen, das festlegt, wie Daten aufbewahrt werden, und Compliance-Maßnahmen enthält, die auf alle anwendbaren rechtlichen und regulatorischen Anforderungen verweisen.
3. Die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder Sicherheitsdomäne müssen mit einer genauen Zeitquelle synchronisiert werden.

17.39 Überwachung der Systemnutzung

Lieferanten müssen sicherstellen, dass die folgenden Ereignisse erfasst, protokolliert und direkt oder durch einen automatisierten Überprüfungsprozess überprüft werden:

1. Alle Systemalarme, die mit einem von einer Firewall oder einem Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS) generierten Sicherheitsereignis verbunden sind.
2. Allen Aktualisierungen von kritischen Ressourcen entsprechend Ausweisung im sicheren Standardbuild.
3. Alle interaktiven Aktivitäten, die von beliebigen IDs (funktional, privilegiert, systembezogen, temporär usw.) mit Zugriff auf Informationen durchgeführt werden, die als vertrauliche personenbezogene Daten oder höher eingestuft sind.
4. Wichtige ISA-Ereignisse sind im Abschnitt „Überwachungsprotokollierung“ oben aufgeführt, mit folgender Ausnahme:
 - a) Entzug von Berechtigungen eines Benutzers, einer Rolle oder eines Profils, wenn die Aktivitäten der Informationssicherheitsverwaltung durch ein automatisiertes Workflow-/Fulfillment-System mit End-to-End-Integritätskontrollen ausgeführt werden.

17.40 Protokollkorrelation und -überprüfung

1. Wenn ein protokolliertes Ereignis eine Warnmeldung auslöst und überprüft wird, muss der Lieferant Folgemaßnahmen einleiten und eine Untersuchung veranlassen, sofern Hinweise darauf bestehen, dass ein potenziell schädlicher Informationssicherheitsvorfall aufgetreten sein könnte.
2. Der Lieferant muss sicherstellen, dass Audit-Protokolle in einem zentralen Protokollverwaltungssystem wie einem Security Information and Event Management (SIEM)-System oder einem Protokollanalyse-Tool für die Protokollkorrelationsanalyse und -überprüfung zusammengefasst werden.
3. Lieferanten müssen die Konfiguration ihres SIEM- oder Protokollanalysetools regelmäßig überprüfen und anpassen, um die Identifizierung von umsetzbaren Ereignissen zu verbessern.

17.41 Kontrolle der Betriebssoftware

Der Lieferant muss sicherstellen, dass er nur Betriebssysteme und Software verwendet, die derzeit von einem branchenweit anerkannten kommerziellen Anbieter unterstützt werden oder für die aktiv und in angemessener Weise Patches und Konfigurationsaktualisierungen zur Behebung von Sicherheitsproblemen bereitgestellt werden.

Der Lieferant muss die Umsetzung eines dokumentierten Prozesses sicherstellen, der den Zeitplan der Abhilfemaßnahmen festlegt, innerhalb dessen alle genehmigten Sicherheitspatches und Konfigurationen angewendet werden müssen.

Unabhängig von bestehenden separaten Wartungsvereinbarungen zwischen dem Lieferanten und Citi muss der Lieferant sicherstellen, dass Software, die für Citi entwickelt wurde und einer Lizenzvereinbarung unterliegt, keine Verwendung nicht unterstützter Versionen mit bekannten Schwachstellen erlaubt und dass diese Software bei Bedarf zeitnah aktualisiert und mit Sicherheits-Patches versehen wird.

Anwendungssoftware zur Verarbeitung von Citi-Informationen muss von etablierten Anbietern erworben und lizenziert, katalogisiert und unterstützt werden.

17.42 Schwachstellen- und Bedrohungsmanagement

1. Der Lieferant muss einen Prozess für das Management von Schwachstellen und Bedrohungen implementieren, der alle folgenden Punkte umfassend berücksichtigt und/oder beinhaltet:
 - a. Tools und Verfahren zur Entdeckung und Verwaltung von Schwachstellen in allen Informationsressourcen, die zur Verarbeitung, Speicherung, zum Zugriff oder zur Übertragung von vertraulichen oder sensibleren Daten von Citi verwendet werden können.
 - b. Es muss sichergestellt werden, dass Schwachstellenscans mindestens wöchentlich unter Verwendung branchenweit anerkannter Schwachstellen-Analysetools und Berichtsmethoden durchgeführt werden.
 - c. Einstufung der Schwachstellen gemäß der aktuellen Version des „Common Vulnerability Scoring System (CVSS)“ (siehe <https://www.first.org/cvss>) mit Zeitplänen für die Behebung entsprechend dem Schweregrad.
 - d. Eine Anforderung zur Prüfung von Schwachstellenbehebungen vor der vollständigen Bereitstellung in der Produktionsumgebung.
 - e. Ein dokumentierter und wiederholbarer Betriebsablauf zur Beschleunigung der Behebung kritischer Schwachstellen.
 - f. Der Lieferant muss Informationsressourcen während ihres unterstützten Lebenszyklus nachverfolgen, um sich auf den End-of-Life-Status (EOL) oder den Status „End of Vendor Support“ (EOVS) vorzubereiten, und über Prozesse verfügen, um solche Assets proaktiv zu aktualisieren oder zu ersetzen.
 - g. Alle kritischen Schwachstellen gemäß CVSS, die durch Informationsbeschaffung, Schwachstellenscans oder Penetrationstests identifiziert werden, müssen priorisiert und innerhalb eines klar definierten Zeitrahmens behoben werden, der dem Schwachstellenrisiko angemessen ist.

17.43 Von Drittanbietern gehostete Anwendungen

Wenn der Lieferant vertrauliche oder sensiblere Daten von Citi auf einer Website oder einem über das Internet zugänglichen System oder einer Website mit der Marke Citi unterhält oder speichert, muss der Lieferant zum Schutz vor einer Schwachstelle oder Bedrohung, die Produkte oder Dienstleistungen von Citi betrifft (jeweils eine „Schwachstelle“), die folgenden Anforderungen erfüllen:

1. Der Lieferant muss einen Mitarbeiter als Ansprechpartner für Anfragen von Citi im Bereich der Informationssicherheit benennen.
2. Nutzung branchenweit anerkannter Best Practices, um mindestens einmal pro Woche seriöse Quellen für Informationen zu Sicherheitslücken in

Computersystemen zu überwachen, darunter FIRST, CERT/CC, CISA Known Exploited Vulnerabilities Catalog und Mailinglisten von Anbietern, und Ergreifen geeigneter Maßnahmen, um relevante Service Packs, Patches, Upgrades und Workarounds zu beschaffen, gründlich zu testen, anzuwenden und Citi zur Verfügung zu stellen.

3. Mindestens vierteljährlich die Umsetzung seiner Informationssicherheitsmaßnahmen mithilfe von Tools zum Scannen von Netzwerk-, System- und Anwendungsschwachstellen und/oder Penetrationstests zu überprüfen.
4. Der Lieferant muss Citi oder einem von Citi autorisierten Dritten gestatten, in angemessenen Zeitabständen Schwachstellenbewertungen, ethische Hacking-Tests oder andere Sicherheitsbewertungen durchzuführen, um die Einhaltung der vertraglichen Verpflichtungen des Lieferanten und dieser Anforderungen zu überprüfen. Dies umfasst unter anderem die Überprüfung von Richtlinien, Prozessen und Verfahren, Vor-Ort-Bewertungen der physischen Sicherheitsvorkehrungen, Schwachstellenscans von Netzwerken, Systemen und Anwendungen sowie Penetrationstests unter Verwendung kommerziell verfügbarer Tools und/oder branchenüblicher Verfahren zur Durchführung dieser Prüfungen.
5. Jeder Auftragnehmer, der für den Lieferanten Dienste zur Schwachstellenbewertung bereitstellt, muss auf der von Citi genehmigten Liste der Anbieter von Schwachstellenbewertungen stehen. Wenn der Lieferant Auftragnehmer oder Subunternehmer einsetzt, um die Dienstleistungen zu erbringen, muss der Lieferant auf eigene Kosten sicherstellen, dass alle gemäß diesen Anforderungen erforderlichen Schwachstellenbewertungen so rechtzeitig abgeschlossen werden, als ob der Lieferant diese Dienstleistungen direkt erbringen würde, und er muss sicherstellen, dass die Anforderung an Auftragnehmer oder Subunternehmer, solche Bewertungen zu ermöglichen, in der Vereinbarung zwischen dem Lieferanten und dem Auftragnehmer/Subunternehmer in Bezug auf die Dienstleistung festgehalten wird, einschließlich einer Formulierung, die Citi ermächtigt, solche Bewertungen durchzuführen.
6. **Benachrichtigung.**
 - a) Identifiziert der Lieferant eine Schwachstelle in einem Produkt oder einer Dienstleistung, die Citi betrifft, muss er Citi innerhalb von 24 Stunden nach ihrer Identifizierung schriftlich informieren und die vom Lieferanten ergriffenen Abhilfemaßnahmen beschreiben.
 - b) Erlangt der Lieferant im Anschluss an eine verantwortungsvolle öffentliche Offenlegung über etablierte Offenlegungsverfahren (z. B. durch die Veröffentlichung einer Schwachstelle in der National Vulnerability Database (NVD) oder über einen Bedrohungskatalog, der externen Sicherheitsanbietern zur Verfügung gestellt wird) Kenntnis von einer Schwachstelle in einem Produkt oder einer Dienstleistung, die Citi betrifft, muss er Citi innerhalb von 24 Stunden nach dieser Veröffentlichung schriftlich benachrichtigen. Jede

Benachrichtigung muss Informationen über die Schwachstelle, die Bedeutung des betroffenen Systems für die von Citi bezogenen Dienstleistungen (d. h. ob es Citi-Informationen hostet oder für die Bereitstellung von Dienstleistungen oder für beides genutzt wird), darüber, ob die Schwachstelle aus der Ferne ausgenutzt werden kann, sowie den CVE-Score (Common Vulnerabilities and Exposures) enthalten. Der Lieferant wird Citi weiterhin Updates bereitstellen, bis die Sicherheitslücke behoben ist. In Fällen, in denen Citi eine Schwachstelle identifiziert, kann Citi den Lieferanten davon in Kenntnis setzen, und der Lieferant muss die Schwachstelle in Übereinstimmung mit diesem Abschnitt unverzüglich beheben.

7. **Abhilfe.** Für jede in diesem Abschnitt gemeldete Schwachstelle bewertet die meldende Partei den Risikograd und die Auswirkungen dieser Schwachstelle auf der Grundlage der Schwere und des Risikos für Citi und weist ihr eine Risikoprioritätsstufe gemäß dem Common Vulnerability Scoring System (CVSS) zu, wie in Anhang A dargelegt (siehe <https://www.first.org/cvss>). Sobald ein Risikograd zugewiesen und von den Parteien vereinbart wurde, behebt der Lieferant alle identifizierten mittleren, hohen oder kritischen Schwachstellen. Wenn möglich, wird die Behebung einer solchen Schwachstelle in einem Sicherheitspaket für die aktuell eingesetzte Version zur Verfügung gestellt.

Wenn der Lieferant nicht in der Lage oder nicht bereit ist, die Sicherheitslücke zur Zufriedenheit von Citi zu beheben, kann Citi die entsprechende Lizenz ohne weitere Haftung oder finanzielle Verpflichtungen (für den gekündigten Teil) kündigen, und der Lieferant hat Citi unverzüglich den anteiligen Teil der gezahlten Lizenzgebühren zurückzuerstatten.

17.44 Kontrollen des Kommunikationssicherheitsnetzwerks

1. Lieferantennetzwerke, die verwendet werden, um auf Citi-Informationen zuzugreifen, sie zu speichern, zu verwalten, zu verarbeiten und/oder zu übermitteln, müssen vor Bedrohungen geschützt werden, und die Sicherheit der Informationssysteme, die die Durchsetzungspunkte im Netzwerk nutzen, muss gewährleistet sein.

