Kontrollpflichten externer Lieferanten

Informations- und Cyber-Sicherheit (ICS)

Version 10.0, Oktober 2020

Restricted - External

Kontrollbereich / Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Steuerung der Informations-/Cyber-Sicherheit – Rahmenwerk	Beim Lieferanten muss ein etabliertes und konsistentes Rahmenwerk zur Steuerung der Informations-/Cyber-Sicherheit, mit dem Einblicke in seine Mitarbeiter, Prozesse und die Technologie-Umgebung sowie den Zustand von Informations- und Cyber-Sicherheitskontrollen gewährt wird, sowie ein Sicherheitsprogramm zum Schutz des Lieferanten vor Cyber-Bedrohungen gemäß den führenden Praktiken der Branche (unter anderem NIST, ISO/IEC 27001) oder den anwendbaren branchenspezifischen Anforderungen eingerichtet sein. Das Rahmenwerk zur Sicherheitssteuerung muss erstellt, dokumentiert, genehmigt und implementiert werden. Dies beinhaltet auch administrative, technische und physische Sicherheitsmaßnahmen, um Ressourcen und Daten vor Verlust, Missbrauch, unbefugtem Zugriff, Offenlegung, Änderung und Vernichtung zu schützen. Das Sicherheitsprogramm sollte unter anderem folgende Schwerpunkte enthalten: • Informations- und Cyber-Sicherheitsrichtlinien, -verfahren und ein entsprechendes Standardprogramm, mit dem die umzusetzenden Informations- und Cyber-Sicherheitsrichtlinien und -standards effektiv erstellt, implementiert und ihre Wirksamkeit gemessen werden kann. • Ein umfassendes Sicherheitsprogramm mit klarer Führungsstruktur und Kontrolle auf Managementebene, um eine Kultur der Verantwortung und des Bewusstseins für die Sicherheit zu schaffen. • Angemessene Informations- und Cyber-Sicherheitsrichtlinien und -verfahren, die innerhalb des gesamten Unternehmens genehmigt und kommuniziert werden. • Gewährleistung, dass die Informations- und Cyber-Sicherheitsrichtlinien sowie die zugehörigen Verfahren/Standards regelmäßig (mindestens einmal jährlich oder bei signifikanten Änderungen) überprüft werden.	Wird dieses Prinzip nicht umgesetzt, gibt es bei Barclays oder seinen Lieferanten möglicherweise keine angemessene Aufsicht oder keine nachweislich vorhandene Aufsichtsfähigkeit in Sachen Informations-/Cyber-Sicherheit. Ein starkes Rahmenwerk zur Sicherheitssteuerung gibt den Ton für die Sicherheit des gesamten Unternehmens an.

	• Der Lieferant muss sicherstellen, dass seine Mitarbeitern persönlich Verantwortung für Informationen und Systeme übernehmen, indem er die entsprechende Verantwortung für kritische Geschäftsumgebungen, Informationen und Systeme festlegt und diese kompetenten Personen überträgt. • Der Lieferant koordiniert und weist den Mitarbeitern Funktionen und Verantwortlichkeiten zu, um die Wirksamkeit der Sicherheitsstrategie und des Rahmenwerks gemeinsam mit internen und externen Partnern zu implementieren, zu verwalten und zu kontrollieren. • Mindestens einmal jährlich müssen unabhängige Prüfungen und Beurteilungen durchgeführt werden, um sicherzustellen, dass das Unternehmen eventuelle Nichtkonformitäten der aufgestellten Richtlinien, Standards, Verfahren und Compliance-Verpflichtungen behebt. **Darüber hinaus muss der Lieferant gewährleisten, dass Barclays schnellstmöglich (schriftlich) informiert wird, wenn der Lieferant Gegenstand einer Fusion, einer Übernahme oder eines sonstige Eigentümerwechsels wird.**	
2. Informations-/Cyber-Sicherheitsrisikomanagement	Der Lieferant muss ein Programm zum Sicherheitsrisikomanagement aufstellen, mit dem Sicherheitsrisiken innerhalb der vom Lieferanten kontrollierten Umgebung effektiv beurteilt, gemindert und überwacht werden können. Das Risikomanagementprogramm sollte unter anderem folgende Schwerpunkte enthalten: • Der Lieferant muss ein Rahmenwerk zum Informations- und Cyber-Sicherheitsrisikomanagement einrichten und von der zuständigen Stelle (z. B. dem Vorstand oder einem seiner Gremien) genehmigen lassen. Dieses sollte in die allgemeine Geschäftsstrategie und das Rahmenwerk zum Risikomanagement eingebunden werden. • Angepasst an den Risikorahmen, müssen mindestens ein Mal pro Jahr oder in festgelegten Intervallen formelle Risikobewertungen durchgeführt oder auf ereignisgesteuerter Basis ausgelöst werden, z. B. in Reaktion auf einen	Dokumentierte Richtlinien und Standards sind unverzichtbare Elemente für das Risikomanagement und die Risikosteuerung. In ihnen wird die Einschätzung des Managements zu den Kontrollen festgelegt, die erforderlich sind, um das Informations-/Cyber-Risiko zu managen. Eine fehlende Umsetzung dieses Prinzips könnte dazu führen, dass Informationen von Barclays

	Zwischenfall oder die daraus resultierenden Erkenntnisse (und in Verbindung mit sämtlichen Änderungen an Informationssystemen), um mithilfe qualitativer und quantitativer Methoden die Wahrscheinlichkeit und die Auswirkungen aller ermittelten Risiken zu bestimmen. Die Wahrscheinlichkeit und die Auswirkungen in Zusammenhang mit inhärenten und verbleibenden Risiken müssen unabhängig und unter Berücksichtigung aller Risikokategorien (z. B. Audit-Ergebnisse, Gefahren- und Schwachstellenanalyse und Einhaltung gesetzlicher Vorschriften) ermittelt werden. • Die Ergebnisse der Risikobewertung sollten Aktualisierungen zu Sicherheitsrichtlinien, -verfahren, -standards und -kontrollen beinhalten, um sicherzustellen, dass diese relevant und effektiv bleiben und ggf. an bewährte Praktiken der Branche angepasst werden. • Unter Berücksichtigung der Risikobewertungsergebnisse sind geeigneter Optionen auszuwählen, um Informationssicherheitsrisiken zu managen. • Formulierung eines Plans zum Management der Informationssicherheitsrisiken und der Risikoakzeptanzkriterien durch entsprechend qualifizierte und verantwortliche Personen. • Durch Priorisierung der Risiken und Implementierung von Gegenmaßnahmen muss der Lieferant gewährleisten, dass die ermittelten Risiken innerhalb der Umgebung minimiert oder eliminiert werden. • Risiken müssen auf ein annehmbares Niveau abgesenkt werden. Dieses annehmbare Niveau basiert auf Risikokriterien und sollte in Übereinstimmung mit angemessenen Fristen und mit Genehmigung der Stakeholder festgelegt und dokumentiert werden. • Bei Risikobewertungen in Verbindung mit Datensteuerungsanforderungen ist Folgendes zu berücksichtigen: o Kategorisierung und Schutz der Daten vor unbefugter Verwendung, Zugriff, Verlust, Zerstörung oder Fälschung.	unrechtmäßig offengelegt werden und/oder Dienste ausfallen, was wiederum rechtliche und regulatorische Strafmaßnahmen sowie Rufschädigung zur Folge haben kann.

	○ Kenntnis, wo sensible Daten gespeichert sind und über welche Anwendungen, Datenbanken, Server und Netzwerkinfrastrukturen diese übermittelt werden. ○ Einhaltung der festgelegten Aufbewahrungsfristen und Entsorgungsauflagen am Lebensende. • Der Lieferant muss mindestens einmal jährlich, ggf. auch häufiger, eine Sicherheitsrisikobewertung in Bezug auf die Informations-/Cyber-Sicherheit und anhand der spezifischen Umgebungen durchführen. **Der Lieferant muss Barclays informieren, falls er mögliche signifikante Risikobereiche nicht mindern bzw. verringern kann, die sich auf die für Barclays erbrachten Dienste auswirken könnten.**	
3. Genehmigte Verwendung	Der Lieferant muss allgemeine Nutzungsbedingungen erstellen und veröffentlichen, die seine Mitarbeiter über ihre Verantwortlichkeiten in Kenntnis setzen. Folgende Themen sind zu berücksichtigen: • Nutzung des Internets, • Nutzung von SaaS (Software as a Service), • Nutzung von öffentlichen Code-Repositorys, • Nutzung von Browser-basierten Plugins und Freeware/Shareware, • Nutzung von Social Media, • Nutzung der Firmen-E-Mail, • Nutzung von Instant Messaging, • Nutzung von IT-Geräten, die vom Lieferanten bereitgestellt werden, • Nutzung von IT-Geräten, die nicht vom Lieferanten bereitgestellt werden (z. B. eigene Geräte der Mitarbeiter [Bring Your Own Device]), • Nutzung tragbarer/wechselbarer Speichergeräte, • Verantwortlichkeiten beim Umgang mit Informationsressourcen von Barclays, und • Output von Kanälen für Datenleckagen.	Allgemeine Nutzungsbedingungen helfen bei der Verstärkung der Kontrollumgebung zum Schutz von Informationsressourcen.