- a. Informationen mit einer Citi-Informationsklassifizierung von „Vertraulich“ oder höher dürfen nicht dauerhaft auf einem System gespeichert sein, das sich in einer zum Internet offenen „demilitarisierten Zone (DMZ)“ befindet. Netzwerke, die zum Zugreifen auf, Speichern, Verwalten, Verarbeiten und/oder Übertragen von Citi-Informationen unter Verwendung von Wireless Local Area Networks (WLANs) oder anderen drahtlosen Gerätelösungen verwendet werden, die angemessene Kontrollen zum Verhindern unbefugten Zugriffs (PEAP-TLS, EAP-TTLS usw.) beinhalten, können mit Netzwerken verbunden sein, die Citi-Informationen enthalten.
 - b. Alle externen IP-Verbindungen zum weltweiten Netzwerk des Lieferanten sind von einer vom Lieferant verwalteten Firewall geschützt.
 - c. Ein Echtzeit-Intrusion-Detection-System (IDS) und ein Intrusion-Prevention-System (IPS) überwachen und schützen Internetverbindungen zum Netzwerk des Lieferanten, über die auf Citi-Informationen zugegriffen wird, die verwaltet, gespeichert, verarbeitet oder übertragen werden.
2. Für alle Internetanwendungen der Marke Citi muss der Lieferant Folgendes sicherstellen:
- a. Die auf den Websites der Lieferanten gehosteten Dienste werden durch von Citi genehmigte Anti-DDoS-Dienste (Distributed Denial of Service) oder vergleichbare, von Citi validierte Kontrollen geschützt.
 - b. Externe Firewalls müssen mit einer Deny-by-Standard-Regel konfiguriert werden. Firewall-Regeln müssen nach dem Prinzip der geringsten Rechte konfiguriert werden, und alle Verbindungsversuche, die von der Firewall abgelehnt werden (z. B. das Verwerfen von Paketen), müssen protokolliert werden.
 - c. Der Netzwerkverkehr sollte standardmäßig blockiert und nur in Ausnahmefällen an verwalteten Schnittstellen zugelassen werden. Die Ausnahmen müssen streng auf bestimmte Quellen, Ziele und Dienste beschränkt sein.
 - d. Der Datenverkehr von Webanwendungen sollte angemessen kontrolliert und gefiltert werden, z. B. über Web Application Firewalls.

17.45 Trennung in Netzwerken

Der Lieferant muss sicherstellen, dass alle Informationssysteme und Anwendungen, die für den Zugriff, die Speicherung, die Verarbeitung, die Verwaltung und/oder die Übertragung von Citi-Informationen verwendet werden und über das Internet zugänglich sind, nur über die entmilitarisierte Zone (DMZ) des Lieferanten zugänglich sind.

Im Notfall muss der Lieferant in der Lage sein, den Zugang zwischen Teilen seines Netzwerkes zu filtern, um die Folgen von Einschränkungen der Netzwerksicherheit zu verringern (z. B. Portfilterung während eines Virusausbruchs).

Für den Fernzugriff und die Host-Sicherheit müssen gruppenbasierte Zugriffskontrollen (z. B. für Mitarbeiter oder Subunternehmer) implementiert werden, um den Zugriff auf Netzwerkressourcen im Netzwerk des Lieferanten zu beschränken. Auf der Host-Ebene kann die Zugangskontrolle auf Gruppen- oder Individualebene erfolgen.

17.46 Geräteidentifikation in Netzwerken

Technologieplattformen müssen andere Technologieplattformen entsprechend dem Informationssicherheitsrisiko der jeweiligen Interaktion und unter Berücksichtigung weiterer risikomindernder Kontrollen identifizieren und authentifizieren.

1. Nur Geräte des Lieferanten (d. h. Hardware, einschließlich, aber nicht beschränkt auf Desktops und Laptops), die diese Anforderungen erfüllen und vom Lieferanten autorisiert sind, dürfen auf das Lieferantennetzwerk zugreifen, in dem Citi-Informationen gespeichert, verarbeitet oder übertragen werden.
2. Nur Geräte des Lieferanten (d. h. Hardware, einschließlich, aber nicht beschränkt auf Desktops, Laptops und entfernbare Datenspeichermedien), die diese Anforderungen erfüllen und von Citi autorisiert sind, dürfen auf das Citi-Netzwerk zugreifen.

17.47 Analyse und Spezifikation der Sicherheitsanforderungen

Der Lieferant muss Informationssicherheitsverfahren in seine Prozesse und Verfahren für die Auswahl, Entwicklung und Implementierung von Anwendungen, Produkten und Dienstleistungen integrieren.

17.48 Online-Geschäftsvorgänge

1. Wo dies geboten ist, muss der Lieferant über Informationssysteme verfügen, die dynamische Passwörter oder digitale Zertifikate zur Validierung von Anmeldedaten verwenden.
2. Alle Endgerätezertifikate müssen mindestens alle 13 Monate ersetzt werden.
3. Anwendungen von Lieferanten, die Citi-Informationen speichern, verarbeiten, verwalten oder auf Citi-Informationen zugreifen, Internet-Anwendungen mit Citi-Markenzeichen hosten oder Verbindung zu Citis Netzwerkressourcen haben, müssen:
 - a. Eine Authentifizierungsmethode nutzen, die auf den Arten der Daten/Funktionen basiert, auf die zugegriffen wird;
 - b. Eine Bewertung der Konformität mit der Multifaktor-Authentifizierung (MFA) durchführen und bei Bedarf Empfehlungen umsetzen;
 - c. Eine Onboarding-Bewertung zum Suspicious Activity Monitoring (SAM) durchführen und bei Bedarf Empfehlungen umsetzen;
 - d. In all diesen Fällen sollte sich der Lieferant an seinen Hauptansprechpartner wenden, um die aktuellen Anforderungen von Citi zu erfahren.

17.49 Verfahrensschritte zur Änderungsüberwachung

1. Der Lieferant muss sicherstellen, dass Konfigurationsänderungen an Firewalls, Eindringungserkennungssystemen (IDS) und Eindringungsverhinderungssystemen (IPS) durch den Änderungsmanagementprozess des Lieferanten geleitet werden.

2. Zugang zur Produktion über befristete Kennungen ist zu protokollieren und auf an der Umgebung vorgenommene Änderungen hin zu überwachen.
3. Für kontrollierte Informationssysteme, die Kundeninformationen mit einer Citi-Klassifizierung „Vertraulich“ oder höher oder einem IS-Risikokomponentenwert für „Integrität“ oder „Verfügbarkeit“ von „Hoch“ enthalten, müssen die gemäß Abschnitt 17.32 (Audit-Protokollierung) erfassten Protokolle vom Lieferanten überprüft werden. Solche Überprüfungen können auf einer geeigneten risikobasierten Stichprobenmethode beruhen.
4. Die Überprüfung muss Änderungen validieren, die Teil des vorübergehenden privilegierten Zugangs sind und wie beabsichtigt vorgenommen wurden.
5. Der Lieferant muss sämtliche Änderungen dokumentieren und Nachweise über den Überprüfungsprozess aufbewahren.

17.50 Datenlecks

Der Lieferant muss über einen dokumentierten Standard für sichere Codierung verfügen, der Datenlecks verhindert, darunter:

1. Detaillierte Systeminformationen (z. B. Serverart und -technik).
2. Stapelzurückverfolgung und Ausnahmefehler, die die Verzeichnisbaumstruktur und die Art der zugrunde liegenden Datenbank zeigen.

17.51 Testdaten

Vertrauliche oder höher eingestufte Informationen gemäß der Definition von Citi dürfen vom Lieferanten nicht in Softwareanwendungsentwicklungs- oder -testumgebungen oder Labors verwendet oder gespeichert werden, es sei denn, diese Informationen werden mithilfe von Tools und Methoden, die den Branchenstandards entsprechen, anonymisiert, maskiert und/oder verschleiert, sodass diese Daten nicht mehr sensibel sind, oder der Lieferant muss Live-Produktionskontrollen innerhalb der Entwicklungs- oder Testumgebungen implementieren.

17.52 Systemabnahme

Lieferanten müssen über dokumentierte Verfahren zum Management des Projektumfangs und zur Systemabnahme verfügen, die die einschlägigen Branchenstandards erfüllen.

17.53 Melden von Schwachstellen in der Informationssicherheit

Der Lieferant muss über einen Prozess verfügen, um sicherzustellen, dass Schwachstellen in Anwendungen und Infrastrukturen, die zu einer Kompromittierung von Citi-Informationswerten führen, unverzüglich an Citi gemeldet werden.

17.54 Verantwortlichkeiten und Verfahren bei Sicherheitsvorfällen

1. Ein SIRT ist ein Sicherheitsereignis, das einen der folgenden Punkte beeinträchtigt, unabhängig davon, wie oder wo der Sicherheitsvorfall aufgetreten ist oder wer den Vorfall verursacht haben könnte:

- Die Vertraulichkeit, Integrität oder Verfügbarkeit von Citi-Daten.
 - Die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten (einschließlich personenbezogener Daten), für die Citi vertraglichen, rechtlichen oder behördlichen Verpflichtungen unterliegt.
 - Die Integrität oder Verfügbarkeit von Citi-Informationssystemen, die Citi-Daten speichern, verarbeiten oder übertragen.
2. Für unsere Zwecke bezieht sich eine Beeinträchtigung der Vertraulichkeit auf die Gefährdung von Daten durch eine unbefugte Person oder durch Szenarien, in denen Citi die Aufsicht und Kontrolle über die Daten verliert. Alle Sicherheitsvorfälle sind unverzüglich zu melden.
 3. Wenn der Lieferant einen SIRT-Vorfall erlebt, muss der Lieferant mit Citi zusammenarbeiten, indem er die von Citi im Rahmen der eigenen Prozesse zur Reaktion auf Vorfälle angeforderten Informationen bereitstellt und kompromittierte Daten in einer Weise analysiert, die es Citi ermöglicht, gesetzliche, regulatorische und/oder interne Governance-Anforderungen zu erfüllen. Der Lieferant muss ferner alle nach Gesetzen, Vorschriften oder regulatorischen Anforderungen erforderlichen oder von Citi nach eigenem Ermessen gewünschten Benachrichtigungen auf Anfrage von Citi und auf Kosten des Lieferanten vornehmen, und zwar erst, nachdem Citi die Möglichkeit hatte, die vorgeschlagene Formulierung der Benachrichtigungsvorlagen zu prüfen und zu ändern. Der Lieferant darf Citi in solchen Benachrichtigungen nicht nennen, es sei denn, Citi fordert ausdrücklich schriftlich die Nennung von Citi.

17.55 Schutz vor Datenlecks (DLP)

Der Lieferant muss Kontrollen zur Verhinderung von Datenverlust (DLP) implementieren, einschließlich der Überwachung von Inhalten und Endpunkten, die alle Mitarbeiter mit Zugriff auf Daten von Citi mit der Klassifizierung „Vertraulich“ oder höher abdeckt.

Der Lieferant muss über Kontrollen verfügen, um Fälle zu erkennen und zu verhindern, in denen Daten von Citi mit der Klassifizierung „Vertraulich“ oder höher über die folgenden Kanäle aus ihrem Netzwerk verschoben werden:

- a. Unverschlüsselte E-Mails
- b. Verschlüsselte E-Mail-Anhänge
- c. Ausdrucken von Citi-Daten
- d. Übertragungen von Citi-Daten an Orte außerhalb ihres Netzwerks (zum Beispiel über FTP)
- e. Versuche, vertrauliche oder höherwertige Daten von Citi auf Wechselmedien wie USB-Laufwerke, Wechselfestplatten, CD/DVD-Laufwerke und andere Wechselmedien mit Datenspeicherfunktion zu kopieren. Dieses Privileg sollte standardmäßig verhindert werden.
- f. Die DLP-Lösung muss alle Ereignisse protokollieren und den Lieferanten alarmieren, die Versuche darstellen (ob erfolgreich oder

blockiert), Daten von Citi mit der Klassifizierung „Vertraulich“ oder höher aus ihrem Netzwerk zu anderen Zielen zu verschieben, zu transportieren oder zu kopieren. Dieses Privileg sollte standardmäßig verhindert werden.

- g. Hochladen von Citi-Daten auf externe Websites, einschließlich SaaS-/Filesharing-Sites. Dieses Privileg sollte standardmäßig verhindert werden.

17.56 Nutzung des Internets

1. Der Lieferant muss über Web-Zugangskontrollen verfügen, um zu verhindern, dass Informationen von Citi mit der Klassifizierung „Vertraulich“ oder höher weitergegeben werden und die Mitarbeiter, die Zugang zu Citi-Daten haben, Malware oder Angriffen ausgesetzt werden.
2. Für Lieferanten, die Zugang zu Daten von Citi mit der Klassifizierung „Vertraulich“ oder höher haben:
 - a. Alle URL-Anfragen müssen protokolliert werden.
 - b. Versuche, auf Websites zuzugreifen, die für die unbefugte Weitergabe von Citi-Daten verwendet werden können (d. h. Webmail, Chat, soziale Medien, Online-Speicher, Gen-AI usw.) müssen gesperrt werden.
 - c. Der Zugang zu Websites, die die Umgebung für Malware oder Angriffe anfällig machen könnten, muss gesperrt werden.
 - d. Versuche, auf Seiten zuzugreifen, die als nicht geschäftsbezogen gelten, müssen gesperrt werden.
 - e. Der Lieferant muss einen regelmäßig aktualisierten URL-Kategorisierungsdienst abonnieren; alle nicht kategorisierten URLs müssen standardmäßig gesperrt werden, oder alle URLs müssen standardmäßig gesperrt und von Fall zu Fall genehmigt werden.
 - f. Die vom Lieferanten verwendeten Webbrowser müssen vollständig unterstützt werden und über die neuesten Sicherheitsupdates des Softwareanbieters verfügen.

17.57 Elektronische Nachrichtenübermittlung

Instant-Messaging-Dienste, Peer-to-Peer-Netzwerke oder andere Internet-basierte Kollaborationstools dürfen nicht zur Übertragung oder Speicherung von Citi-Informationen außerhalb des Lieferantennetzwerks oder aus Netzwerken mit Citi-Informationen verwendet werden, sofern nicht für sämtliche Citi-Daten eine angemessene Verschlüsselung gemäß Abschnitt 17.9 („Richtlinie zur Verwendung kryptografischer Kontrollen“) vorhanden ist.

17.58 E-Mail

Der Lieferant muss über E-Mail-Kontrollen verfügen, um die Weitergabe von Citi-Informationen und die Gefährdung durch Malware oder Angriffe zu verhindern. Dazu gehören:

1. Eingehende Dateianhänge, die das E-Mail-Gateway erreichen, werden gescannt und blockiert, wenn sie ein Risiko für das System darstellen.
2. Die Software für die E-Mail-Filterung (Anti-Spam, Anti-Phishing) ist in Gebrauch und auf dem neuesten Stand.

3. Alle Citi-Daten der Klassifizierung „Vertraulich“ oder höher müssen verschlüsselt werden, wenn sie außerhalb der Organisation des Lieferanten versendet werden.
4. E-Mail-Clients, die vom Lieferanten verwendet werden, werden vollständig unterstützt und verfügen über die neuesten Sicherheitsupdates des Softwareherstellers.

17.59 Wechseldatenträger

1. Der Lieferant muss Citi-Informationen schützen, unabhängig davon, auf welchem Medium sie gespeichert sind. Dieser Standard gilt unter anderem für die folgenden Arten von Medien, auf denen Informationen gespeichert sind: Karte, Kassette, Compact Disk (CD), Scheckvorrat, Diskette oder ein anderes entfernbares Speichergerät, Hardcopy-Ausgabe, Magnetplatte, Magnetband, Mikrofilm, Mikrofiche, optische Platte oder Papierdokument.
2. Die Voreinstellung für den Zugriff auf tragbare Medien/Speichergeräte auf den Systemen, auf denen Citi-Informationen gespeichert werden, muss „Kein Zugriff“ lauten. Wenn Ausnahmen gewährt und somit Schreib-Lese-Zugriff erlaubt wird, müssen die Daten auf dem tragbaren Mediengerät verschlüsselt werden.
3. Wenn die Verwendung von Wechseldatenträgern erlaubt ist, muss es für diese Verwendung einen Genehmigungsprozess der Geschäftsleitung geben, der auch die geschäftlichen Gründe für die Verwendung von Wechseldatenträgern enthält. Wechseldatenträger müssen von der Geschäftsleitung inventarisiert werden. Wechseldatenträger, die Daten von Citi mit der Klassifizierung „Vertraulich“ oder höher enthalten, müssen automatisch verschlüsselt werden, ohne dass eine Aktion des Benutzers erforderlich ist.

17.60 Medienentsorgung

1. Sind Citi-Informationen mit der Einstufung „vertraulich“ oder höher gemäß den Anweisungen von Citi zur Entsorgung freigegeben (d. h. zu dem Zeitpunkt, zu dem die Informationen für Citi nicht mehr erforderlich oder nützlich sind und alle zusätzlichen Aufbewahrungsfristen gemäß Gesetzen, Vorschriften und/oder Citi-Richtlinien abgelaufen sind), muss der Lieferant diese Informationen so vernichten, dass sie unbrauchbar und nicht wiederherstellbar sind.
2. Zum sicheren Löschen von anschließbaren Medien muss ein zugelassenes Tool verwendet werden, das die Sektoren des Laufwerks nach dem Zufallsprinzip mit bestimmten, unterschiedlichen Zeichen überschreibt, wobei die folgenden Regeln zu beachten sind:
 - a. Bei Datenträgern, auf denen Informationen gespeichert sind, die als vertraulich oder höher eingestuft sind, muss das Tool drei Durchläufe des Datenträgers durchführen.
 - b. Das Medium entmagnetisieren (falls zutreffend).

3. Das Medium physisch zerstören, um es unlesbar zu machen (d. h. Schreddern, Zerstören der Laufwerke).
4. Papier und andere nicht-elektronische Speichermedien, die Informationen mit der Klassifizierung „Vertraulich“ oder höher enthalten, müssen sicher gesammelt und vor der endgültigen Entsorgung in einem sicheren „Behälter für vertrauliche Unterlagen“ aufbewahrt werden. Behälter für vertrauliche Unterlagen müssen immer verschlossen und nur von autorisiertem Personal zu öffnen sein.
 - a. Kopierer, Drucker, Faxgeräte sowie alle anderen Geräte mit Speicher- oder Speichermedien, die vertrauliche Citi-Informationen oder höher eingestufte Informationen enthalten können, müssen ebenfalls einer sicheren Datenbereinigung unterzogen werden.

17.61 Management und Schulung zur Informationssicherheit

1. Ein angemessenes Programm zur Sensibilisierung und Schulung im Bereich Cyber-/Informationssicherheit muss aufrechterhalten werden, das unter anderem die Prävention von Phishing- und anderen Social-Engineering-Angriffen, den angemessenen Umgang mit vertraulichen oder höher klassifizierten Informationen sowie die Meldung von Sicherheitsvorfällen und das Management der Reaktion darauf umfasst.
2. Der Lieferant muss sicherstellen, dass alle Mitarbeiter, einschließlich Auftragnehmer und Zeitarbeitskräfte, angemessene Sensibilisierungsmaßnahmen sowie Schulungen zu den für ihre jeweiligen Aufgaben relevanten Organisationsrichtlinien und -verfahren erhalten.
3. Der Lieferant muss sicherstellen, dass das Schulungs- und Sensibilisierungsprogramm jährlich überprüft und aktualisiert wird, um neu auftretende Risiken und Bedrohungen, aktuelle Best Practices und neue Technologien im Bereich Cybersicherheit zu berücksichtigen.
4. Mindestens die folgenden Themen müssen enthalten sein:
 - b. Beschriftung und Handhabung von Informationen
 - c. Sichere Übertragung (sichere E-Mail, sicherer SharePoint-Speicher, kein Senden von Citi-eigenen Daten an persönliche E-Mails)
 - d. Meldung von Informationssicherheitsvorfällen
 - e. Sicherer Arbeitsplatz (z. B. angemessene Internetnutzung, nicht autorisierte Software, Verbot des Herunterladens nicht genehmigter Software)
 - f. Passwortverwaltung (z. B. starke Passwörter, Verbot der Weitergabe von Passwörtern)
 - g. Social Engineering (z. B. Phishing, Spear Fishing, Vishing, SMiShing)
 - h. Fernarbeit (z. B. sichere Verbindung, persönliche Gerätesicherheit)
5. Mitarbeiter von Lieferanten müssen die Schulung bei oder vor Erhalt des Zugriffs auf Systeme, auf denen Citi-Daten gespeichert sind, zugewiesen bekommen und die Schulung bis zum in der Zuweisungsmitteilung angegebenen Termin absolvieren.
 - a. Allen Mitarbeitern sollte mindestens einmal jährlich eine IS-Schulung angeboten werden, sofern dies gesetzlich zulässig ist.
6. Die Schulung sollte ein Mittel zur Erfassung der Wirksamkeit enthalten (z. B. einen Abschlusstest mit einem definierten Bestehens-/Nichtbestehensgrenzwert), sofern dies durch lokale Gesetze zulässig ist.

17.62 Programm zum Umgang mit Cyberrisiken

Der Lieferant muss außerdem mindestens ein angemessenes Cyber-Risikomanagementprogramm unterhalten, das mindestens Folgendes umfasst:

1. Ein gut definiertes, dokumentiertes Risikomanagementprogramm für die Informationssicherheit und/oder ein betriebliches Risikomanagementprogramm mit einer klar definierten Komponente für das Management von Cyber-/Informationsrisiken, das die Risikobereitschaft des Lieferanten für Cyberrisiken festlegt und sicherstellt, dass sein Cyberrisiko mit dieser Risikobereitschaft übereinstimmt.

2. Aufrechterhaltung eines soliden Programms zur Steuerung des Sicherheitsrisikomanagements, das u.a. die Erfassung und/oder Durchführung von Sicherheitsaudits und -prüfungen umfasst, die den Gesamtzustand der Sicherheit innerhalb des Unternehmens bewerten und mindestens einmal jährlich an die Unternehmensleitung berichten, um zu überprüfen und sicherzustellen, dass die Risikobereitschaft des Lieferanten in Bezug auf Cyberrisiken nicht verletzt wurde.
3. Der Lieferant muss die Einhaltung aller für ihn geltenden PCI-Datensicherheitsstandards (PCI-DSS) sicherstellen, wenn der Lieferant Kredit-/Debitkartentransaktionen, Zahlungen und/oder entsprechende Informationen verarbeitet, speichert und/oder überträgt.
4. Einhaltung eines Krisenmanagementplans und eines Leitfadens sowie eines Plans für das Reaktionsteam bei Sicherheitsvorfällen gemäß den Branchenstandards, um sicherzustellen, dass der Lieferant über ausreichende und angemessene Fähigkeiten verfügt, um versuchte, vermutete und/oder tatsächliche Cybersicherheitsvorfälle zu erkennen, einzudämmen, zu untersuchen, darauf zu reagieren und sich davon zu erholen.

17.63 Anwendungs-, API-, Code-, System- und Infrastruktursicherheit

Wenn der Lieferant eine oder mehrere Softwareanwendungen hostet, entwickelt, mitentwickelt, Entwicklungsumgebungen bereitstellt und/oder liefert, führt der Lieferant Codeüberprüfungen dieser Software und/oder Patches für die Software auf Sicherheitsmängel, die Verhinderung des unbefugten Zugriffs, der Modifizierung und/oder des Einfügens von Malware oder anderen Formen von böartigem Code sowie Schwachstellentests durch, um sicherzustellen, dass die Anwendung (einschließlich APIs) zusammen mit den zugrunde liegenden Systemdiensten, Betriebssystemen und Netzwerken frei von bekannten Schwachstellen und Defekten sind, die zu einem Sicherheitsvorfall, einer Verletzung des Datenschutzes, Betrug, einem unbefugten Zugriff und/oder einer Offenlegung vertraulicher Informationen, einem Verlust der Integrität der von der/den Anwendung(en) verarbeiteten, gespeicherten oder übertragenen Informationen und/oder einem Verlust der Verfügbarkeit führen könnten, die die Qualität der Produkte und/oder Dienstleistungen beeinträchtigen könnte, die der Lieferant Citi bereitstellt.

17.64 Mobile Sicherheit

Wenn der Lieferant eine mobile Anwendungslösung bereitstellt, muss er die folgenden Anforderungen erfüllen:

1. Die mobile Anwendung darf nur allgemein verfügbare (GA), stabile und nicht am Ende ihres Lebenszyklus ² (Non-EOL) befindliche Versionen der Plattformen Google Android (ausgenommen Android Go) und/oder Apple iOS/iPadOS unterstützen. Wenn die mobile Lösung mit Unterstützung für

² Produktversionen, die aktiv unterstützt werden und regelmäßig Sicherheits- und Wartungsupdates vom Plattformbetreiber oder Lieferanten erhalten.

weitere Betriebssysteme ausgestattet ist, müssen die unterstützten Betriebssysteme/Versionen von Citi konfigurierbar sein.