	Der Lieferant unternimmt angemessene Schritte, um die Einhaltung der allgemeinen Nutzungsbedingungen sicherzustellen.	
4. Weiterbildung und Awareness	Der Lieferant muss über ein Schulungsprogramm zur Sicherheitssensibilisierung verfügen, das für alle Mitarbeiter, Auftragnehmer und externen Benutzer der unternehmenseigenen Systeme entwickelt und ggf. vorgeschrieben wurde. Alle Personen mit Zugriff auf Barclays-Daten/-Informationen müssen, je nach beruflicher Funktion bezogen auf das Unternehmen, eine geeignete Sensibilisierungsschulung sowie regelmäßige Updates zu Geschäftsverfahren, -prozessen und -richtlinien erhalten. Das Schulungs- und Sensibilisierungsniveau muss den auszuführenden Aufgaben entsprechen und auf einer geeigneten Schulungsmanagement-Plattform protokolliert werden. Der Lieferant muss sicherstellen, dass alle ihm unterstehenden Mitarbeiter innerhalb von einem Monat nach Arbeitsbeginn im Unternehmen eine obligatorische Sicherheitsinformationsschulung absolvieren, in der sie mehr über bewährte Verfahren zur Cyber-Sicherheit und den Schutz von Barclays-Daten erfahren und die mindestens einmal jährlich aufzufrischen ist. Sofern zutreffend, sollten dabei die folgenden Schwerpunkte aufgegriffen werden: Risikogruppen, wie solche, die privilegierten Systemzugriff genießen oder sensible Geschäftsfunktionen bekleiden (darunter privilegierte Benutzer, leitende Führungskräfte, Informations- und Cyber-Sicherheitsverantwortliche oder externe Stakeholder), müssen, je nach Funktion und Verantwortlichkeiten, an einer Situationssensibilisierungsschulung in Bezug auf die Informations- und Cyber-Sicherheit teilnehmen.	Durch Weiterbildung und Awareness werden alle anderen Kontrollen im Rahmen dieses Vertragsanhangs unterstützt. Wird dieses Prinzip nicht umgesetzt, sind relevante Mitarbeiter sich der Cyber-Risiken und Angriffsvektoren nicht bewusst und wären nicht in der Lage, Angriffe zu erkennen beziehungsweise zu verhindern.
5. Management von Sicherheitsvorfällen	Der Lieferant muss ein Rahmenwerk zum Management von Cyber-Sicherheitsvorfällen aufstellen, mit dem Sicherheitsvorfälle innerhalb der Lieferantenumgebung effektiv beurteilt, eingedämmt und ausgeräumt/gemindert werden können.	Mit Hilfe eines Vorfallmanagement- und Vorfallbehandlungsprozesses wird sichergestellt, dass Vorfälle schnell in Grenzen gehalten werden

	Der Lieferant muss gewährleisten, dass schriftliche Vorfallbehandlungspläne vorliegen, in denen die Funktionen der Mitarbeiter wie auch die einzelnen Phasen von Vorfallbehandlung/-management festgelegt sind: • Beurteilung des Vorfalls – Einrichtung eines Prozesses zur Vorfallbeurteilung, in den verschiedene Datenquellen einbezogen werden und der im gesamten Unternehmen eingeführt wird, um Sicherheitsvorfälle effektiv zu beurteilen. • Klassifizierung des Vorfalls – Einrichtung eines Prozesses zur Vorfallklassifizierung, mit dem sich ein beurteilter Vorfall schnell und effektiv nach Ereignisarten klassifizieren lässt, um schnelle Maßnahmen zur Vorfallbehandlung einzuleiten. • Eindämmung des Vorfalls – Nutzung von Mitarbeiter-, Verfahrens- und Technologiekompetenzen, um einen Sicherheitsvorfall schnell und effektiv in der Umwelt einzudämmen. • Beseitigung/Minderung von Bedrohungen – Nutzung von Mitarbeiter-, Verfahrens- und Technologiekompetenzen, um eine Sicherheitsbedrohung und/oder deren Komponenten innerhalb der Umgebung schnell und effektiv zu beseitigen/zu mindern. Der Lieferant sollte versuchen, die Behandlungsmaßnahmen möglichst zu optimieren, indem er Erkenntnisse aus aktuellen und früheren Feststellungen/Behandlungsmaßnahmen einfließen lässt. Der Lieferant muss Sorge dafür tragen, dass Teams und Prozesse für die Vorfallbehandlung mindestens einmal jährlich getestet werden, um sicherzustellen, dass der Lieferant zur Behandlung von Cyber-Sicherheitsvorfällen in der Lage ist. • Bestandteil der Tests muss eine Validierung der Fähigkeit zur Benachrichtigung von Barclays sein; dies geschieht durch den Nachweis der Fähigkeit, die entsprechenden Personen zu kontaktieren. • Kommunikation – Der Lieferant muss einen Ansprechpartner für eventuelle Sicherheitsvorfälle ernennen, der bei einem auftretenden Vorfall mit Barclays	und verhindert wird, dass sie sich ausweiten.

	zusammenarbeitet. Der Lieferant muss Barclays die Kontaktdaten dieser Person(en) und alle eventuellen Änderungen mitteilen, einschließlich Geschäftszeiten und Telefonnummern. **Die Angaben müssen Folgendes beinhalten: Name, Verantwortlichkeiten innerhalb des Unternehmens, Funktion, E-Mail-Adresse und/oder Telefonnummer** Nach Feststellung eines Vorfalls, der sich auf den für Barclays erbrachten Dienst bzw. Barclays-Informationen/-Daten auswirkt, muss der Lieferant Barclays innerhalb einer angemessenen Frist informieren, in jedem Fall aber maximal **zwei (2) Stunden**, nachdem der Lieferant vom Vorfall Kenntnis erlangt hat. Im Fall einer entweder vermuteten oder tatsächlichen Datenschutzverletzung muss der Lieferant Barclays gemäß den im betroffenen Land geltenden Datenschutzanforderungen darüber informieren. Der Lieferant legt Barclays einen Bericht über jedweden Vorfall vor, der sich auf den für Barclays erbrachten Dienst bzw. Barclays-Informationen/-Daten auswirkt. Der Bericht muss folgende Angaben enthalten: • Datum und Uhrzeit • Ort • Art des Zwischenfalls • Auswirkungen • Status • Schadensminderung oder eingeleitete Maßnahmen Diese Vorfälle sind dem Barclays Supplier Manager und dem Barclays Joint Operations Centre innerhalb des **Barclays Chief Security Office (CSO) Joint Operations Centre (JOC) – gcsojoc@barclays.com –** zu melden.	

6. Klassifizierung und Schutz von Informationen	Der Lieferant muss über ein etabliertes und angemessenes Rahmenwerk/Programm zur Informationsklassifizierung und -handhabung (angepasst an bewährten Praktiken der Branche und/oder die Anforderungen von Barclays) verfügen, das folgende Komponenten abdeckt: • Zuweisung des korrekten Kennzeichnungsschemas für Informationen. • Sichere Handhabung der Informationen gemäß ihrer jeweiligen Klassifizierungsstufe. • Sicherstellung, dass alle Mitarbeiter mit den Kennzeichnungs- und Handhabungsanforderungen des Lieferanten/von Barclays vertraut sind und wissen, wie die korrekte Informationsklassifizierung richtig anzuwenden ist. Der Lieferant muss sich auf das Barclays-Kennzeichnungsschema für Informationen und die Anforderungen an die Handhabung (Anhang B, Tabelle B1 und B2) oder ein alternatives Schema berufen, um zu gewährleisten, dass sämtliche von ihm verwahrten oder verarbeiteten Barclays-Informationen gesichert und geschützt werden. Diese Anforderung gilt für sämtliche im Auftrag von Barclays verwahrten oder verarbeiteten Informationsressourcen.	Es sind angemessene, effektiv durchgeführte Kontrollen nötig, damit vertrauliche Informationen von Barclays auf Personen beschränkt werden, die darauf zugreifen dürfen (Vertraulichkeit), vor unbefugten Änderungen geschützt sind (Unversehrtheit) und bei Bedarf abgerufen und vorgehalten werden können (Verfügbarkeit). Werden diese Anforderungen nicht erfüllt, besteht die Gefahr, dass vertrauliche Informationen von Barclays durch unbefugte Änderungen, Offenlegung, Zugriff, Beschädigung, Verlust oder Vernichtung gefährdet sind, was wiederum rechtliche und regulatorische Strafmaßnahmen sowie Rufschädigung und Verluste bzw. Unterbrechungen von Geschäftsprozessen zur Folge haben kann.
7. Ressourcenmanageme	Der Lieferant muss sicherstellen, dass über den gesamten Lebenszyklus der Ressourcen hinweg ein effektives Programm zum Ressourcenmanagement eingerichtet ist. Das Ressourcenmanagement muss den Lebenszyklus der Ressourcen steuern – von der	Eine vollständige und genaue Bestandsliste der Informationsressourcen ist

nt (Hardware & Software)	Beschaffung bis hin zur Außerbetriebnahme – und so über alle Ressourcenklassen in der Umgebung hinweg für Transparenz und Sicherheit sorgen. Der Lieferant muss eine vollständige und genaue Bestandsliste aller geschäftskritischen Ressourcen führen, die sich an sämtlichen Standorten bzw. Regionen befinden, an denen Dienste für Barclays erbracht werden, darunter auch Barclays-Ausrüstung, die in den Räumlichkeiten des Lieferanten bzw. eines Unterauftragsnehmers des Lieferanten gehostet oder von Barclays bereitgestellt wird, und sicherstellen, dass diese mindestens einmal jährlich überprüft wird, um zu validieren, dass die Bestandsliste der Informationsressourcen aktuell, vollständig und genau ist. Der Prozess zum Ressourcenmanagement sollte die folgenden Bereiche abdecken: • Informationsressourcen und -infrastrukturen, die je nach Klassifizierung, Kritikalität und Geschäftswert geschützt werden. • Pflege einer genauen und aktuellen Bestandsliste aller technischen Ressourcen, mit deren Hilfe Informationen gespeichert oder verarbeitet werden können. Diese Bestandsliste muss sämtliche Ressourcen beinhalten, ungeachtet dessen, ob sie mit dem Unternehmensnetzwerk verbunden sind oder nicht (je nach Barclays-Dienst). • **Lieferanten mit Tier-1-, Tier-2- oder Tier-3-Spezifikation müssen aktuelle, vollständige und genaue Ressourcen-Bestandslisten führen (einschließlich Desktop-PCs, Laptops, Netzwerk-Ausstattung, RSA-Token oder von Barclays bereitgestellte Ressourcen).** • Gewährleistung, dass nicht genehmigte Ressourcen entweder aus dem Netzwerk entfernt bzw. unter Quarantäne gestellt werden oder dass die Bestandsliste schnellstmöglich aktualisiert wird. • Pflege einer aktuellen Liste der gesamten genehmigten Software, die zur Erbringung des Dienstes für Barclays benötigt wird. • Gewährleistung, dass nur aktuell unterstützte und vom Lieferanten regelmäßig aktualisierte Software-Anwendungen oder Betriebssysteme in den genehmigten	unverzichtbar, um sicherzustellen, dass die Kontrollen angemessen sind. Wird dieses Prinzip nicht umgesetzt, könnten Ressourcen von Barclays oder von Lieferanten zur Erbringung von Leistungen für Barclays genutzte Ressourcen beeinträchtigt werden, was finanzielle Verluste, Datenverlust, Rufschädigung und Rügen von Aufsichtsbehörden nach sich ziehen kann.