2. Die mobile Lösung sollte keine mobilen Plattformen/Geräte unterstützen, die nicht mit regulären Befehlssätzen zur Unterstützung kryptografischer Algorithmen ausgestattet sind, einschließlich, aber nicht beschränkt auf, Verschlüsselung gemäß Abschnitt 17.9 (Verschlüsselungsanforderungen) dieses Dokuments.
3. Vorproduktionsversionen des Betriebssystems, einschließlich, aber nicht beschränkt auf Beta-, Early-Access- und Feature-Preview-Versionen/-Releases, sind in der Produktionsumgebung nicht zulässig.
4. Der Lieferant muss in der Lage sein, eine Liste der integrierten Komponenten von Drittanbietern bereitzustellen, einschließlich, aber nicht beschränkt auf kostenlose und Open-Source-Softwarebibliotheken, die in der mobilen Lösung gebündelt/genutzt werden.
5. Die mobile Anwendung muss den Anforderungen und Best Practices entsprechen, die die Veröffentlichung mobiler Anwendungen über öffentliche App Stores wie den Apple App Store oder Google Play Store ermöglichen. Die aufgeführten öffentlichen App-Stores sind die bevorzugte und primäre Methode zur Verbreitung/Veröffentlichung der mobilen Anwendung.
6. Mobile Android-Anwendungen müssen das APK-Signaturschema v2+ nutzen. Das APK-Signaturschema Version 1 (auch bekannt als JAR-Signatur) darf nicht verwendet werden.
7. Der Typ und die Länge des Signaturschlüssels für die mobile Anwendung müssen dem Abschnitt 17.9 – **Verschlüsselungsanforderungen** dieses Dokuments entsprechen.
8. Jeder Anwendungssignaturschlüssel und das zugehörige X.509v3-Zertifikat müssen einzeln verwaltet und einer einzigen Anwendungs-ID/Bundle-ID zugeordnet werden. Signaturschlüssel dürfen nicht von mehreren Anwendungen gemeinsam genutzt werden.
9. Sofern eine mobile Anwendung die Aufbewahrung von Daten auf dem mobilen Gerät erfordert, dürfen auf dem Gerät nur die aktuellsten Daten gespeichert werden, die für den Zweck bzw. die Zwecke der Anwendung/des Dienstes erforderlich sind, oder nur so lange, wie dies aufgrund gesetzlicher oder regulatorischer Anforderungen vorgeschrieben ist.
 - a. Die Erhebung, Verarbeitung und/oder Speicherung von Benutzerdaten muss den lokalen Gesetzen entsprechen, darunter insbesondere Datenschutzbestimmungen wie die Datenschutz-Grundverordnung (DSGVO) und die Richtlinie 2002/58/EG (ePrivacy) oder deren regionale Entsprechungen.
 - b. Eingebundene Drittkomponenten (z. B. Bibliotheken) dürfen keine Benutzerdaten erheben, verarbeiten und/oder speichern.
10. Mobile Anwendungen dürfen keine Anwendungsdaten weltweit zugänglich machen.
 - a. Wenn eine gemeinsame Nutzung von Daten mit anderen Anwendungen erforderlich ist, müssen die Anwendungen für die jeweiligen Betriebssysteme wirtschaftlich angemessene Techniken,

Methoden und Kontrollen einsetzen, um nur die erforderliche Datenmenge mit einer minimalen Anzahl anderer Anwendungen zu teilen, sofern eine solche gemeinsame Nutzung ordnungsgemäß gerechtfertigt und dokumentiert ist.

11. Mobile Anwendungen müssen sich ausschließlich auf die sicheren Kommunikationsmöglichkeiten verlassen, die von den jeweiligen mobilen Betriebssystemen bereitgestellt werden. Zum Beispiel:
 - a. Android-Anwendungen müssen in ihrem Anwendungsmanifest und/oder ihrer Netzwerkkonfigurationsdatei ausdrücklich erklären, dass unsicherer Netzwerkverkehr zu keiner Netzwerkdomeäne zulässig ist.
 - b. iOS-/iPadOS-Anwendungen müssen ausnahmslos Application Transport Security (ATS) nutzen.
12. Kryptografische Materialien sollten an einen hardwaregestützten, sicheren Schlüsselspeicher gebunden sein.
13. Mobile Anwendungen müssen im Release-Modus erstellt werden und dürfen Folgendes nicht enthalten:
 - a. Jede Funktion oder Methode, die Sicherheitskontrollen umgehen kann,
 - b. Debug-Informationen wie Quellcode-Dateinamen, Variablennamen, Symbolnamen, Kommentare usw., die eine Rückentwicklung erleichtern könnten.
14. Mobile Anwendungen müssen mit wirksamen Anti-Hooking- oder Anti-Manipulationsmechanismen ausgestattet sein, um die Einschleusung von Schadcode zu verhindern, der das Verhalten der Anwendung zur Laufzeit verändern oder überwachen könnte.
15. Mobile Anwendungen müssen umfassende Anti-Debugging- oder Anti-Reverse-Engineering-/Verschleierungstechniken implementieren, um Reverse-Engineering-Angriffe zu verhindern.
16. Mobile Anwendungspakete müssen mit einer Funktion ausgestattet sein, die eine Überprüfung der Authentizität und Integrität ihres Inhalts ermöglicht (z. B. mithilfe kryptografischer Prüfsummen und/oder digitaler Signaturen).
17. Wenn die mobile Anwendung eine Benutzerauthentifizierung erfordert, sollten die Integritätsprüfungen der Anwendung und/oder des Geräts abgeschlossen sein, bevor mit der Benutzerauthentifizierung begonnen wird.
18. Mobile Anwendungen, die auf Informationen von Citi zugreifen, diese verarbeiten oder speichern, die von Citi als vertraulich oder höher eingestuft sind und/oder deren IS-Risikoeinstufung „mittel“ oder höher ist, dürfen nur starke biometrische Verfahren verwenden (z. B. müssen sie die Anforderungen der Klasse 3/Stufe „stark“ gemäß der Definition im entsprechenden [Android Compatibility Definition Document](#) erfüllen oder übertreffen).
19. Mobile Anwendungen müssen Gegenmaßnahmen zum Schutz vor Man-in-the-Middle-Angriffen (MitM) implementieren.

20. Mobile Anwendungen müssen kompromittierte Geräte erkennen können, einschließlich, aber nicht beschränkt auf mobile Geräte mit „Jailbreak“ oder „Rooting“, und gemäß der Risikobewertung des Unternehmens und den regulatorischen Anforderungen entsprechende Maßnahmen ergreifen.
21. Mobile Anwendungen müssen eine starke Gerätebindung implementieren, um zu verhindern, dass der Software-Token (z. B. der Besitznachweis) geklont wird.
22. Mobile Anwendungen müssen sichere Tastaturanwendungen/-lösungen verwenden (z. B. solche, die in die mobilen Betriebssysteme integriert/vorinstalliert sind).
23. Push-Benachrichtigungen dürfen keine sensiblen Informationen enthalten (z. B. Citi-Informationen mit der Klassifizierung „Vertraulich“ oder höher). Allerdings kann ein Einmalpasswort (OTP) per Push-Benachrichtigung verteilt werden.
24. Mobile Anwendungslösungen müssen mit der Fähigkeit ausgestattet sein, Kommunikationsversuche mit mobilen Clients abzulehnen/zu ignorieren, die Anwendungsversionen mit bekannten/ausnutzbaren Schwachstellen verwenden.
25. Mobile Anwendungen müssen die Best Practices der Branche einhalten, einschließlich, aber nicht beschränkt auf die in den [OWASP Mobile Top 10](#) veröffentlichten Präventionstechniken.
26. Mobile Anwendungen, die sich Techniken der künstlichen Intelligenz und des maschinellen Lernens (KI/ML) zunutze machen, müssen dies auf ethische Weise und in Übereinstimmung mit Abschnitt 19 – **Error! Reference source not found.** (einschließlich generativer KI/agentischer KI) tun.
27. Die mobile Anwendung muss die minimalen Geräteberechtigungen nutzen, die zum Ausführen der von Citi genutzten Zwecke/Funktionen erforderlich sind.
28. Mobile Anwendungen dürfen keine nicht öffentlichen Informationen auf externen/entfernbaren Speichern wie SD-Karten speichern.**Error! Reference source not found.Error! Reference source not found.**

17.65 Offenlegung von Software

Der Lieferant muss sämtliche Softwarekomponenten offenlegen, einschließlich, aber nicht beschränkt auf Open-Source-Software, die in Produkten oder Dienstleistungen enthalten sind, die Citi bereitgestellt werden (zusammenfassend „Softwarekomponenten“). Der Lieferant wird keine Softwarekomponenten per Update, Upgrade oder auf andere Weise in eine Version der Produkte oder Dienstleistungen integrieren, die auf den Systemen von Citi installiert werden sollen, ohne Citi in jedem Einzelfall vorher darüber zu informieren. Darüber hinaus stellt der Lieferant sicher, dass seine Produkte oder Dienstleistungen keine Softwarekomponenten enthalten, die unter Bedingungen lizenziert ist, die Citi oder seine verbundenen Unternehmen Verpflichtungen unterwerfen, die von Citi nicht ausdrücklich in einer Vereinbarung offengelegt und akzeptiert wurden. Der Lieferant muss Citi innerhalb von 30 Tagen nach der Entdeckung alle schädlichen Softwarekomponenten offenlegen, die innerhalb der Organisation des Lieferanten oder in den für Citi bereitgestellten Produkten oder

Dienstleistungen erkannt wurden. Insbesondere muss der Lieferant seine Verwendung von Softwarekomponenten in jeder Version der Produkte oder Dienstleistungen offenlegen, indem er Citi eine Software Bill of Materials („SBOM“) entweder im OWASP CycloneDX-Dateiformat oder im ISO/IEC 5962:2021 Software Package Data Exchange (SPDX) Dateiformat zur Verfügung stellt. Eine solche Offenlegung muss enthalten, woher die Software-Komponenten stammen (z. B. kommerzieller Anbieter, eingebettete Datenbank, öffentlicher Binärpaket-Manager, aus Quellcode erstellt oder von einem Anbieter für eingebettete Software bzw. kuratierte Softwarekomponenten bereitgestellt), und ob der Lieferant oder eine seiner Abhängigkeiten in der Software-Lieferkette eine Kopie der Softwarekomponenten erstellt hat (bekannt als „Fork“) und diese anschließend in seine Produkte oder Dienstleistungen integriert hat – entweder als Paketabhängigkeit oder als Quellcode, der in den Quellcode des Lieferanten integriert wurde, aus dem die Produkte und Dienstleistungen kompiliert werden.

17.66 Bedrohungsmodellierung

Der Lieferant muss einen Prozess zur Bedrohungsmodellierung implementieren, der alle folgenden Punkte umfassend berücksichtigt und/oder umfasst:

1. Definition des Umfangs: Der Lieferant muss den Umfang des Bedrohungsmodells klar definieren, wobei der Schwerpunkt auf Softwarekomponenten und Datenflüssen liegen muss, die Citi-Informationen mit der Klassifizierung „Vertraulich“ oder höher verarbeiten, speichern oder übertragen.
2. Identifizierung von Bedrohungen: Der Lieferant muss potenzielle Bedrohungen und Schwachstellen, die für das Design, die Architektur und die beabsichtigte Verwendung der Software relevant sind, systematisch identifizieren und dabei verschiedene Angriffsvektoren und Bedrohungsakteure früh im Lebenszyklus des Designs berücksichtigen.
3. Risikoanalyse: Der Lieferant muss identifizierte Bedrohungen analysieren, um ihre potenziellen Auswirkungen zu bewerten und somit die Priorisierung von Sicherheitsrisiken zu ermöglichen.
4. Integration von Kontrollen: Der Lieferant muss angemessene Sicherheitskontrollen und Strategien zur Risikominderung definieren und in den Entwurf und die Entwicklung der Software integrieren, um diese priorisierten Risiken zu beheben.
5. Dokumentation: Der Lieferant muss das Bedrohungsmodell dokumentieren, einschließlich der identifizierten Bedrohungen, der damit verbundenen Risiken und der entsprechenden implementierten Risikominderungsmaßnahmen.
6. Regelmäßige Überprüfung: Der Lieferant muss Bedrohungsmodelle regelmäßig überprüfen und aktualisieren, insbesondere wenn sich die Design-, Funktions- oder Einsatzumgebung der Software erheblich ändert.

17.67 Künstliche Intelligenz

1. Lieferanten müssen für alle KI-/ML-Systeme und -Komponenten, die Citi bereitgestellt oder in Citi integriert werden, einen robusten Secure Software Development Lifecycle (SSDLC) implementieren und einhalten. Dies umfasst

sicheres Design, sichere Entwicklung, sichere Tests, sichere Bereitstellung und die laufende Wartung.

2. Vom Lieferanten zur Verfügung gestellte KI-Systeme müssen Integrität in ihren Prozessen nachweisen und eine stabile Widerstandsfähigkeit gegenüber Angriffen aufzeigen. Dies umfasst die Implementierung von Mechanismen zur Erkennung von Prompt-Injection-Angriffen, zur Eingabesanitierung und zur Gewährleistung der Datenisolation.
3. Von Lieferanten bereitgestellte KI-Agenten und -Komponenten müssen sicher mit den Systemen und anderen Tools von Citi interagieren. Dies erfordert ein starkes Identitäts- und Zugriffsmanagement, eine strikte Validierung der Argumente für die Toolausführung sowie die Isolation von Tool-Operationen mit hohem Risiko. Human-in-the-Loop-Mechanismen (HITL) müssen für sensible oder risikoreiche Aktionen integriert werden.
4. KI-Systeme des Lieferanten müssen für alle wesentlichen Ereignisse umfassende, unveränderliche und prüfbare Protokolle erzeugen. Diese Protokolle müssen vor Manipulation geschützt, zusammengefasst und in Übereinstimmung mit den Richtlinien von Citi aufbewahrt werden. Kontinuierliche Überwachungs- und Anomalie-Erkennungsfunktionen sind erforderlich, um sicherheitsrelevante Vorfälle und verdächtige Aktivitäten zu identifizieren und entsprechende Warnmeldungen auszulösen.
5. KI-Systeme des Lieferanten müssen eine risikobasierte menschliche Überwachung unterstützen, die angemessene Eingriffe ermöglicht, und so konzipiert sein, dass eine klare Verantwortlichkeit für KI-Ergebnisse und -Aktionen gewährleistet ist. Dies umfasst die Klassifizierung von KI-Ergebnissen nach Risikostufe und die Unterstützung von Funktionen zur menschlichen Übersteuerung.
6. Alle von Lieferanten bereitgestellten KI-Agenten, -Komponenten und -Systeme müssen robuste Identitäts- und Zugriffsmanagementkontrollen implementieren. Jede KI-Interaktion muss einer identifizierbaren Identität (menschlich oder nicht menschlich) zugeordnet werden können, wobei für jeden Zugriff eine Authentifizierung erforderlich ist. KI-Agenten müssen verwaltete Identitäten verwenden und beim Zugriff auf Citi-Ressourcen das Least-Privilege-Prinzip befolgen.
 - a. Lieferanten müssen alle KI-Agenten bereitstellen und sicherstellen, dass diesen Citi Object Identity Network (COIN)-Agentenidentitäten zugewiesen werden, die mit den Identity- und Access-Management-(IAM)-Systemen von Citi föderiert sind, damit Citi-Sicherheitsrichtlinien angewendet, Identitäten zentral verwaltet und Prüfpfade gewährleistet werden können.
 - b. Lieferanten müssen Drittanbieter-Agenten mithilfe von von Citi genehmigten Integrationsmechanismen in COIN aufnehmen, einschließlich der über sichere Gateways (z. B. SSG Gateway oder Apigee) verfügbaren COIN-API, und sicherstellen, dass diese Aufnahme sicher und in Übereinstimmung mit den anwendbaren Sicherheitsanforderungen von Citi erfolgt.
 - c. Intern gehostete Lieferanten müssen ein eigenes Token generieren, das mit COIN kompatibel ist. Extern gehostete Lieferanten, die eingehende Authentifizierungen über ihr eigenes föderiertes Token

durchführen, müssen einen unterstützten Token-Austausch für Citi-Token implementieren, beispielsweise den Austausch von MSFT-Token zu COIN-Token. Jeder neue Tokentyp, der derzeit nicht über den Austauschmechanismus unterstützt wird, muss vom IAM-Team von Citi geprüft und genehmigt werden.

7. Wenn Lieferanten Model Context Protocol (MCP)-Server oder -Clients einsetzen oder bereitstellen, müssen sie den MCP RFC 7591 einschließlich sämtlicher optionaler Funktionen implementieren.
8. KI-Systeme des Lieferanten müssen System-Prompts sowie interne Mechanismen vor unbefugter Offenlegung und Manipulation schützen. Das Kontextmanagement muss strenge Isolationsgrenzen gewährleisten, um Datenlecks zwischen Mandanten, Benutzern oder Umgebungen zu verhindern.
9. Lieferanten müssen über dokumentierte Verfahren verfügen, um KI-spezifische Sicherheitsvorfälle zu erkennen, darauf zu reagieren und diese zu melden, einschließlich adversarialer Angriffe, Manipulationen von Modellen, unbefugter KI-Aktionen oder Datenverletzungen im Zusammenhang mit KI-Systemen. Citi muss unverzüglich über solche Vorfälle informiert werden.

18 RICHTLINIEN ZUR SICHERHEIT AM ARBEITSPLATZ

Anwendbar auf Lieferanten, die auf Citi-Informationen zugreifen/ diese verarbeiten/verwalten/speichern UND/ODER Internetanwendungen der Marke Citi hosten UND/ODER eine Verbindung zu den Netzwerkressourcen von Citi haben UND/ODER unbegleiteten Zugang zu Citi-Einrichtungen benötigen.

Lieferanten haben die materiellen und immateriellen Vermögenswerte von Citi und ihren Kunden zu schützen. Vermögenswerte von Citi und ihren Kunden dürfen nur für die genehmigten Zwecke und in der genehmigten Weise (d. h. entsprechend einschlägigen Lizenzen und Bedingungen), und dies auch nur für die geschäftlichen Zwecke von Citi und den Citi-Lieferanten, verwendet werden. Zu Vermögenswerten zählen Bargeld, Wertpapiere, physisches Eigentum, Dienstleistungen, Geschäftspläne, Citi-Informationen, Lieferanteninformationen, Vertreiberinformationen, geistiges Eigentum (Computerprogramme, Modelle und andere Gegenstände) sowie sonstige persönliche, urheberrechtlich geschützte sowie vertrauliche Informationen. Die widerrechtliche Aneignung oder unbefugte Offenlegung von Citi-Vermögenswerten ist eine Verletzung Ihrer Pflicht gegenüber Citi und kann einen Betrugsakt gegen Citi darstellen. Ebenso stellt Nachlässigkeit, Verschwendung oder unbefugte Verwendung im Hinblick auf das Vermögen von Citi einen Verstoß gegen Ihre Pflichten gegenüber Citi dar.

Artikel	Anforderungen
Citi-Informationen (elektronische und ausgedruckte Dokumentation)	Citi-Informationen sind nach den gewöhnlichen Arbeitszeiten einzuschließen und zu sichern. Dies gilt auch, wann immer der Lieferant sich nicht am zugewiesenen Arbeitsplatz aufhält.

Artikel	Anforderungen
Desktop-Personal-Computer (PCs) und Laptops	PCs und Laptops, die dazu verwendet werden, Citi-Informationen einzusehen oder darauf zuzugreifen, müssen nach einem Zeitraum der Nichtbenutzung mit Bildschirmschoner-Passwörtern geschützt werden. Wann immer ein Lieferant sich von einem zugewiesenen Arbeitsplatz entfernt, muss er den PC und/oder Laptop mit STRG + ALT + ENTF und der Auswahl „Computer sperren“ sperren. Verwendet ein Lieferant einen Laptop, um Citi-Informationen einzusehen, muss der Lieferant sicherstellen, dass der Laptop während der Arbeitszeit mithilfe von Kabel- oder Sicherheitsschlössern mit der Basiseinheit verbunden ist und nach der üblichen Arbeitszeit sicher weggeschlossen ist.
Absperren	Aktenschränke und Schubladen, in denen Citi-Informationen aufbewahrt werden, müssen nach den normalen Arbeitszeiten verschlossen werden.
Offene Bürobereiche	Großraumbüros dürfen nicht als Dateiserver/Mini-Rechenzentren zum Speichern von Citi-Informationen verwendet werden, es sei denn, sie sind speziell für eine solche Verwendung vorgesehen und bei Citi dokumentiert.
Drucker, Kopierer und Faxablagen	Alle Citi-bezogenen Materialien müssen aus Druckern, Kopierern und Faxablagen entfernt werden.
Entsorgung	Citi-Informationen, die nicht mehr benötigt werden, sind zu entsorgen (dabei sind spezifische Aufbewahrungsfristen zu beachten). Unterlagen sind im Reißwolf zu zerkleinern oder in einen sicheren/abgeschlossenen Recyclingbehälter zu geben. Magnetmedien sind sicher zu entsorgen, nachdem ordnungsgemäße Löschverfahren eingehalten wurden.

19 KÜNSTLICHE INTELLIGENZ/MASCHINELLES LERNEN (EINSCHLIESSLICH GENERATIVER KI/AGENTISCHER KI)

Anwendbar auf Lieferanten, die künstliche Intelligenz/maschinelles Lernen (KI/ML), einschließlich generativer KI/agentischer KI, wie von Citi in diesen Anforderungen an Lieferanten definiert, in einem beliebigen Teil der von ihnen bereitgestellten Produkte oder Dienstleistungen einsetzen.

19.1 Der Lieferant darf die nachstehend beschriebenen KI-/ML-Technologien weder verwenden noch deren Verwendung durch Subunternehmer zulassen, es sei denn, eine solcher Verwendung wurde von den Vertragsparteien im jeweils anwendbaren Anhang oder Arbeitsauftrag des Vertrags vereinbart:

- a. In einem Produkt oder einer Dienstleistung, das bzw. die sie aufgrund des Vertrags unmittelbar oder mittelbar für Citi bereitstellen, oder in einem Teil davon verwendet, enthalten oder anderweitig integriert sind, einschließlich darin enthaltener oder eingebetteter Produkte oder Dienstleistungen Dritter; oder
2. In irgendeiner Weise vom Lieferanten zur Erfüllung eines Vertrags eingesetzt werden, unabhängig davon, ob diese KI-/ML-Technologien in dem tatsächlich an Citi gelieferten Produkt oder der tatsächlich an Citi erbrachten Dienstleistung verwendet, enthalten oder anderweitig integriert sind; oder
3. Vom Lieferanten in irgendeiner Weise eingesetzt, die dazu führen kann, dass Citi-Informationen solchen KI-/ML-Technologien ausgesetzt werden, einschließlich, aber nicht beschränkt auf KI-/ML-Technologien, die der Lieferant in seinen nicht kommerziellen Geschäftstätigkeiten einsetzt (z. B. für die Führung von Geschäftsunterlagen, Prozessverbesserungen, Forschung und Entwicklung, Compliance und interne Revision).

19.2 Die Nichterfüllung dieser Verpflichtungen durch den Lieferanten gilt als wesentlicher Verstoß gegen die Bedingungen dieser Vereinbarung.

19.3 Wenn eine Aufsichtsbehörde im Rahmen einer behördlichen Inspektion oder forensischen Untersuchung des Einsatzes von KI/ML in einem Teil des Produkts/der Dienstleistung eine Anfrage stellt, muss der Lieferant Citi bei der Beantwortung der Anfrage der Aufsichtsbehörde unterstützen, einschließlich der Durchführung und/oder Erleichterung der Durchführung von Algorithmus-Audits, die erforderlich sind, um die tatsächlichen Operationen der Algorithmen, die die KI/ML-Modelle umfassen, aufzudecken.

19.4 Außerdem sind folgende Grundsätze einzuhalten:

Rechtmäßigkeit. Die KI-/ML-Systeme des Lieferanten müssen den geltenden Gesetzen entsprechen.

Zweck und Verhältnismäßigkeit. Der Lieferant darf Inhalte oder Citi-Informationen nicht mit Daten des Lieferanten oder Dritten zusammenführen. Der Lieferant darf ohne schriftliche Genehmigung von Citi keine Inhalte oder Citi-Informationen zur Schulung von KI/ML verwenden. Der Lieferant für KI/ML darf Inhalte oder Citi-Informationen nur in dem Umfang nutzen, der für die Erbringung der Dienstleistungen erforderlich ist.