	Software-Bestand des Unternehmens aufgenommen werden. Nicht unterstützte Software muss im Bestandssystem als „nicht unterstützt" gekennzeichnet werden. Der Lieferant muss sicherstellen, dass effektive und effiziente Verfahren implementiert werden, um nicht unterstützte Technologien zu reduzieren sowie Lebensende, Außerbetriebnahme und Vernichtung von Ressourcen und Daten zu managen und so das Risiko einer Datenkompromittierung zu minimieren.	
8. Vernichtung/Löschung /Außerbetriebnahme von physischen und logischen Informationen	Bei Informationsressourcen von Barclays, ob in physischer oder elektronischer Form gespeichert, muss im Falle der Vernichtung oder Löschung auf sichere und dem damit verbundenen Risiko entsprechende Art und Weise vorgegangen werden, damit keinerlei Barclays-Daten wiederherstellbar sind. Der Lieferant muss Richtlinien und Verfahren mit unterstützenden Geschäftsprozessen und technischen Maßnahmen einrichten, die zur sicheren Entsorgung und vollständigen Entfernung von Barclays-Daten von allen Speichermedien angewendet werden und sicherstellen sollen, dass sich keinerlei Daten durch beliebige computerforensische Mittel wiederherstellen lassen.	Die sichere Vernichtung von Informationsressourcen hilft dabei, sicherzustellen, dass Informationsressourcen von Barclays nicht im Zusammenhang mit Datenschutzverletzungen, Datenverlust oder böswilligen Aktivitäten wiederherstellbar sind.
9. Perimeter- und Netzwerksicherheit	Der Lieferant muss sicherstellen, dass sämtliche vom Lieferanten oder von dessen Unterauftragnehmern betriebenen IT-Systeme, mit denen für Barclays erbrachte Dienste unterstützt werden, vor Seitwärtsbewegungen von Bedrohungen im Netzwerk des Lieferanten (und jeglicher relevanter Unterauftragnehmer) geschützt sind. Der Lieferant muss die Informationsübermittlung über Netzwerke mit unterschiedlichen Vertraulichkeitsstufen hinweg erkennen/verhindern/korrigieren und sich dabei insbesondere auf sicherheitsgefährdende Daten konzentrieren. Mechanismen zur Netzwerkintegrität sollten die folgenden Bereiche abdecken: • Pflege einer aktuellen Bestandsliste aller Netzwerkperimeter des Unternehmens (in Form eines Netzwerkplans/-diagramms).	Bei Nichtbeachtung dieses Prinzips könnten externe oder interne Netzwerke durch Angreifer unterwandert werden, die sich dadurch Zugang zum Dienst bzw. den damit verbundenen Daten verschaffen wollen.

	• Aufbau und Implementierung des Netzwerks müssen mindestens ein Mal pro Jahr oder bei Eintritt eines Ereignisses, das Änderungen nach sich zieht, geprüft werden. • Externe Verbindungen zum Lieferantennetzwerk werden dokumentiert, durch eine Firewall geleitet und vor ihrer Aktivierung geprüft und genehmigt, um Sicherheitsverletzungen zu verhindern. • Die Netzwerke des Lieferanten werden durch Anwendung von „Defense-in-Depth"-Prinzipien geschützt (z. B. Netzwerksegmentierung, Firewalls, physische Zugriffskontrollen auf die Netzwerkausrüstung usw.). • Der Lieferant muss über Technologien zur Verhinderung von Netzwerkzugriffen verfügen, um bösartigen Datenverkehr zu erkennen und vom Netzwerk fernzuhalten. • Einsatz starker Netzwerk-Firewall-Funktionen, um eine Perimeterabwehr zum Schutz vor bösartigen Netzwerkangriffen zu schaffen. • Der gesamte Netzwerk-Datenverkehr ins oder aus dem Internet läuft über einen authentifizierten Proxyserver auf Anwendungsebene, der so konfiguriert ist, dass er unbefugte Verbindungen herausfiltert. • Netzwerkgeräte werden sicher verstärkt, um bösartige Angriffe zu verhindern. • Logische Trennung der Gerätemanagement-Ports/-Schnittstellen vom Datenverkehr der Benutzer; angemessene Authentifizierungskontrollen. • Alle Konfigurationsregeln, die den Datenverkehr über Netzwerkgeräte erlauben, müssen in einem Konfigurationsmanagementsystem zusammen mit einem spezifischen Geschäftsgrund für jede Regel dokumentiert werden. • Kommunikation über nicht genehmigte TCP- oder UDP-Ports bzw. Datenverkehr über Anwendungen muss abgewiesen werden, um sicherzustellen, dass an allen Netzwerkperimetern des Unternehmens nur autorisierte Protokolle in das Netzwerk hinein oder aus dem Netzwerk heraus gelangen können.	

	• Durchführung regelmäßiger Scans von außerhalb der Perimeter jedes vertrauenswürdigen Netzwerks, um alle unbefugten Verbindungen zu erkennen, die über die Perimeter zugänglich sind. • Sicherung der Kommunikation zwischen Geräten und Managementstationen/-konsolen. • Konfiguration der Überwachungssysteme, um Netzwerkpakete zu protokollieren, welche die Grenzen an allen Netzwerkperimetern des Unternehmens passieren. • Die Netzwerkverbindung zwischen einzelnen Büros/Cloud-Serviceprovider/Datenzentren muss über ein sicheres Protokoll verschlüsselt werden. Barclays-Daten, die innerhalb des lieferantenseitigen Wide Area Network (WAN) übermittelt werden, sind zu verschlüsseln. • Der Lieferant muss die Firewall-Regeln (für externe und interne Firewalls) in jährlichen Abständen prüfen. • Jeder drahtlose Zugang zum Netzwerk wird durch Protokolle zur Autorisierung, Authentifizierung, Segmentierung und Verschlüsselung überwacht, um Sicherheitsverletzungen zu vermeiden. • Der Lieferant muss durch angemessene Netzwerkzugriffskontrollen sicherstellen, dass der Zugriff auf das interne Netzwerk überwacht werden muss und nur Geräte mit entsprechender Berechtigung erlaubt sind. • Für den Remotezugriff auf das Lieferantennetzwerk muss eine Multifaktor-Authentifizierung erfolgen. Der Lieferant muss gewährleisten, dass alle Server, die zur Erbringung des Dienstes für Barclays genutzt werden, nicht über nicht vertrauenswürdige Netzwerke (Netzwerke außerhalb Ihrer Sicherheitsperimeter, die sich Ihrer administrativen Kontrolle entziehen, z. B. mit Internetverbindung) laufen, und dass angemessene Sicherheitskontrollen durchgeführt werden. Der Lieferant, der Barclays-Informationen in einem Datenzentrum oder einer Cloud hostet (gilt auch für Unterauftragnehmer), muss eine gültige Zertifizierung nach ISO/IEC 27001	

	und/oder SOC 1 bzw. 2 zum Sicherheitsmanagement besitzen (oder Zertifizierungen, die äquivalente Kontrollen belegen, gestützt durch den Bericht eines unabhängigen Gutachters). T2- und T3-Netzwerk – • T2-Netzwerke müssen durch eine Firewall logisch vom Unternehmensnetzwerk des Lieferanten getrennt und der gesamte ein- und ausgehende Datenverkehr muss beschränkt und überwacht werden. • Routing-Konfigurationen müssen sicherstellen, dass Verbindungen nur zum Netzwerk von Barclays und nicht zu beliebigen anderen Lieferantennetzwerken geleitet werden. • Der Edge-Router des Lieferanten, der sich mit den Extranet-Gateways von Barclays verbindet, muss sicher konfiguriert werden und einem Konzept der Beschränkungskontrollen für Ports, Protokolle und Dienste folgen. o Sicherstellung, dass Protokollierung und Überwachung aktiviert sind. *Anm.: Als „Netzwerk" wird in dieser Kontrolle jedes nicht zu Barclays gehörige Netzwerk bezeichnet, für das der Lieferant verantwortlich ist, darunter auch Netzwerke von Subunternehmen des Lieferanten.*	
10. DoS-Erkennung	Der Lieferant muss in der Lage sein, DoS-Attacken (Denial of Service, Überlastangriffe) oder DDoS-Attacken (Distributed Denial of Service, verteilte Überlastangriffe) zu erkennen und sich vor diesen zu schützen. Der Lieferant muss dafür sorgen, dass mit dem Internet verbundene oder externe Kanäle zur Unterstützung der für Barclays erbrachten Dienste mit einem hinreichenden DoS-Schutz versehen sind, um die Verfügbarkeit sicherzustellen.	Wird dieses Prinzip nicht umgesetzt, sind Barclays und Lieferanten von Barclays möglicherweise nicht in der Lage, zu verhindern, dass ein DoS-Angriff sein Ziel erreicht.
11. Remotezugriff	Remotezugriff auf das Barclays-Netzwerk über die Barclays Citrix-Anwendung und/oder auf Barclays-Daten, die in einer vom Lieferanten kontrollierten Umgebung aufbewahrt/gespeichert werden, wird nicht standardmäßig gewährt und kann nicht von	Remotezugriffskontrollen helfen zu gewährleisten, dass sich keine nicht autorisierten und unsicheren Geräte

	nicht genehmigten Standorten/außerhalb des Büros/zu Hause aus hergestellt werden. Zudem muss jeder Remotezugriff von Barclays (Chief Security Office/ECAM-Team) genehmigt und autorisiert werden. Der Lieferant sorgt dafür, dass die folgenden Komponenten für den Remotezugriff gewährleistet sind: • Für den Remotezugriff auf das Lieferantennetzwerk müssen die übermittelten Daten verschlüsselt werden und es muss eine Multifaktor-Authentifizierung erfolgen. • Der Zugriff auf das Barclays-Netzwerk muss über eine Barclays Citrix-Anwendung mit von Barclays bereitgestelltem RSA-Token (Hard & Soft) erfolgen. • Der Lieferant muss eine Bestandsliste aller von Barclays bereitgestellten RSA-Token (Hard & Soft) sowie einen Managementprozess pflegen, der Prüfung und Überwachung der Zuweisung, Verwendung und Rückgabe der Token (Hard Token) beinhaltet. • Der Lieferant muss Protokoll über Mitarbeiter, die Telearbeit beantragt haben, und die jeweiligen Gründe für diesen Antrag führen. • **Der Lieferant muss in vierteljährlichen Abständen eine Abstimmung aller Remotebenutzer durchführen und Barclays (Chief Security Office/ECAM-Team) eine entsprechende Bescheinigung vorlegen.** • Auf Benachrichtigung, dass kein Zugriff mehr benötigt wird (z. B. aufgrund von Mitarbeiterkündigung, Projektneuzuweisung usw.), deaktiviert Barclays die entsprechenden Authentifizierungsdaten innerhalb von **vierundzwanzig (24) Stunden**. • Darüber hinaus deaktiviert Barclays umgehend Authentifizierungsdaten, die über einen bestimmten Zeitraum hinweg nicht verwendet wurden (dieser Zeitraum der Nichtverwendung beträgt maximal einen Monat).	aus der Ferne mit der Barclays-Umgebung verbinden.

<table>
<tr>
<td></td>
<td>

Der Lieferant muss sicherstellen, dass Endpunkte, über die sich aus der Ferne mit Barclays-Informationssystemen verbunden wird, sicher konfiguriert werden (z. B. Patch-Ebene, Anti-Malware-Status usw.).
Dienste mit Remote-Druckerzugriff über eine Barclays Citrix-Anwendung müssen von Barclays (Chief Security Office/ECAM-Team) genehmigt und autorisiert werden. Der Lieferant muss Protokoll führen und eine vierteljährliche Abstimmung durchführen.
Persönlichen Geräten/BYOD darf kein Zugriff auf die Barclays-Umgebung und/oder Barclays-Daten gewährt werden, die in einer vom Lieferanten kontrollierten Umgebung aufbewahrt/gespeichert werden (dazu zählen Mitarbeiter, Berater, Leiharbeiter, Auftragnehmer und Managed Service Partner des Lieferanten).

Anmerkung: Der Remotezugriff auf das Barclays-Netzwerk und Barclays-Daten ist nur mit ausdrücklicher Genehmigung und Autorisierung durch Barclays erlaubt.
</td>
<td></td>
</tr>
<tr>
<td>12. Management von Sicherheitsprotokollen</td>
<td>
Der Lieferant muss sicherstellen, dass ein etabliertes und unterstützendes Rahmenwerk zum Prüf- und Protokollmanagement vorliegt, welches bestätigt, dass wichtige IT-Systeme, einschließlich Anwendungen, Netzwerk-Ausrüstung, Sicherheitsvorrichtungen und Server, so eingestellt sind, dass sie signifikante Ereignisse protokollieren. Diese Protokolle wiederum müssen von Lieferanten zentralisiert, angemessen gesichert und mindestens 12 Monate lang aufbewahrt werden.
<table>
<tr><th>Kategorie</th><th>Systeme/Dienste mit geringen Auswirkungen</th><th>Systeme/Dienste mit mittleren Auswirkungen</th><th>Systeme/Dienste mit hohen Auswirkungen</th></tr>
<tr><td>Aufbewahrung von Protokollen</td><td>3 Monate</td><td>6 Monate</td><td>12 Monate</td></tr>
</table>
</td>
<td>Wird diese Kontrolle nicht durchgeführt, sind Lieferanten nicht in der Lage, eine unerwünschte oder böswillige Nutzung ihrer Dienste bzw. Daten zeitnah zu erkennen und darauf zu reagieren.</td>
</tr>
</table>

	Der Prozess zum Sicherheitsprotokollmanagement sollte die folgenden Bereiche abdecken: • Der Lieferant muss Richtlinien und Verfahren zum Protokollmanagement aufstellen. • Der Lieferant muss eine Infrastruktur zum Protokollmanagement einrichten und pflegen. • Der Lieferant muss die Funktionen und Verantwortlichkeiten einzelner Mitarbeiter und Teams festlegen, die voraussichtlich am Protokollmanagement beteiligt sind. • Es müssen Prüfprotokolle von Ereignissen gesammelt, verwaltet und analysiert werden, die helfen können, Angriff zu erkennen, zu verstehen und sich davon zu erholen. • Die Systemprotokollierung muss detaillierte Informationen, wie Ursache eines Ereignisses, Datum, Benutzer, Zeitstempel, Ausgangsadressen, Zieladressen und andere nützliche Elemente beinhalten. • Beispiele für Ereignisprotokolle: o IDS/IPS, Router, Firewall, Web-Proxy, Remotezugriffssoftware (VPN), Authentifizierungsserver, Anwendungen, Datenbankprotokolle. o Erfolgreiche Anmeldungen, fehlgeschlagene Anmeldeversuche (beispielsweise falsche Benutzerkennung oder falsches Passwort), Erstellung, Änderung und Löschung von Benutzerkonten. o Konfiguration von Änderungsprotokollen. • Barclays-Dienste in Bezug auf Geschäftsanwendungen und technische Infrastruktursysteme, auf denen die Ereignisprotokollierung aktiviert werden muss, einschließlich ausgelagerter oder „in der Cloud" befindlicher Lösungen. • Analyse sicherheitsspezfischer Ereignisprotokolle (einschließlich Normalisierung, Aggregation und Korrelation). • Synchronisierung der Zeitstempel in Ereignisprotokollen anhand einer gemeinsamen, vertrauenswürdigen Quelle.	

	• Schutz sicherheitsspezfischer Ereignisprotokolle (z. B. durch Verschlüsselung, Zugriffskontrolle und Sicherungskopien). • Einleitung notwendiger Maßnahmen, um alle eventuell festgestellten Probleme zu beheben und auf Cyber-Sicherheitsvorfälle schnell und effektiv zu reagieren. • Nutzung von SIEM- (Security Information and Event Management) oder Protokollanalysetools zur Korrelation und Auswertung der Protokolle. • Gegebenenfalls Nutzung von Tools, um in Echtzeit eine zentralisierte Aggregation und Korrelation anomaler Aktivitäten, Netzwerk- und Systemwarnungen sowie relevanter Ereignis- und Cyber-Bedrohungsinformationen aus unterschiedlichen Quellen durchzuführen, einschließlich sowohl interner als auch externer Quellen, um facettenreiche Cyber-Angriffe besser zu erkennen und zu verhindern. Zu den wichtigen protokollierten Ereignissen müssen jene gehören, die potenziell die Vertraulichkeit, Integrität und Verfügbarkeit der für Barclays bereitgestellten Dienste beeinflussen könnten und die zur Identifizierung oder Untersuchung wesentlicher Vorfälle und/oder Zugriffsrechtsverletzungen bezüglich der Lieferantensysteme beitragen können.	
13. Malware-Abwehr	Der Lieferant muss Richtlinien und Verfahren aufgestellt sowie unterstützende Geschäftsprozesse und technische Maßnahmen implementiert haben, um der Ausführung von Malware auf unternehmenseigenen oder -verwalteten Benutzerendgeräten (d. h. eingerichteten Arbeitsplätzen, Laptops und mobilen Geräten) und Netzwerk- bzw. Systemkomponenten der IT-Infrastruktur vorzubeugen. Der Lieferant muss sicherstellen, dass alle entsprechenden IT-Ressourcen jederzeit mit Malware-Schutz versehen sind, damit Störungen des Dienstes und Verletzungen der Sicherheit verhindert werden. Der Malware-Schutz sollte Folgendes beinhalten bzw. umfassen: • Zentral verwaltete Anti-Malware-Software, um alle Arbeitsplätze und Server des Unternehmens kontinuierlich zu überwachen und zu schützen.	Anti-Malware-Lösungen sind für den Schutz der Informationsressourcen von Barclays vor Schadcode unerlässlich.

	• Gewährleistung, dass die unternehmenseigenenAnti-Malware-Software regelmäßig auch ihre Scan Engine und Signaturdatenbank aktualisiert. • Versendung aller erkannten Malware-Ereignisse zur Analyse und Warnung an die unternehmenseigenen Anti-Malware-Administrationstools und Ereignisprotokollserver. • Der Lieferant muss angemessene Kontrollen einrichten, um vor mobiler Malware und Angriffen auf mobile Geräte zu schützen, die sich mit den Netzwerken von Barclays oder des Lieferanten verbinden und auf Barclays-Daten zugreifen. Hinweis: Anti-Malware muss (unter anderem) unerlaubten mobilen Code, Viren, Spyware, Key-Logger-Software, Botnetze, Würmer, Trojaner usw. erkennen.	
14. Sichere Konfigurationsstandards	Der Lieferant muss ein Rahmenwerk einrichten, um zu gewährleisten, dass alle konfigurierbaren Systeme/Netzwerkausrüstungselemente gemäß Branchenstandards (z. B. NIST, SANS, CIS) sicher konfiguriert sind. Der Standardkonfigurationsprozess sollte die folgenden Bereiche abdecken: • Einrichtung von Richtlinien, Verfahren und Tools zu den Sicherheitskonfigurationsstandards für alle autorisierten Netzwerkgeräte und Betriebssysteme. • Durchführung regelmäßiger (jährlicher) Umsetzungsprüfungen, um sicherzustellen, dass eine eventuelle Nichteinhaltung der grundlegenden Sicherheitsstandards umgehend korrigiert wird. Es gibt eine angemessene Prüfung und Überwachung, um die anhaltende Integrität der Builds/Geräte zu gewährleisten. • Systeme und Netzwerkgeräte sind so zu konfigurieren, dass sie gemäß den Sicherheitsprinzipien funktionieren (z. B. Konzept der Beschränkungskontrollen für Ports, Protokolle und Dienste sowie keine nicht autorisierte Software).	Standardmäßige Build-Kontrollen helfen, Informationsressourcen vor unbefugtem Zugriff zu schützen. Die Einhaltung von Standard-Builds und Kontrollen, die sicherstellen, dass Änderungen genehmigt sind, hilft dabei, die Informationsressourcen von Barclays zu schützen.

	Sicherstellung, dass das Konfigurationsmanagement sichere Konfigurationsstandards über alle Ressourcenklassen hinweg steuert und Konfigurationsänderungen bzw. -abweichungen erkennt, meldet und effektiv darauf reagiert.	
15. Endpunkt-Sicherheit	Der Lieferant muss sicherstellen, dass die für den Zugriff auf das Barclays-Netzwerk oder für den Zugriff auf bzw. die Verarbeitung von Barclays-Daten verwendeten Endpunkte zum Schutz vor Angriffen verstärkt werden. Das Endpunkt-Sicherheitskonzept muss Folgendes beinhalten: • Datenträgerverschlüsselung. • Deaktivierung aller nicht benötigten Softwareprogramme/Dienste/Ports. • Deaktivierung der Administratorrechte für lokale Benutzer. • Die Mitarbeiter des Lieferanten dürfen keine grundlegenden Einstellungen wie Standard-Service-Pack, Systempartition, Standarddienste usw. ändern. • USB-Ports müssen deaktiviert werden, um das Kopieren von Barclays-Daten auf externe Datenträger zu unterbinden. • Virenschutzsignaturen und Sicherheitspatches sind stets auf die neueste Version zu aktualisieren. • Eingeschränkter Schutz vor Datenverlust, damit keinerlei Barclays-Daten ausgeschnitten/kopiert/eingefügt bzw. Screenshots davon erstellt werden können. • Der Druckerzugriff muss standardmäßig deaktiviert sein. • Der Lieferant sollte den Zugriff auf soziale Netzwerke, Webmail-Dienste und Websites beschränken, über die Informationen im Internet gespeichert werden können, wie beispielsweise Google Drive, Dropbox oder iCloud. • Der Austausch/die Übertragung von Barclays-Daten über Instant-Messaging-Tools/-Software sollte deaktiviert werden. • Möglichkeiten und Prozesse, um unzulässige, als bösartig identifizierte Software zu erkennen und die Installation unzulässiger Software zu verhindern.	Wird diese Kontrolle nicht umgesetzt, sind das Netzwerk und Endpunkte von Barclays und dem Lieferanten möglicherweise für Cyber-Angriffe anfällig.