20 KUNDENBESCHWERDEN

20.1 Eine Beschwerde ist eine mündliche oder schriftliche Mitteilung, die mündlich (persönlich oder telefonisch) oder schriftlich (per Post oder über elektronische Kommunikationsmittel wie E-Mail, Chat oder soziale Medien usw.) erfolgen kann und in der ein Kunde, Nichtkunde, Citi-Kunde, potenzieller Kunde oder ein bevollmächtigter Vertreter eines Kunden (zusammenfassend als „Kunde“ bezeichnet) seine Unzufriedenheit über eine Richtlinie von Citi, ein Produkt oder eine

Dienstleistung, die von oder über Citi angeboten wird, einen Mitarbeiter von Citi, einen Auftragnehmer von Citi oder einen Drittanbieter, der im Namen von Citi handelt, oder eine Kombination der vorgenannten Punkte zum Ausdruck bringt.

- 20.2** Lieferanten müssen sich an die Richtlinie von Citi zum Umgang mit Kundenbeschwerden sowie an alle geltenden Standards und Verfahren von Citi im Zusammenhang mit Beschwerden halten. Der Lieferant wird seinen primären Citi-Geschäftskontakt (oder einen Beauftragten) innerhalb von vierundzwanzig (24) Stunden nach Erhalt einer schriftlichen oder mündlichen Beschwerde bzw. Beanstandung (jeweils eine „Beschwerde“) schriftlich benachrichtigen, die der Lieferant von einem Kunden (oder einem Nichtkunden oder potenziellen Kunden gemäß der Citi-Definition von Beschwerden) oder von einer Aufsichtsbehörde erhalten hat und die sich auf die vom Lieferanten im Namen von Citi erbrachten Dienstleistungen oder anderweitig auf Citi bezieht. Sofern Citi dem Lieferanten kein solches System zur Verfügung stellt, entwickelt, implementiert und unterhält der Lieferant ein für Citi zufriedenstellendes System („Tracking-System“) zur Verfolgung von Beschwerden und stellt Citi nach eigenem Ermessen eine Kopie der Berichte oder Zugang zum System zur Verfügung. Das Tracking-System wird:
- a. Beschwerden nach Art, Eingangsdatum und Datum, an dem Citi über die Beschwerde informiert wurde, kategorisieren,
 - b. den Verlauf der Bearbeitung der Beschwerde bis zum Abschluss/zur Lösung verfolgen und
 - c. alle sonstigen Angelegenheiten regeln, die von Citi vernünftigerweise verlangt werden können. Das Tracking-System muss so konzipiert sein, dass der Lieferant feststellen kann, ob er eine übermäßige Anzahl von Beschwerden in Bezug auf eine bestimmte Angelegenheit erhält, so dass der Lieferant (in Absprache mit Citi) feststellen kann, ob es ein systemisches Problem in Bezug auf das Geschäft des Lieferanten oder die Erbringung seiner Dienstleistungen gibt, und die Probleme umgehend beheben kann.

21 RICHTLINIE FÜR DEN PRIVATEN HANDEL UND PRIVATE INVESTITIONEN

Die Richtlinie für den privaten Handel und private Investitionen (PTIP) von Citi definiert zulässige und unzulässige Handels- und Investitionstätigkeiten, Vorabgenehmigungsanforderungen sowie Anforderungen hinsichtlich der Führung, Offenlegung und Überwachung der Brokerage- oder Handelskonten einer betroffenen Person. Sie legt Mindeststandards fest, um die Einhaltung der Gesetze und Vorschriften zur Verhinderung der missbräuchlichen Nutzung der Position oder Beziehung einer Person zu Citi zu fördern, einschließlich der Kenntnisse dieser Person über (1) wesentliche nicht öffentliche Informationen oder Insiderinformationen (zusammenfassend als „MNPI“ bezeichnet) über Citi oder einen Dritten oder (2) Informationen über Wertpapier-, Derivate- und Rohstoffpositionen, Transaktionen und Strategien von Kunden.

Alle Mitarbeiter von Lieferanten, die im Rahmen ihrer Tätigkeit bei Citi regelmäßig Zugang zu MNPI benötigen und als betroffene Personen und/oder Citi-Zugangsberechtigte benannt sind, müssen die Anforderungen der PTIP einhalten. Die Mitarbeiter des Lieferanten müssen den Anforderungen von ICRM in Bezug auf die Offenlegung persönlicher Konten, die Vorabgenehmigung persönlicher Handelsaktivitäten, persönliche Handelsbeschränkungen und die Einreichung regelmäßiger Erklärungen nachkommen.

22 RECHNUNGS- UND ABRECHNUNGSSTANDARDS

Im Zusammenhang mit den Bemühungen von Citi, die Pünktlichkeit der Dienstleistungen zu verbessern und die Kontrollen zu verstärken, sind alle Lieferanten verpflichtet, die von Citi bevorzugten Methoden zur Rechnungsstellung sowie die bevorzugten Zahlungsoptionen für Rechnungen zu unterstützen, wie nachstehend aufgeführt:

- Der Lieferant erstellt elektronische Dateien, die an Citi in dem vom Lieferanten mitgeteilten Format übermittelt werden, und/oder nutzt das Citi iSupplier-Tool, um die erforderlichen Rechnungs-/Abrechnungsdaten für die anschließende digitale Übermittlung an Citi einzugeben.
- Der Lieferant stellt Citi alle erforderlichen Bankdaten und Unterlagen zur Verfügung, um die elektronische Zahlung an den Lieferanten zu ermöglichen und/oder das Angebot von Citi für Zahlungen mit virtuellen Karten (sofern verfügbar) zu nutzen.

Hinweis: Die Zahlungsbedingungen werden ab dem Datum berechnet, an dem die Rechnung bei Citi eingeht.

Um eine pünktliche Zahlung und die Einhaltung vertraglicher Verpflichtungen zu gewährleisten, verlangt Citi von allen Lieferanten, dass sie bei der Rechnungsstellung für Waren oder Dienstleistungen an Citi die folgenden Rechnungsdaten angeben und die entsprechenden Richtlinien einhalten:

1. Die korrekte Citi-Geschäftseinheit, die Rechnungsadresse und der zugehörige Name des Citi-Geschäftskontakts.
2. Rechnungsnummer, Rechnungsdatum und Bestellnummer.
3. Rechnungen sind an die Citi-Niederlassung oder E-Mail-Adresse zu senden, die auf der Citi-Bestellung angegeben ist.
4. Die in Rechnung gestellten Waren oder Dienstleistungen müssen in der Rechnung klar und detailliert beschrieben sein.
5. Geben Sie nur die aktuellen Beträge für die jeweilige Rechnung an (keine anderen ausstehenden Rechnungsbeträge).
6. Rechnungen sind in englischer Sprache zu erstellen, einschließlich aller Begleitdokumente.

23 RICHTLINIE ZU VERPFLICHTENDEN ABWESENHEITEN

Die Richtlinie von Citi zu verpflichtenden Abwesenheiten verlangt von Personen, die sensible oder risikoreiche Tätigkeiten ausüben, insbesondere solche, die sich auf die Bücher und Aufzeichnungen des Unternehmens auswirken, diese Aufgaben regelmäßig vorübergehend nicht wahrzunehmen. Diese vorgeschriebene Trennung von den Aufgaben soll die internen Kontrollen stärken, indem sie Gelegenheiten schafft, potenziellen Betrug, Diebstahl oder sonstiges Fehlverhalten aufzudecken, das andernfalls unentdeckt bleiben könnte. Die Richtlinie entspricht den Aufsichtsanforderungen des US Federal Reserve Board in Bezug auf eine vorgeschriebene Abwesenheit von Mitarbeitern in sensiblen Positionen.

Alle Mitarbeiter des Lieferanten, die im Rahmen ihrer Aufgaben bei Citi Zugriff auf sensible Daten haben **und** als „sensible“ Personen eingestuft sind, müssen die Anforderungen der Richtlinie zu verpflichtenden Abwesenheiten einhalten. Sensible Personen sind verpflichtet, jährlich eine obligatorische Abwesenheitsphase gemäß allen Vorschriften und Einschränkungen der Richtlinien zu planen und vollständig einzuhalten. Während dieses Zeitraums dürfen sie keine sensiblen Tätigkeiten durchführen, anweisen, autorisieren oder genehmigen. Sie dürfen ferner auf keine Kommunikation – einschließlich Interaktionen mit Kunden – reagieren, es sei denn, dies dient ausschließlich der Weiterleitung von Anfragen an die zuständige Vertretung. Wenn der Abwesenheitszeitraum nach seinem Beginn unterbrochen werden muss, müssen Manager oder Citi-Geschäftskontakte diesen in den Compliance-Systemen stornieren, damit der Systemzugriff wiederhergestellt werden kann. Anschließend muss der Mitarbeiter einen neuen Abwesenheitszeitraum planen.

ANHANG – DEFINITIONEN

Air-Gap ist eine Sicherheitsmaßnahme, bei der ein Computer, System oder Netzwerk physisch von anderen Computern, Systemen oder Netzwerken getrennt ist. Eine Air-Gap-Datenbackup-Architektur begrenzt die Gefährdung durch einen Cyberangriff und ermöglicht die Wiederherstellung von Daten zu einem Zeitpunkt vor Beginn des Angriffs.

Anwendbares Recht umfasst: (a) die Gesetze und Verordnungen der Bundesstaaten zur Zwangsvollstreckung und (b) die Regeln, Richtlinien und sonstigen Mitteilungen verschiedener Bundesbehörden der Vereinigten Staaten, einschließlich des Office of the Comptroller of the Currency (manchmal als Red Flag Guidelines and Regulations bezeichnet), die Abschnitt 114 des Fair and Accurate Credit Transactions Act von 2003 umsetzen

Verfügbarkeitszonen sind Bereiche, in denen der Cloud Service Provider eine Gruppe logisch zusammengefasster Rechenzentren betreibt. Eine Verfügbarkeitszone besteht aus einem oder mehreren räumlich getrennten Rechenzentren mit redundanter Stromversorgung sowie redundanten Netzwerk- und Telekommunikationsverbindungen innerhalb einer Cloud-Region.

Künstliche Intelligenz (KI) bezieht sich auf eine quantitative Methode, ein System oder einen Ansatz („Techniken“), mit dem menschliche Intelligenz durch Computerprogramme nachgebildet wird, um Schätzungen, Prognosen, Empfehlungen oder Entscheidungen zu generieren, die über klassische statistische, mathematische, ökonometrische oder finanzwirtschaftliche Verfahren hinausgehen. Dies umfasst alle unten aufgeführten KI-Kategorien sowie Varianten der KI – zum Beispiel: generative KI, agentische KI, große Sprachmodelle, Allzweck-KI-Modelle (GPAI) usw.

Zu den KI-Kategorien gehören:

- **Statische KI:** KI-Techniken, die manuell offline trainiert werden oder deren Parameter explizit programmiert und dann verwendet werden, um Schätzungen, Vorhersagen, Empfehlungen oder Entscheidungen zu treffen.
- **Dynamische KI:** Techniken, die im Gegensatz zu „statischer KI“ Parameter regelmäßig automatisch in der Produktion neu trainieren können.
- **Automatische KI:** „Dynamische KI“-Techniken, die zusätzlich in der Lage sind, ihre Grundstruktur automatisch zu verändern (z. B. Hyperparameter, Eingangsvariablen).
- **Kognitive KI:** Techniken, die autonom Entscheidungen treffen und entsprechende Maßnahmen ergreifen können, auch in Angelegenheiten, für die sie nicht speziell ausgebildet wurden.

Maschinelles Lernen (ML) ist die Teilmenge der KI, die Darstellungen oder Schlussfolgerungen aus Daten ableitet, ohne jede Parameterdarstellung oder jeden Computerschritt explizit zu programmieren, z. B. Random Forests, auf neuronalen Netzwerken basierende Ansätze. Im Gegensatz dazu umfassen KI-Techniken, die nicht Mitglieder der ML-Untergruppe sind, Techniken wie Fuzzy-Logik, komplexe Abhängigkeits-Parsing-Techniken für die Verarbeitung natürlicher Sprache.

Business Activity Owner (BAO) ist ein Mitarbeiter von Citi, der für die Durchführung und aktive Verwaltung bestimmter Aktivitäten im Zusammenhang mit Lieferantenbeziehungen verantwortlich ist.

Geschäftsvermittler ist ein von Citi beauftragter Lieferant, der im Namen von Citi neue Geschäftsmöglichkeiten identifiziert oder bestehende Kundenbeziehungen verwaltet.