	Hinweis: Wechseldatenträger/tragbare Geräte sollten standardmäßig deaktiviert und nur zu legitimen Geschäftszwecken erlaubt werden. Gemäß den genehmigten Konfigurationsstandards des Unternehmens muss der Lieferant sichere Abbildungen oder Vorlagen für alle Systeme im Unternehmen aufbewahren. Jedes neu eingerichtete oder bestehende System, das kompromittiert wird, sollte mithilfe einer dieser Abbildungen oder Vorlagen abgebildet werden. Mobile Geräte, die für Barclays-Dienste genutzt werden – 1. Um das Risiko einer Datenkompromittierung zu senken, muss der Lieferant MDM-Möglichkeiten (Mobile Device Management) implementieren, um mobile Geräte, die Zugriff auf klassifizierte Barclays-Informationen haben bzw. diese enthalten, über ihren gesamten Lebenszyklus hinweg sicher kontrollieren und verwalten zu können. 2. Der Lieferant muss sicherstellen, dass Möglichkeiten zur Remotesperrung und -löschung mobiler Geräte eingerichtet sind, um die Informationen im Falle von Verlust, Diebstahl oder kompromittierten Geräten zu schützen. 3. Verschlüsselung mobiler Gerätedaten (Barclays-Daten). 4. Auf vom Lieferanten bereitgestellten Geräten sollten standardmäßig keinerlei Cloud-basierte Dienste erlaubt sein.	

16. Verhinderung von Datenleckagen	Der Lieferant muss ein Rahmenwerk einrichten, um den Schutz vor unrechtmäßigen Datenleckagen zu gewährleisten. Dieser Schutz sollte (unter anderem) die folgenden Kanäle für Datenleckagen umfassen:
	
	• Unzulässige Übertragung von Informationen außerhalb des internen Netzwerks bzw. außerhalb des Lieferantennetzwerks.
	  ○ E-Mail
	  ○ Internet-/Web-Gateway (einschließlich Online-Speicher und Webmail).
		Es sind angemessene, effektiv durchgeführte Kontrollen nötig, damit Informationen von Barclays auf den Personenkreis eingeschränkt werden, die darauf zugreifen dürfen (Vertraulichkeit), vor unbefugten Änderungen geschützt sind

	• Verlust oder Diebstahl von Informationsressourcen von Barclays, die sich auf tragbaren elektronischen Medien befinden (darunter Informationen in elektronischer Form auf Laptops, Mobilgeräten sowie tragbaren Medien). • Unzulässige Übertragung von Informationen auf tragbare Medien. • Unsicherer Austausch von Informationen mit Dritten (Subunternehmen). • Unangebrachtes Ausdrucken oder Kopieren von Informationen.	(Unversehrtheit) und bei Bedarf abgerufen und vorgehalten werden können (Verfügbarkeit). Werden diese Anforderungen nicht erfüllt, besteht die Gefahr, dass vertrauliche Informationen von Barclays durch unbefugte Änderungen, Offenlegung, Zugriff, Beschädigung, Verlust oder Vernichtung gefährdet sind, was wiederum rechtliche und regulatorische Strafmaßnahmen sowie Rufschädigung und Verluste bzw. Unterbrechungen von Geschäftsprozessen zur Folge haben kann.
17. Datenschutz	Der Lieferant muss dafür sorgen, dass Barclays-Daten, die sich in der Obhut/im Netzwerk des Kunden befinden, einen angemessenen Datenschutz genießen, der durch eine Kombination aus Maßnahmen zur Verschlüsselung, zum Integritätsschutz und zum Schutz vor Datenverlust erreicht wird. Es ist unbedingt angemessene Sorgfalt geboten, um den Zugriff auf die Daten von Barclays zu beschränken. Die Datenschutzkontrollen sollten die folgenden Bereiche abdecken: 1. Richtlinien und Verfahren sollten eingerichtet sowie unterstützende Geschäftsprozesses und technische Maßnahmen implementiert werden, um beispielsweise Datenströme für Daten zu erfassen, zu dokumentieren und zu pflegen, die sich (dauerhaft oder vorübergehend) in den geografisch verteilten (physischen und virtuellen) Anwendungen sowie Infrastrukturnetzwerk- und Systemkomponenten des Dienstes befinden und/oder mit anderen Drittparteien geteilt werden. 2. Pflege eines Bestandsverzeichnisses aller vom Lieferanten gespeicherten, verarbeiteten oder übermittelten sensiblen Informationen (Barclays-Daten). 3. Aufstellung eines Standards zur Datenklassifizierung, um sicherzustellen, dass sensible Informationen (Barclays-Daten) ordnungsgemäß klassifiziert und geschützt werden. 4. Gewährleistung, dass alle Daten innerhalb des Unternehmens gemäß diesem Standard zur Datenklassifizierung gekennzeichnet werden. 5. Richtlinie zur Datennutzung – Datenzugriff	

	6. Schutz von archivierten Daten; a. Archivierte Daten sind zu verschlüsseln, um einen Missbrauch sensibler Informationen durch unbefugten Zugriff zu verhindern. 7. Überwachung der Datenbank-Aktivitäten; a. Datenbank-Zugriff und -Aktivitäten sind zu überwachen, um bösartige Aktivitäten schnell und effektiv zu erkennen. 8. Schutz von im Gebrauch befindlichen Daten; a. Abruf und Nutzung sensibler Daten sind unbedingt mittels Zugriffsmanagement zu kontrollieren, um dem Missbrauch sensibler Informationen vorzubeugen. b. Einsatz von Technologien zur Datenmaskierung und -verschleierung, um sensible, im Gebrauch befindliche Daten effektiv vor versehentlicher Preisgabe und/oder böswilliger Verwendung zu schützen. 9. Schutz von übermittelten Daten; a. Nutzung effektiver Verschlüsselungstechniken, um den Schutz der Daten während ihrer Übermittlung zu gewährleisten. b. Die Verschlüsselung von übermittelten Daten geschieht in der Regel mithilfe von Transport- oder Nutzlastverschlüsselung (der Nachricht oder selektiver Felder). Zu den Mechanismen zur Transportverschlüsselung zählen unter anderem: • Transport Layer Security (TLS) • Secure Tunneling (IPsec) • Secure Shell (SSH) c. Die Transportsicherheitsprotokolle müssen so konfiguriert werden, dass eine Verhandlung schwächerer Algorithmen und/oder kürzerer Schlüssellängen verhindert wird, wenn beide Endpunkte die stärkere Option unterstützen.	

	10. Datensicherung – a. Es müssen Vorkehrungen getroffen werden, um sicherzustellen, dass Informationen unter Einhaltung der mit Barclays vereinbarten Anforderungen angemessen durch Backups gesichert werden und wiederherstellbar sind. b. Die Sicherungskopien müssen während ihrer Speicherung bzw. Bewegung innerhalb des Netzwerks ordnungsgemäß mittels physischer Sicherheitsvorkehrungen oder Verschlüsselungstechniken geschützt werden. Dies umfasst Remotesicherungen und Cloud-Dienste. c. Auch ist sicherzustellen, dass alle Barclays-Daten in regelmäßigen Abständen automatisch gesichert werden.	
18. Sicherheit von Anwendungssoftware	Der Lieferant muss mithilfe sicherer Codierungsverfahren und in einer sicheren Umgebung Anwendungen entwickeln. Wenn der Lieferant Anwendungen entwickelt, die der Nutzung durch Barclays dienen oder zur Unterstützung des für Barclays erbrachten Dienstes genutzt werden, muss der Lieferant einen sicheren Entwicklungsrahmen aufstellen, um Sicherheitsverletzungen vorzubeugen sowie während des Entwicklungsprozesses Schwachstellen im Code zu identifizieren und zu beheben. Die Sicherheit von Anwendungssoftware sollte die folgenden Bereiche abdecken:	Kontrollen zum Schutz der Anwendungsentwicklung helfen, dafür zu sorgen, dass Anwendungen beim Einsatz geschützt sind.

	• Zur Vorbeugung von Sicherheitslücken und Dienstunterbrechungen und zum gleichzeitigen Schutz vor möglichen bekannten Schwachstellen müssen sichere Codierungsstandards gemäß den bewährten Praktiken der Branche eingerichtet und angewendet werden. • Entwicklung sicherer Codierungsverfahren gemäß der jeweiligen Programmiersprache. • Sämtliche Entwicklungen müssen in einer Nicht-Produktionsumgebung durchgeführt werden. • Einrichtung separater Umgebungen für Produktions- und Nicht-Produktionssysteme. Entwicklern sollte kein unbeaufsichtigter Zugang zu Produktionsumgebungen gewährt werden. • Aufgabentrennung für Produktions- und Nicht-Produktionsumgebungen. • Systeme werden in Übereinstimmung mit bewährten sicheren Entwicklungsmethoden (z. B. OWASP) entwickelt. • Code muss sicher gespeichert und einer Qualitätssicherung unterzogen werden. • Nach Abschluss der Tests und Weiterleitung in die Produktion muss der Code ordnungsgemäß vor unbefugter Modifizierung geschützt werden. • Für die vom Lieferanten entwickelte Software dürfen nur aktuelle und vertrauenswürdige Drittkomponenten genutzt werden. • Anwendung statischer und dynamischer Analysetools, um zu verifizieren, dass sichere Codierungsverfahren eingehalten wurden. • Der Lieferant gewährleistet, dass in Nicht-Produktionsumgebungen keine Live-Daten (einschließlich personenbezogener Daten) genutzt werden. • Anwendungen und Programmierschnittstellen (APIs) müssen gemäß führenden Branchenstandards (z. B. OWASP für Webanwendungen) gestaltet, entwickelt, bereitgestellt und getestet werden. Der Lieferant sollte Webanwendungen mithilfe von Web Application Firewalls (WAF) schützen, die den gesamten Datenverkehr, der die Webanwendung erreicht, auf geläufige Webanwendungsangriffe prüfen. Für nicht-webbasierte Anwendungen sollten spezifische Anwendungsfirewalls genutzt werden, sofern für die jeweilige Anwendungsart verfügbar.	

	Ist der Datenverkehr verschlüsselt, sollte das Gerät entweder hinter der Verschlüsselung positioniert werden oder in der Lage sein, den Datenverkehr vor der Analyse zu entschlüsseln. Ist keine Option zutreffend, sollte eine Host-basierte Web Application Firewall verwendet werden.	

19. Logische Zugriffsverwaltung (Logical Access Management (LAM))	Der Zugriff auf Informationen muss eingeschränkt sein und unter gebührender Berücksichtigung der Grundsätze des Wissensbedarfs, der Minimalberechtigung und der Aufgabentrennung erfolgen. Dem Verantwortlichen für die Informationsressource obliegt die Entscheidung darüber, wer welchen Zugriff benötigt. • Der Grundsatz des Wissensbedarfs besagt, dass Personen nur auf Informationen Zugriff haben sollten, deren Kenntnis sie zur Erfüllung der ihnen ordnungsgemäß übertragenen Aufgaben benötigen. Wenn zum Beispiel ein Mitarbeiter nur Umgang mit Kunden im Vereinigten Königreich hat, besteht bei ihm kein Wissensbedarf in Bezug auf Informationen zu Kunden in den USA. • Der Grundsatz der Minimalberechtigung besagt, dass Personen nur den Mindestumfang an Berechtigungen haben sollten, die zur Erfüllung der ihnen ordnungsgemäß übertragenen Aufgaben erforderlich sind. Wenn zum Beispiel ein Mitarbeiter die Adresse eines Kunden einsehen, diese aber nicht ändern muss, benötigt er nach dem Grundsatz der Minimalberechtigung Nur-Lese-Zugriff. Dieser sollte dem Mitarbeiter verschafft werden, Schreib-/Lese-Zugriff hingegen nicht. • Der Grundsatz der Aufgabentrennung besagt, dass zur Verhinderung von Fehlern und Betrug mindestens zwei Einzelpersonen für die separaten Bestandteile einer Aufgabenstellung verantwortlich sind. Wenn zum Beispiel ein Mitarbeiter die Erstellung eines Kontos beantragt, sollte der Antrag nicht von ihm, sondern von einem anderen genehmigt werden. Zugriffsverwaltungsprozesse müssen gemäß den bewährten Praktiken der Branche definiert sein und Folgendes beinhalten: • Der Lieferant muss dafür sorgen, dass die Zugriffsmanagementprozesse dokumentiert werden und auf alle IT-Systeme angewandt werden (auf denen die Informationsressourcen von Barclays gespeichert bzw. verarbeitet werden) und	Angemessene LAM-Kontrollen helfen dabei, sicherzustellen, dass Informationsressourcen vor unangemessener Verwendung geschützt werden. Es sind angemessene, effektiv durchgeführte Kontrollen nötig, damit Informationen von Barclays auf den Personenkreis eingeschränkt werden, die darauf zugreifen dürfen (Vertraulichkeit), vor unbefugten Änderungen geschützt sind (Unversehrtheit) und bei Bedarf abgerufen und vorgehalten werden können (Verfügbarkeit). Werden diese Anforderungen nicht erfüllt, besteht die Gefahr, dass vertrauliche Informationen von Barclays durch unbefugte Änderungen, Offenlegung, Zugriff, Beschädigung, Verlust oder Vernichtung gefährdet sind, was wiederum rechtliche und regulatorische Strafmaßnahmen sowie Rufschädigung und Verluste bzw. Unterbrechungen von

	nach ihrer Einrichtung angemessene Kontrollen der folgenden Personengruppen bieten: Neuangestellte/Versetzte/Ausscheidende/Remotezugriff. • Damit der Prozess der Erteilung, Änderung und Aufhebung von Zugriffsrechten eine Berechtigungsstufe erhält, die den erteilten Privilegien entspricht, müssen entsprechende Berechtigungssteuerungen vorhanden sein. • Es sind geeignete Kontrollmechanismen einzurichten, damit die Zugriffsmanagementprozesse über angemessene Mechanismen zur Überprüfung der Identität verfügen. • Jedes Konto muss einer einzelnen Person zugeordnet sein, die für sämtliche mit dem Konto durchgeführten Aktivitäten verantwortlich ist. • Rezertifizierung des Zugriffs – Es müssen Kontrollmechanismen vorhanden sein, die gewährleisten, dass Zugriffsberechtigungen mindestens alle 12 Monate überprüft werden, damit diese weiterhin ihrem Zweck dienen. • Alle privilegierten Zugriffsrechte müssen mindestens im Intervall von sechs (6) Monaten überprüft werden; für den Bedarf an privilegierten Zugriffsrechten müssen angemessene Kontrollmechanismen eingerichtet sein. • Kontrollen für Personen, die in eine neue Position gewechselt sind – Die Zugriffsmöglichkeiten werden innerhalb von vierundzwanzig (24) Stunden nach dem Wechsel geändert. • Kontrollen für ausscheidende Personen – Sämtliche zum Erbringen von Diensten für Barclays verwendeten logischen Zugriffsmöglichkeiten werden innerhalb von vierundzwanzig (24) Stunden nach dem Ausscheiden entfernt. • Remotezugriff – Remotezugriffssteuerungen dürfen nur über die von Barclays (Chief Security Office/ECAM-Team) zugelassenen Mechanismen erlaubt werden, und beim Remotezugriff muss eine Multifaktor-Authentifizierung erfolgen. • Authentifizierung – Angemessene lange und komplexe Passwörter, Häufigkeit der Passwortänderungen, Multifaktor-Authentifizierung, sichere Verwaltung, von Passwörtern/Zugangsdaten und anderen Kontrollen müssen gemäß bewährten Praktiken der Branche erfolgen.	Geschäftsprozessen zur Folge haben kann.

	• Ruhende Konten – Konten, die 60 Tage in Folge oder länger nicht verwendet wurden, müssen • gesperrt/deaktiviert werden. • Passwörter für interaktive Konten sollten mindestens alle 90 Tage geändert werden und sich von den zwölf (12) vorangegangenen Passwörtern unterscheiden. • Passwörter für privilegierte Konten sollten nach jedem Gebrauch, mindestens jedoch alle 90 Tage, geändert werden. • Interaktive Konten sollten spätestens nach fünf (5) fehlgeschlagenen Versuchen in Folge deaktiviert werden.	
20. Schwachstellenmanagement	Der Lieferant muss Richtlinien und Verfahren aufgestellt sowie unterstützende Prozesse und technische Maßnahmen implementiert haben, um Schwachstellen innerhalb von unternehmenseigenen oder -verwalteten Anwendungen bzw. Infrastrukturnetzwerk- und Systemkomponenten rechtzeitig zu erkennen und so die Effizienz der implementierten Sicherheitskontrollen zu gewährleisten. Das Schwachstellenmanagement sollte die folgenden Bereiche abdecken: • Es sollten Richtlinien und Verfahren aufgestellt sowie unterstützende Prozesse und technische Maßnahmen implementiert werden, um Schwachstellen innerhalb von unternehmenseigenen oder -verwalteten Anwendungen bzw. Infrastrukturnetzwerk- und Systemkomponenten rechtzeitig zu erkennen und so die Effizienz der implementierten Sicherheitskontrollen zu gewährleisten. • Festgelegte Funktionen und Verantwortlichkeiten. • Geeignete Tools und Infrastrukturen zur Suche nach Schwachstellen. • Regelmäßige Durchführung von Schwachstellenprüfungen, die innerhalb sämtlicher Ressourcenklassen in der Umgebung effektiv bekannte und unbekannte Schwachstellen aufdecken.	Wird diese Kontrolle nicht umgesetzt, könnten Angreifer Schwachstellen innerhalb von Systemen ausnutzen, um Cyber-Angriffe auf Barclays und Lieferanten von Barclays durchzuführen.

	• Anwendung eines Risikobewertungsprozesses, um die Behebung der festgestellten Schwachstellen zu priorisieren. • Aufstellung eines Prozesses zur Validierung der Schwachstellenbehebung, um innerhalb sämtlicher Ressourcenklassen in der Umgebung schnell und effektiv die Behebung der festgestellten Schwachstellen zu prüfen. • Gewährleistung, dass Schwachstellen durch solide Korrekturmaßnahmen und Patchmanagement effektiv behoben werden, um das Risiko einer Ausnutzung der Schwachstellen zu verringern. • Regelmäßiger Abgleich der Ergebnisse aufeinanderfolgender Schwachstellenprüfungen, um zu überprüfen, ob die Schwachstellen rechtzeitig behoben wurden. Alle Sicherheitsprobleme und Schwachstellen, die wesentliche Auswirkungen auf die Hosting-Infrastruktur von Barclays oder auf die vom Lieferanten bereitgestellten Webanwendungen haben könnten, bei denen sich der Lieferant zur Inkaufnahme des Risikos entschieden hat, müssen Barclays umgehend kommuniziert/mitgeteilt und mit Barclays (Chief Security Office/ECAM-Team) schriftlich abgestimmt werden.	
21. Patchmanagement	Der Lieferant muss Richtlinien und Verfahren aufgestellt sowie unterstützende Geschäftsprozesse und technische Maßnahmen implementiert haben, um Sicherheitspatches auf unternehmensverwalteten Benutzerendgeräten (z. B. eingerichteten Arbeitsplätzen, Laptops und mobilen Geräten) und Netzwerk- bzw. Systemkomponenten der IT-Infrastruktur zu installieren. Der Lieferant muss sicherstellen, dass die aktuellsten Sicherheitspatches zeitnah in den Systemen/Ressourcen/Netzwerken/Anwendungen installiert werden und somit Folgendes gewährleistet werden kann: • Bevor er einen Patch auf Produktionssystemen installiert, muss der Lieferant alle Patches auf Systemen testen, die genau der Konfiguration der Ziel-Produktionssysteme entsprechen. Darüber hinaus ist nach jedem Patching die	Wird diese Kontrolle nicht umgesetzt, sind Dienste möglicherweise anfällig für Sicherheitsprobleme, die zur Gefährdung von Verbraucherdaten oder zum Ausfall des Dienstes führen oder andere bösartige Aktivitäten ermöglichen könnten.