Geschäftsgeschenk ist jeglicher Wertgegenstand (außer geschäftliche Unterhaltung), die ein Citi-Mitarbeiter im Zusammenhang mit der geschäftlichen Tätigkeit von Citi oder des Unternehmens der externen Partei gewährt oder empfängt. Gegenstände im Wert von 25 USD oder weniger sind davon ausgeschlossen.

Citi-Informationen sind Informationen, die Citi besitzt oder zu deren Schutz Citi während der Speicherung, Verarbeitung, Übertragung oder Entsorgung in digitalen und nicht-digitalen Formaten verpflichtet ist.

Klassifizierungen von Citi-Informationen umfassen:

Vertraulich bezeichnet Informationen über Citi-Geschäftsbereiche und/oder verbundene Parteien, die sich nicht auf Einzelpersonen beziehen und ein hohes Schutzniveau erfordern. Eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit dieser Informationen könnte schwerwiegende Auswirkungen auf die Geschäftstätigkeit, die finanzielle Lage, das Franchise oder die Unternehmenskunden von Citi haben.

Vertrauliche personenbezogene Daten sind persönliche Informationen über eine Person, die potenziell rechtswidrige Aktivitäten wie Identitätsdiebstahl, Kreditbetrug oder andere finanzielle Betrügereien gegen die besagte Person ermöglichen könnten. Eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit dieser Informationen könnte erhebliche Auswirkungen auf die betroffene(n) Person(en) haben, unter anderem finanzielle Verluste oder Betrug.

- Zu den personenbezogenen Datenelementen, die in Kombination mit anderen personenbezogenen Daten vertrauliche PII darstellen, gehören der Name oder die Kontaktdaten (Adresse, Telefonnummer oder E-Mail-Adresse) in Kombination mit:
 - Transaktionsdatenelementen, die zu Geldbewegungen führen oder für Identitätsdiebstahl oder Betrug verwendet werden können, wie zum Beispiel:
 - Kredit-/Debitkartennummer
 - Kartenprüfwert (CVV) oder PIN
 - Daten zur Kreditauskunft (Kredit-Score)
 - Vollständiges Geburtsdatum
 - Informationen zur Leistung der Mitarbeiter (Beurteilung/Feedback) oder zur Vergütung
 - Videoaufzeichnungen einschließlich CCTV-Aufzeichnungen und Aufzeichnungen am Bankautomaten
- Bestimmte personenbezogene Datenelemente sollten isoliert betrachtet vertrauliche PII darstellen:
 - U.S.-Sozialversicherungsnummer, von der Regierung ausgestellte Identifikationsnummer (die der U.S.-Sozialversicherungsnummer in der Verwendung und/oder im rechtlichen Schutzstatus gleichwertig ist), Reisepassnummer, Führerscheinnummer oder die Steuernummer einer Person

Intern bezeichnet Informationen, die nicht eine Einzelperson betreffen, für geschäftliche Zwecke bestimmt sind und ein moderates Schutzniveau erfordern. Eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit dieser Informationen könnte nur **begrenzte Auswirkungen** auf ein Team oder eine Arbeitsgruppe haben.

- **Personenbezogene Daten (PII):** Personenbezogene Informationen sind alle

Informationen, die:

- Eine Person oder einen Haushalt identifizieren oder zur Identifizierung verwendet werden können (z. B. Name, Unterschrift, Adresse, eindeutige nationale Kennung wie Sozialversicherungsnummer, Einwohnermeldeamtsnummer, Geburtsdatum, Führerscheinnummer).
- Sich auf eine Person oder einen Haushalt beziehen, diese/n beschreiben, mit ihr/ihm verknüpft werden können oder vernünftigerweise (direkt oder indirekt) mit ihr/ihm in Verbindung gebracht werden könnten.
- Verwendet werden können, um eine Person zu authentifizieren oder Zugang zu einem Konto zu gewähren (wie
- Benutzername, E-Mail-Adresse, Passwort, PIN, Identifikationsnummer, Antworten auf Sicherheitsfragen); oder sich auf eine Person bezieht und sensibel sein könnte (wie persönliche medizinische oder gesundheitliche Informationen, Kontonummer, Kontowert).
- Zu den personenbezogenen Daten gehören auch geschützte Gesundheitsdaten (gemäß der Definition im U.S. Health Insurance Portability and Accountability Act), sensible personenbezogene Daten und Kreditinformationen (gemäß der Definition in verschiedenen Datenschutz- und Bankgeheimnisgesetzen).

Öffentlich bezeichnet Informationen, die außerhalb von Citi frei verfügbar sind oder für die öffentliche Nutzung bestimmt sind, wie beispielsweise Citi-Pressemittelungen oder Nachrichtenartikel über Citi.

Eingeschränkt bezeichnet Informationen, deren Nutzung auf bestimmte Personen oder Gruppen beschränkt ist, die für Citi oder seine verbundenen Unternehmen besonders sensibel sind und ein Höchstmaß an Schutz erfordern. Eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit dieser Informationen könnte **schwerwiegende Auswirkungen (unternehmensweit, mehrere Regionen, mehrere Sektoren)** auf die Geschäftstätigkeit, die finanzielle Lage, das Franchise oder die Unternehmenskunden von Citi haben.

- **Sensible PII:** Personenbezogene Daten, die nach bestimmten gesetzlichen Vorschriften einen besonderen Schutz erfordern oder die potenziell dazu verwendet werden könnten, eine Person unrechtmäßig zu diskriminieren oder ihr anderweitig Nachteile oder Schaden zuzufügen. Eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit dieser Informationen könnte erhebliche Auswirkungen auf den Einzelnen haben (einschließlich, aber nicht beschränkt auf finanzielle Verluste, Betrug oder diskriminierende Auswirkungen).
- Daten speziell in Bezug auf: Rasse, Religion, religiöse oder philosophische Überzeugungen, ethnische Zugehörigkeit, politische Zugehörigkeit oder Meinung, Gewerkschaftsmitgliedschaft, kriminelle Hintergrundinformationen oder Straftaten, genetische Daten, biometrische Daten oder Daten zur sexuellen Orientierung oder Aktivität einer Person.
- Persönliche Gesundheitsinformationen (PHI), die Informationen zur Krankengeschichte oder zum geistigen oder körperlichen Zustand der Person enthalten.

Kunde bezeichnet jeden Klienten oder Kunden von Citi und kann Einzelpersonen (d. h. natürliche Personen) sowie Unternehmen, Institutionen, Organisationen und juristische Personen umfassen.

Cloud-Region ist ein physischer Standort, an dem der Cloud-Service-Provider Datenzentren zusammenfasst.

Kommunikationsgeräte, -systeme und -dienste sind jegliche Hardware, Software oder Anwendungen, die bei der Übertragung von schriftlicher, sprachlicher oder elektronischer Videokommunikation verwendet werden. eComm-Kanäle umfassen, sind aber nicht beschränkt auf: Computer, Laptops, Tablets, Mobilgeräte oder Mobiltelefone, einschließlich „Bring Your Own Device“ (BYOD), BlackBerry, Telefon, Fax (Faxdienste), Intranet- und Internetzugang, WLAN-Dienste, E-Mail-Dienste, Instant Messaging Dienste wie Microsoft Lync, Skype und Bloomberg-Nachrichten, Websites und Anwendungen mit eingebetteten Kommunikationsfunktionen, Videokonferenz- oder Kollaborationsplattformen wie Zoom oder Microsoft Teams sowie Social-Media-Dienste, interaktive Informationsaustauschdienste, Chatrooms von Drittanbietern, elektronische Bulletin Boards und Blogs.

Inhalt bezeichnet Citi vertrauliche Informationen und alle anderen Daten, Berichte, Statistiken oder Informationen jeglicher Art, (a) die dem Lieferanten direkt oder indirekt von oder im Namen von Citi oder ihren Verbundenen Unternehmen oder von oder im Namen ihrer oder seiner Klienten, Kunden oder Dienstleistungsanbieter zur Verfügung gestellt werden, (b) die über die Dienstleistungen erstellt oder produziert werden oder (c) die aus einem der vorgenannten Punkte abgeleitet werden.

Vertrag bezeichnet ein schriftliches Rechtsdokument, das von zwei oder mehr Parteien unterzeichnet wurde und ein Angebot, eine Annahme, eine Gegenleistung, die Verpflichtungen der Parteien sowie einen rechtmäßigen Zweck umfasst. Beispiele von Verträgen sind Hauptvereinbarungen zu Produkten und Dienstleistungen, Leistungsbeschreibungen/Arbeitsaufträge, Änderungen und Ergänzungen, Anhänge, Bestellungen oder jedes andere von einem Citi-Unternehmen und einem Lieferanten unterschriebene schriftliche Dokument. Auch eine Geheimhaltungsvereinbarung (NDA) gilt für die Zwecke dieser Standards als Vertrag.

Zugangsverweigerungstest (Denial of Access, DOA) überprüft die Personalbesetzung und den Support des Lieferanten für Citi-Geschäftsprozesse, die innerhalb des definierten RTO wiederhergestellt werden können.

Systemausfalltest (Denial of Service, DOS) prüft die Anwendung und die zugrunde liegenden Infrastrukturkomponenten des Lieferanten, die Geschäftsprozesse von Citi unterstützen, die innerhalb des definierten Wiederherstellungszeitziels wiederhergestellt werden können.

„Hinterlegte Materialien“ bezeichnet die folgenden Unterabschnitte (i) bis (vi) zusammen, jeweils in Bezug auf die Software, die Citi für den Betrieb innerhalb der Citi-Umgebung lizenziert wurde, oder die Materialien, die vom Lieferanten für die für Citi erbrachten Hosted Services verwendet werden:

- (i) Eine exakte, identische Kopie des Quellcodes der Software, die für die Entwicklung, den Betrieb, die Wartung und den Support der lizenzierten Software oder der gehosteten Dienste gemäß der geltenden Vereinbarung mit Citi verwendet wird (sowie aller nachfolgenden Versionen dieser Software oder gehosteten Dienste), sowie die gesamte Dokumentation für diese Software (unabhängig davon, ob Citi bereits über eine Kopie von Teilen dieses Quellcodes verfügt) („**Quellcodehinterlegung**“);
- (ii) Der Quellcode für jede Software von Drittanbietern, an der der Lieferant Rechte in Bezug auf die Entwicklung, den Betrieb, die Wartung und den Support der lizenzierten Software oder der gehosteten Dienste hat;
- (iii) Eine lizenzierte Kopie aller Softwaretools, wie Debugger, Assembler und Compiler, die erforderlich sind, um den in den hinterlegten Materialien enthaltenen Quellcode in eine

ausführbare Form zu konvertieren, die für den Betrieb, die Wartung und den Support der Software oder der gehosteten Dienste erforderlich ist.

- (iv) Soweit oben nicht bereits vorgesehen, gilt für alle Dokumentationen, die Folgendes enthalten: (A) allgemeine Beschreibungen und Funktionsweisen der hinterlegten Materialien; (B) Architektur und grundlegende Programmfunktionen; (C) Informationen zum Datenfluss; (D) detaillierte Speicherkarte und Auflistung; (E) Eingabe-/Ausgabe-Port-Zuordnungen; und (F) sonstige Details, die es einem Programmierer mit durchschnittlichen Kenntnissen in der/den anwendbaren Programmiersprache(n) ermöglichen würden, den in den hinterlegten Materialien enthaltenen Quellcode zu verwenden und zu ändern;
- (v) Alle sonstigen technischen Informationen in Bezug auf die Software oder die gehosteten Dienste, die vernünftigerweise erforderlich sind, damit Citi oder ein kompetenter Dritter im Namen von Citi die Software oder die gehosteten Dienste nutzen, betreiben, ändern und verbessern kann; und
- (vi) Eine Liste aller Softwareprodukte und Technologien von Drittanbietern, die in Verbindung mit der Software oder den gehosteten Diensten verwendet werden, einschließlich angemessener Details zu ihrer Verwendung in der Software und Kontaktinformationen des Anbieters dieser Software oder Technologie. Citi bestätigt und stimmt zu, dass die Einzahlungsunterlagen keinen Quellcode von Dritten enthalten, außer dem in Unterabschnitt (ii) genannten; und
- (vii) in Bezug auf gehostete Dienste:
 - a. eine verkleinerte Nachbildung der cloudbasierten Produktionsumgebung oder umgebungsspezifische Cloud-bezogene Materialien und sonstige Informationen, die zur Nachbildung der Produktionsumgebung von Citi erforderlich sind, einschließlich (aber nicht beschränkt auf): Infrastruktur wie Code, Terraform-Skripte, Cloud-Ressourcen, Cloud-Formation-Vorlagen, Konfigurationsdateien, Cloud-Mandanten, Cloud-Abonnements, Maschinenabbilder, Docker-Abbilder und Infrastruktur als Quellcode der Software; und
 - b. eine Kopie der im Softwareprogramm gespeicherten Citi-Daten.

Elektronische Kommunikation sind Nachrichten oder Informationen, die vom Personal unter Verwendung elektronischer Mittel gesendet, empfangen oder verwendet werden, die über Kabel oder drahtlose Signale übertragen werden. Elektronische Kommunikation umfasst unter anderem Textnachrichten, E-Mails, Peer-to-Peer- oder Sofortnachrichten, Blog-Posts, Beiträge in sozialen Medien, Nachrichten, die über Messaging-Anwendungen wie WhatsApp, WeChat, Line, Signal oder Viber gesendet werden, sowie Anhänge, Screenshots, aufgezeichnete Sprach- oder Videodateien, Live-Sprach- oder Videodateien und Dateien, die über elektronische Kommunikationsgeräte, -systeme und -dienste erstellt, empfangen, heruntergeladen, gespeichert, übertragen, gelöscht oder verwendet werden.

Funktions-IDs sind generische IDs wie ADMIN oder ROOT, die von einer Person oder einem Prozess für den Zugriff auf ein Sicherheitssystem verwendet werden. Eine Schlüsselinitiative im Bereich Identity and Access Management (IAM) besteht darin, sicherzustellen, dass Citi spezifische definierte Kontrollen zum Schutz vor den Risiken bei der Verwendung funktionaler Kennungen vorsieht.

Franchise-kritische Prozesse/Franchise-kritische Anwendungen (FCA) sind jene Prozesse/Anwendungen, die von Citi als wesentlich für die erfolgreiche Ausführung ihrer Franchise-kritischen Geschäftsfunktionen identifiziert wurden.

Betrug ist eine vorsätzliche Handlung, Falschaussage oder Unterlassung, die darauf abzielt, andere zu täuschen, was entweder dazu führt, dass das Opfer einen Verlust erleidet oder der Täter einen Gewinn erzielt.

Gehostete Dienste umfassen alle installierten Anwendungen und alle Einrichtungen und Umgebungen, die vom Anbieter verwaltet oder genutzt werden, um die gehosteten Dienste bereitzustellen, alle Anwendungen und andere Software, Datenbanken, Websites, Server, Hardware, Netzwerke, Telekommunikations- und andere Geräte und andere Technologien, die in der Umgebung der Gehosteten Dienste installiert sind oder genutzt werden, sowie in jedem Fall alle Aktualisierungen und Supportleistungen, jedoch nicht alle Inhalte und Systeme von Citi.

Identitätsprüfungsdaten (IVD) sind definiert als Sicherheitsfragen (SQ) oder wissensbasierte Authentifizierungsfragen (KBA). Sicherheitsfragen werden normalerweise von der Anwendung definiert und vom Endbenutzer beantwortet. Beispiele sind der Mädchenname der Mutter, der Geburtsort, das Lieblingseis usw. Beide Arten von Fragen müssen als Authentifizierungsdaten behandelt werden.

Informationssicherheit oder „IS“ bezeichnet den Zustand, in dem ein Computer oder ein Computersystem vor unbefugtem Zugriff oder Angriff geschützt ist und aufgrund dieses Zustands (a) der Computer oder das Computersystem weiterhin verfügbar und betriebsbereit ist; (b) die Integrität des Computers oder des Computersystems gewahrt bleibt; und (c) die Integrität und Vertraulichkeit der in dem Computer oder Computersystem gespeicherten, verarbeiteten oder übermittelten Informationen gewahrt bleibt.

Sicherheitsbedrohung bezeichnet eine Handlung oder Aktivität (ob bekannt oder vermutet), die auf oder durch einen Computer oder ein Computersystem ausgeführt wird, welche die Informationssicherheit dieses oder eines anderen Computers oder Computersystems gefährden oder beeinträchtigen kann.

Sicherheitsvorfälle bedeuten eine Sicherheitsanfälligkeit bei einem Computer oder Computersystem, die von einer oder mehreren Sicherheitsbedrohungen ausgenutzt werden kann.

Nicht kundenbezogene/nicht umsatzgenerierende Tätigkeiten werden als geschäftskritische Aktivitäten definiert, die nicht mit umsatzgenerierenden Aktivitäten verbunden sind, darunter gesetzlich, kontrollierend und behördlich vorgeschriebene Maßnahmen sowie Maßnahmen zur Geschäftsfortführung.

Vertraulichkeitsvereinbarung (Non-Disclosure Agreement, NDA) ist eine Vereinbarung zwischen Citi und einem Lieferanten, wonach der Austausch, die Verwendung und Weitergabe von Informationen den Bestimmungen der Vereinbarung unterliegt.

Open-Source-Software bezeichnet Quellcode oder ein kompiliertes Computerprogramm, bei dem der Quellcode der Allgemeinheit zur Nutzung oder Änderung gegenüber seinem ursprünglichen Entwurf zur Verfügung steht.

Personal: bedeutet, ob direkt angegeben oder aus dem Kontext abgeleitet, den Lieferanten und seine Tochtergesellschaften, Direktoren, leitenden Angestellten, Mitarbeiter, Vertreter, Wirtschaftsprüfer, Berater, Dienstleister und Auftragnehmer (ausgenommen Mitarbeiter von Citi). Zum Personal des Lieferanten zählen auch die Direktoren, leitenden Angestellten, Mitarbeiter, Vertreter, Wirtschaftsprüfer, Berater oder andere Vertreter eines Subunternehmers.

Unterlagenverzeichnis ist ein detailliertes, ausführliches Verzeichnis einschließlich Art, Ort, Erstellungstag usw. der Unterlagen von Citi, wie es für die ordnungsgemäße Führung und Aufbewahrung dieser Aufzeichnungen über den gesamten Lebenszyklus der Informationen durch das Unternehmen erforderlich ist.

Informationssperre bezeichnet eine Anforderung, die für Aufzeichnungen und Informationen gilt und deren Änderung oder Vernichtung aussetzt, bis sie von der Stelle aufgehoben wird, die die Sperre erteilt hat.

Wiederherstellungskapazität bedeutet das Volumen, die Menge oder die Geschwindigkeit der Lieferung der Produkte und Dienstleistungen des Lieferanten, ausgedrückt als Prozentsatz der normalen Lieferung von Produkten und Dienstleistungen.

Wiederherstellungsdauer bezeichnet die maximale Anzahl von Kalendertagen, für die der Lieferant den Betrieb im Wiederherstellungsmodus aufrechterhalten kann.

Ziel des Wiederherstellungspunktes ist der Zeitpunkt in der Vergangenheit, angegeben in Stunden, bis zu dem Daten nach einer Betriebsunterbrechung wiederhergestellt werden müssen. Dies ist der maximal zulässige Zielzeitraum, in dem Daten aufgrund eines schwerwiegenden Vorfalls aus einem IT-Service verloren gehen können. Das Wiederherstellungspunktziel ist nur ein Maß für den längsten Zielzeitraum, in dem Daten wegen eines größeren Vorkommnisses verloren gehen können, das einen EDV-Dienst betrifft. Es handelt sich nicht um einen direkten Maßstab dafür, wie viele Daten verloren gehen können, beispielsweise bis zum Ende der Verarbeitung des Vortages.

Wiederherstellungszeitziel bezeichnet die Anzahl der Stunden zwischen der Dienstunterbrechung und der Wiederherstellung von Produkten und Dienstleistungen.

„**Release-Event**“ bezeichnet eines oder mehrere der folgenden Ereignisse:

- (i) Der Lieferant (A) wird zahlungsunfähig oder gibt seine allgemeine Zahlungsunfähigkeit zu; (B) wird freiwillig oder unfreiwillig Gegenstand eines Verfahrens nach inländischem oder ausländischem Insolvenzrecht, das nicht innerhalb von sieben (7) Werktagen vollständig ausgesetzt oder innerhalb von fünfundvierzig (45) Tagen nach Einreichung des Antrags zurückgenommen oder aufgehoben wird; (C) eine allgemeine Abtretung zugunsten der Gläubiger vornimmt; oder (D) durch Beschluss eines zuständigen Gerichts einen Konkursverwalter, Treuhänder, Verwahrer oder einen ähnlichen Beauftragten bestellt, der einen wesentlichen Teil seines Vermögens oder Geschäftsbetriebs übernimmt oder veräußert.

Die **Resource Management Organization (RMO)** ist für das globale End-to-End-Ressourcenmanagement für Citi verantwortlich, einschließlich strategischer Beschaffung, Purchase-to-Pay-Operationen, Staffing Office und Supplier Management Framework.

Der **RMO Sourcing Manager** ist eine Person innerhalb der Resource Management Organization (RMO), die für die Aushandlung von Vertragsbedingungen, Anforderungen und Preisen verantwortlich ist, einschließlich

Ausschreibungen (RFPs) und andere Aktivitäten zur Lieferantenauswahl, Verwaltung der Vertragsbedingungen und Akkreditierungsanforderungen für die Finanzbewertung.

Schwere oder katastrophale nachteilige Auswirkungen auf eine Person bedeutet, dass die Auswirkung nach vernünftigem Ermessen zu erheblichen nachteiligen Auswirkungen für die Person führen könnte, einschließlich finanziellem Verlust, Verlust des Arbeitsplatzes oder Verlust oder Schwierigkeiten bei der Erlangung eines Arbeitsplatzes, Verlust der Menschenrechte, persönlicher oder öffentlicher Demütigung oder unangemessener Inhaftierung.

Subunternehmer: Ein Subunternehmer ist eine vierte Partei (natürliche oder juristische Person), die von einem Dritten beauftragt wurde, einige oder alle Dienste oder Tätigkeiten auszuführen, die Citi an den Dritten vergeben hat.

Hinweise:

Frage 1: Müssen alle Subunternehmer des Drittanbieters gemeldet werden?

Antwort 1: Lediglich die an der Leistungserbringung beteiligten Subunternehmer müssen gemeldet werden. Zu den von einem Subunternehmer ausgeführten Dienstleistungen oder Tätigkeiten zählen beispielsweise (jedoch ohne Beschränkung hierauf):

*Ein Subunternehmer, der Technologie- oder Softwaredienste erbringt, die die Dienste/Aktivitäten, die Citi an den Dritten vergeben hat, direkt oder indirekt unterstützen; oder

*Ein Subunternehmer, dessen Dienstleistungen den Zugriff auf vertrauliche oder höherwertige Informationen von Citi umfassen; oder

*Ein Subunternehmer, der direkt oder indirekt mit einem bestehenden/potenziellen Citi-Kunden interagiert; oder

*Ein Subunternehmer, der unbegleitet ist und innerhalb oder außerhalb eines Citi-Geländes Schredder- oder Archivierungsdienstleistungen für Citi-Dokumente erbringt; oder

*Ein Subunternehmer, der Kernfunktionen oder -dienste des Bankgeschäfts unterstützt, wie z. B. Zahlungen, Inkasso, Kreditvergabe usw.

Lieferant: Für die Zwecke dieses Dokuments „Citi-Anforderungen an Lieferanten“ bezeichnet der Begriff „Lieferant“ ausschließlich einen externen Dritten, der eine Geschäftsvereinbarung geschlossen hat, um Produkte oder Dienstleistungen direkt an eine Citi-Einheit zu liefern oder eine Citi-Einheit bei der Erreichung ihrer Geschäftsziele zu unterstützen. Ein externer Dritter ist definiert als ein Unternehmen, das nicht zu Citi gehört. Lieferanten können auch Kunden oder Klienten einer Citi-Einheit sein oder die Interaktion mit Kunden und Klienten von Citi unterstützen. Vereinbarungen, die ausschließlich auf ihrer Eigenschaft als Kunde oder Klient von Citi beruhen, gelten jedoch nicht als Lieferantenbeziehungen im Sinne dieses Dokuments.

Vorübergehende Informationen: Ein Datensatz ist die endgültige und vollständigste Version der Informationen, die Citi aus rechtlichen, behördlichen oder genehmigten geschäftlichen Gründen aufbewahren muss. Alle übrigen Informationen werden als „Vorübergehende Informationen“ eingestuft.