	ordnungsgemäße Funktion des gepatchten Dienstes zu prüfen. Kann ein System nicht gepatcht werden, sind entsprechende Gegenmaßnahme einzuleiten. • Alle wesentlichen Änderungen im IT-Bereich vor der Implementierung müssen über einen genehmigten, stabilen Änderungsmanagementprozess protokolliert, getestet und genehmigt werden, um jede Dienstunterbrechung oder Schutzverletzung zu verhindern. • Der Lieferant muss dafür sorgen, dass Patches in Produktions- und DR-Umgebungen angewendet werden.	
22. Bedrohungssimulation / Penetrationstests / IT-Sicherheitsbewertung	Der Lieferant muss unter Einbeziehung eines unabhängigen qualifizierten Sicherheitsdienstleisters eine IT-Sicherheitsbewertung/Bedrohungssimulation durchführen, die sich auf die IT-Infrastruktur, einschließlich Notfallwiederherstellungsseite, und Webanwendungen im Zusammenhang mit dem (den) vom Lieferanten für Barclays erbrachten Dienst(en) bezieht. Dies muss mindestens einmal jährlich erfolgen, um Schwachstellen zu identifizieren, die ausgenutzt werden könnten, um die Vertraulichkeit der Daten von Barclays durch Cyberattacken zu verletzen. Alle Schwachstellen müssen vorrangig behandelt und bis zu ihrer Auflösung überwacht werden. Der Test muss in Übereinstimmung mit den bewährten Praktiken der Branche durchgeführt werden. Für Lieferantendienste, die sich auf das Hosting von Infrastrukturen/Anwendungen im Auftrag von Barclays beziehen, gilt: • Der Lieferant muss Barclays über den Umfang der Sicherheitsbewertung informieren und den Umfang mit Barclays abstimmen, insbesondere Datum/Uhrzeit für deren Start und Ende, damit Störungen bei wichtigen Aktivitäten von Barclays vermieden werden. • Jedes Problem, bei dem das Risiko in Kauf genommen wird, muss mit Barclays (Chief Security Office/ECAM-Team) abgesprochen und abgestimmt werden.	Wird diese Kontrolle nicht umgesetzt, sind Lieferanten möglicherweise nicht in der Lage, die Cyber-Bedrohungen, mit denen sie es zu tun haben, und die Angemessenheit und Stärke ihrer Abwehrmaßnahmen einzuschätzen. Die Informationen von Barclays könnten offengelegt werden und/oder Dienste ausfallen, was wiederum rechtliche und regulatorische Strafmaßnahmen sowie Rufschädigung zur Folge haben kann.

23. Kryptografie	• Grund für Kryptografie – Der Lieferant muss den Grund für die von ihm angewendeten Verschlüsselungstechnologien dokumentieren und diese überprüfen, um sicherzustellen, dass sie noch für ihren Zweck geeignet sind. • Verfahren für den Kryptografie-Lebenszyklus – Der Lieferant muss eine dokumentierte Reihe von Managementverfahren für den Kryptografie-Lebenszyklus besitzen und pflegen, in denen sämtliche Prozesse zum Schlüsselmanagement von Erstellung, Laden und Verteilung bis hin zur Vernichtung dargelegt sind. • Manuelle Prozessgenehmigung – Der Lieferant muss sicherstellen, dass alle von Menschen verwalteten Ereignisse für Schlüssel und digitale Zertifikate, einschließlich Registrierung und Generierung neuer Schlüssel und Zertifikate, auf ordnungsgemäßer Ebene genehmigt werden und ein entsprechendes Genehmigungsprotokoll geführt wird. • Digitale Zertifikate – Der Lieferant muss gewährleisten, dass alle Zertifikate über eine Reihe zugelassener und geprüfter Zertifizierungsstellen (CA) bezogen werden, die über Widerrufsoptionen und Richtlinien zum Zertifizierungsmanagement verfügen, und sicherstellen, dass selbst unterzeichnete Zertifikate nur dann genutzt werden, wenn eine CA-gestützte Lösung technisch unmöglich ist. Außerdem muss er manuelle Kontrollen einrichten, um die Integrität und Authentizität der Schlüssel sowie den fristgerechten Widerruf bzw. die fristgerechte Verlängerung zu gewährleisten. • Schlüsselgenerierung und Krypto-Lebensdauer – Der Lieferant muss dafür sorgen, dass alle Schlüssel nach dem Zufallsprinzip generiert werden – entweder durch zertifizierte Hardware oder eine CSPRNG-Software (Cryptographically Secure Pseudo Random Number Generator). o Der Lieferant muss sicherstellen, dass allen Schlüsseln dann eine begrenzte und festgelegte Krypto-Lebensdauer zugewiesen wird, nach der sie entweder ausgetauscht oder deaktiviert werden. Dies muss außerdem in Übereinstimmung mit den Auflagen des National Institute of Standards & Technology (NIST) und geltenden Branchenanforderungen geschehen.	Wird diese Kontrolle nicht umgesetzt, sind angemessene physische und technische Kontrollen möglicherweise nicht vorhanden, was zu Verzögerungen oder Unterbrechungen des Dienstes oder zu Verletzungen der Cyber-Sicherheit führen kann.

	• Schlüsselspeicherschutz – Der Lieferant muss sicherstellen, dass geheime/private Kryptografieschlüssel nur in folgenden Formen vorliegen: o Innerhalb der kryptografischen Grenzen eines Hardware-zertifizierten Sicherheitsgeräts/-moduls. o In verschlüsselter Form unter einem anderen festgelegten oder Passwort-abgeleiteten Schlüssel. o Bei gesplitteten Komponententeilen erfolgt eine Aufgabentrennung zwischen einzelnen Eigentümergruppen. o Automatische Löschung der Host-Speicherdaten nach Ablauf der Krypto-Lebensdauer, sofern nicht zum HSM-Schutz benötigt. • Der Lieferant muss sicherstellen, dass Schlüssel generiert und Hochrisikoschlüssel innerhalb der Grenzen des HSM-Speichers aufbewahrt werden. Dies beinhaltet Folgendes: o Schlüssel für regulierte Dienste, für die HSMs vorgeschrieben sind. o Zertifikate von CAs, die Barclays repräsentieren. o Root-, Issuing-, OCSP- und RA-Zertifikate (Registrierungsstelle) werden zur Ausstellung von Zertifikaten zum Schutz der Barclays-Dienste genutzt. o Schlüssel zum Schutz gespeicherter aggregierter Schlüsselarchive, Authentifizierungsdaten oder PII-Daten. • Schlüsselsicherung und -speicherung – Der Lieferant pflegt eine Sicherungskopie aller Schlüssel, um Dienstunterbrechungen zu verhindern, falls die Schlüssel kompromittiert werden oder wiederhergestellt werden müssen. Der Zugriff auf die Sicherungskopien ist unter Kenntnisaufteilung und dualer Kontrolle auf sichere Standorte beschränkt. Schlüsselsicherungen müssen mindestens ebenso streng geschützt werden wie die im Gebrauch befindlichen Schlüssel. • Bestandsliste – Der Lieferant pflegt eine vollständige und aktuelle Bestandsliste der von ihm für den für Barclays erbrachten Dienst angewendeten kryptografischen Technologien. In dieser sind alle kryptografischen Schlüssel, digitalen Zertifikate, die Kryptografie-Software und die Kryptografie-Hardware dargelegt, die vom Lieferanten	

	verwaltet werden, um bei einem Zwischenfall Schäden zu verhindern. Zu Belegzwecken wird die Bestandsliste nach der mindestens vierteljährlich stattfindenden Prüfung unterzeichnet und Barclays vorgelegt. Die Bestandslisten müssen, sofern relevant, Folgendes enthalten: o IT-Supportteam o Verbundene Ressourcen o Algorithmen, Schlüssellänge, Umgebung, Schlüsselhierarchie, Zertifizierungsstelle, Fingerabdruck, Schlüsselspeicherschutz sowie den technischen und operationellen Zweck • Funktionaler und operationeller Zweck – Schlüssel müssen einem spezifischen funktionalen und operationellen Zweck dienen und dürfen nicht zwischen verschiedenen Diensten oder über die Barclays-Dienste hinaus ausgetauscht werden. • Prüfpfade – Der Lieferant muss mindestens ein Mal pro Quartal einen Nachweis über die Überprüfung prüfbarer Datensätze erbringen und pflegen. Dazu zählen alle Ereignisse in Bezug auf das Schlüssel- und Zertifikat-Lebenszyklusmanagement, die eine vollständige Kontrollkette für alle Schlüssel demonstrieren, einschließlich Generierung, Verteilung, Laden und Vernichtung, um unbefugte Nutzung zu erkennen. • Hardware – Der Lieferant speichert die Hardware-Geräte in sicheren Bereichen und pflegt während des Lebenszylus des Schlüssels einen Prüfpfad, um sicherzustellen, dass die Kontrollkette der Kryptografie-Geräte nicht kompromittiert ist. Dieser Pfad wird in vierteljährlichen Abständen geprüft. o Der Lieferant muss dafür sorgen, dass die Kryptografie-Hardware mindestens nach FIPS140-2 Level 2 zertifiziert ist und Level 3 im „Physical Security and Cryptographic Key Management“ oder PCI HSM erreicht. Der Lieferant kann entscheiden, ob Chip-basierte Smartcards oder FIPS-zertifizierte E-Token als akzeptable Hardware zur Speicherung von Schlüsseln zulässig sind, die einzelne Mitarbeiter oder Kunden symbolisieren und abseits des Standorts von diesen aufbewahrt werden.	

	• Schlüsselkompromittierung – Der Lieferant pflegt und überwacht einen Plan für den Fall einer Schlüsselkompromittierung, um zu gewährleisten, dass Ersatzschlüssel unabhängig vom kompromittierten Schlüssel generiert werden und so sicherzustellen, dass der kompromittierte Schlüssel beliebige Informationen hinsichtlich seines Ersatzes preisgibt. Tritt eine Kompromittierung ein, ist umgehend das Barclays **Chief Security Office (CSO) Joint Operations Centre (JOC) – gcsojoc@barclays.com –** zu informieren. • Stärke von Algorithmen und Schlüsseln – Der Lieferant gewährleistet, dass die Algorithmen und Längen der Schlüssel den Auflagen des National Institute of Standards & Technology (NIST) und geltenden Branchenanforderungen entsprechen. o Starke Algorithmen und Schlüssellängen minimieren das Risiko, dass sensible Daten verloren gehen oder von Hackern mithilfe ausgeklügelter Verarbeitungsfertigkeiten kompromittiert werden. o Die Stärke der eingesetzten Verschlüsselung muss im richtigen Verhältnis zur Risikoneigung stehen, da sie sich auf den Betrieb oder die Leistung auswirken kann.	
24. Cloud-Computing	Der Lieferant sollte nach ISO/IEC 27017 bzw. 27001 oder SOC 1 bzw. 2 zertifiziert sein sowie unterstützende Geschäftsprozesse und technische Maßnahmen einrichten, um sicherzustellen, dass jedwede Nutzung von Cloud-Technologie angemessenen, implementierten Sicherheitskontrollen unterliegt. Barclays-Daten, die im Rahmen des für Barclays erbrachten Dienstes in der Cloud gespeichert werden, müssen von Barclays (Chief Security Office/ECAM-Team) genehmigt werden. Cloud-Kontrollen sollten die folgenden Bereitstellungsmodelle (IaaS/PaaS/SaaS) abdecken: • Identitäts- & Zugriffsmanagement/Zugangskontrolle • Netzwerkkonnektivität • Datenschutz (Übermittlung/Archivierung/Speicherung)	Eine fehlende Umsetzung dieser Kontrolle könnte dazu führen, dass Daten von Barclays aufgrund unzureichender Schutzmaßnahmen gefährdet werden, was wiederum rechtliche und regulatorische Strafmaßnahmen sowie Rufschädigung zur Folge haben kann.

	• Sicherheitsprotokollierung und -überwachung • Verschlüsselung & Schlüsselmanagement • Anwendungs- & Schnittstellensicherheit • Infrastruktur- & Virtualisierungssicherheit • Abgrenzung der Dienste	
25. Banktechnischer Raum (BDS)	Für Dienste, die formell einen banktechnischen Raum (BDS, Bank Dedicated Space) benötigen, müssen bestimmte physische und technische Anforderungen erfüllt werden. (Wenn für den Dienst ein BDS vorgeschrieben ist, gelten die Kontrollbestimmungen.) Die unterschiedlichem BDS-Arten lauten: Tier 1 (Erste Klasse) – Die gesamte IT-Infrastruktur wird von **Barclays** durch Bereitstellung eines von **Barclays** verwalteten LAN, WAN & Desktops an einem Lieferantenstandort mit einem speziell für Barclays vorgesehenem Raum gemanagt. Tier 2 (Business Class) – Die gesamte IT-Infrastruktur wird vom **Lieferanten** gemanagt und ist mit **Barclays**-Gateways verbunden – LAN, WAN & Desktop-Geräte gehören dem Lieferanten und werden von diesem verwaltet. Tier 3 (Economy Class) – Die gesamte IT-Infrastruktur wird vom **Lieferanten** gemanagt und ist mit **Barclays**-Internetgateways verbunden – LAN, WAN & Desktop-Geräte gehören dem Lieferanten und werden von diesem verwaltet.	Wird diese Kontrolle nicht umgesetzt, sind angemessene physische und technische Kontrollen möglicherweise nicht vorhanden, was zu Verzögerungen oder Unterbrechungen des Dienstes oder zu Verletzungen der Cyber-Sicherheit führen kann.
25.1 BDS – Physische Trennung	Der physisch belegte Bereich muss Barclays zur Verfügung gestellt werden und darf nicht mit anderen Firmen bzw. Lieferanten geteilt werden. Es sollte eine logische und physische Abgrenzung eingerichtet werden.	
25.2 BDS – Physische Zugangssteuerung	• Der Lieferant muss über ein physisches Zugangsverfahren verfügen, das Zugangsmethoden und -genehmigungen zu BDS-Bereichen beinhaltet, in denen Dienste erbracht werden. • Der Eintritt in und der Ausgang aus BDS-Bereichen muss durch physische Zugangskontrollmechanismen beschränkt und überwacht werden, um sicherzustellen, dass nur autorisiertem Personal Zutritt gewährt wird. • Eine autorisierte elektronische Zugangskarte ist nötig, um die BDS-Bereiche innerhalb der Geschäftsräume zu betreten.	

	• Der Lieferant muss in vierteljährlichen Abständen Prüfungen durchführen, um sicherzustellen, dass nur autorisierten Personen Zutritt zu BDS-Bereichen gewährt wird. Ausnahmen werden bis zur endgültigen Klärung gründlich untersucht. • Die Zugangsrechte von Mitarbeitern, die aus dem Unternehmen ausscheiden oder versetzt werden, sind innerhalb von 24 Stunden zu löschen. • Wachpersonal muss routinemäßige Rundgänge innerhalb der BDS-Bereiche durchführen, um unbefugten Zugang oder potenziell böswillige Aktivitäten effektiv festzustellen. • Für den Zugriff auf den BDS müssen u. A. die folgenden sicheren und automatischen Kontrollen eingesetzt werden: Für autorisierte Mitarbeiter: o Fotoausweis (jederzeit sichtbar zu tragen) o Berührungslose Kartenleser sind installiert o Aktiviertes Anti Passback (Verhinderung von zweimaligem Zutritt ohne vorhergehenden Austritt) • Der Lieferant muss über Prozesse und Verfahren zur Kontrolle und Überwachung externer Personen verfügen, einschließlich Dritten, denen zu Wartungs- oder Reinigungsarbeiten physischer Zugang zu BDS-Bereichen gewährt wird.
25.3 BDS – Videoüberwachung	• Installation von Videoüberwachung in BDS-Bereichen, um unbefugten Zugang oder böswillige Aktivitäten zuverlässig zu erkennen und Ermittlungen zu unterstützen. • Alle Zugangs- und Ausgangspunkte eines BDS-Bereichs müssen videoüberwacht werden. • Die Überwachungskameras sind ordnungsgemäß zu positionieren und müssen jederzeit deutlich erkennbare Bilder liefern, um böswillige Aktivitäten zu erkennen und Ermittlungen zu unterstützen. Der Lieferant muss die aufgezeichneten Überwachungsvideos 30 Tage lang speichern und alle Überwachungsaufzeichnungen und -aufzeichnungsgeräte müssen sicher stationiert sein, um Manipulation, Löschung oder den „beiläufigen" Blick auf die zugehörigen Überwachungsbildschirme zu verhindern. Außerdem muss der Zugriff auf die Aufzeichnungen kontrolliert und nur auf autorisierte Mitarbeiter beschränkt werden.
25.4 BDS – Zugang zum Barclays-Netzwerk und Barclays-	• Alle Einzelbenutzer können sich vom BDS aus nur mit einem von Barclays gestellten Multifaktor-Authentifizierungstoken beim Barclays-Netzwerk anmelden. • Der Lieferant muss Protokoll über Mitarbeiter führen, die Barclays-Authentifizierungstoken erhalten haben, und in vierteljährlichen Abständen eine Abstimmung vornehmen.

Authentifizierungstoken	• Auf Benachrichtigung, dass kein Zugriff mehr benötigt wird (z. B. aufgrund von Mitarbeiterkündigung, Projektneuzuweisung usw.), deaktiviert Barclays Authentifizierungsdaten innerhalb von vierundzwanzig (24) Stunden. • Darüber hinaus deaktiviert Barclays umgehend Authentifizierungsdaten, die über einen bestimmten Zeitraum hinweg nicht verwendet wurden (dieser Zeitraum der Nichtverwendung beträgt maximal einen Monat). • Dienste mit Remote-Druckerzugriff über eine Barclays Citrix-Anwendung müssen von Barclays (Chief Security Office/ECAM-Team) genehmigt und autorisiert werden. Der Lieferant muss Protokoll führen und eine vierteljährliche Abstimmung vornehmen. Siehe Abschnitt 11 – Sicherer Remotezugriff
25.5 BDS – Unterstützung außerhalb des Büros	Für den Support außerhalb der Büro-/Geschäftszeiten bzw. während der Heimarbeit ist der Remotezugriff auf die BDS-Umgebung standardmäßig nicht vorgesehen. Jeder Remotezugriff muss durch die relevanten Teams von Barclays (einschließlich Chief Security Office/ECAM-Team) genehmigt werden.
25.6 BDS – Netzwerksicherheit	• Pflege einer aktuellen Bestandsliste aller Netzwerkperimeter des Unternehmens (in Form eines Netzwerkplans/-diagramms). • Aufbau und Implementierung des Netzwerks müssen mindestens ein Mal pro Jahr geprüft werden. • BDS-Netzwerke müssen durch eine Firewall logisch vom Unternehmensnetzwerk des Lieferanten getrennt und der gesamte ein- und ausgehende Datenverkehr muss beschränkt und überwacht werden. • Routing-Konfigurationen müssen sicherstellen, dass Verbindungen nur zum Netzwerk von Barclays und nicht zu beliebigen anderen Lieferantennetzwerken geleitet werden. • Der Edge-Router des Lieferanten, der sich mit den Extranet-Gateways von Barclays verbindet, muss sicher konfiguriert werden und einem Konzept der Beschränkungskontrollen für Ports, Protokolle und Dienste folgen. ○ Sicherstellung, dass Protokollierung und Überwachung aktiviert sind. • Das BDS-Netzwerk muss überwacht und durch angemessene Netzwerkzugriffskontrollen dürfen nur Geräte mit entsprechender Berechtigung erlaubt werden. Siehe Abschnitt 9 – Perimeter- und Netzwerksicherheit
25.7 BDS – Drahtlosnetzwerk	Drahtlosnetzwerke müssen im Barclays-Netzwerksegment deaktiviert werden, um Barclays-Dienste bereitzustellen.

25.8 BDS – Endpunkt-Sicherheit	Computer innerhalb des BDS-Netzwerks müssen einen sicheren Desktop haben, der nach den bewährten Praktiken der Branche konfiguriert ist. Das Sicherheitskonzept für BDS-Endgeräte muss Folgendes beinhalten: • Datenträgerverschlüsselung; • Das Starten über andere aktive Geräte muss deaktiviert werden; • Deaktivierung aller nicht benötigten Softwareprogramme/Dienste/Ports; • Deaktivierung der Administratorrechte für lokale Benutzer; • Die Mitarbeiter des Lieferanten dürfen keine grundlegenden Einstellungen wie Standard-Service-Pack, Standarddienste usw. ändern; • USB-Ports müssen deaktiviert werden, um das Kopieren von Barclays-Daten auf externe Datenträger zu unterbinden; • Virenschutzsignaturen und Sicherheitspatches sind stets auf die neueste Version zu aktualisieren; • Eingeschränkter Schutz vor Datenverlust, damit keinerlei Barclays-Daten ausgeschnitten/kopiert/eingefügt bzw. Screenshots davon erstellt oder Print-Capture-Tools verwendet werden können; • Der Druckerzugriff muss standardmäßig deaktiviert sein; • Der Austausch/die Übertragung von Barclays-Daten über Instant-Messaging-Tools/-Software sollte deaktiviert werden; • Möglichkeiten und Prozesse, um unzulässige, als bösartig identifizierte Software zu erkennen und die Installation unzulässiger Software zu verhindern; Siehe Abschnitt 15 – Endpunkt-Sicherheitskontrolle

25.9 BDS – E-Mail und Internet	• Netzwerkverbindungen müssen sicher konfiguriert sein, damit E-Mail- und Internet-Aktivitäten im BDS-Netzwerk eingeschränkt sind.
	• Der Lieferant muss den Zugriff auf soziale Netzwerke, Webmail-Dienste und Websites beschränken, über die Informationen im Internet gespeichert werden können, wie beispielsweise Google Drive, Dropbox oder iCloud.
	• Die unbefugte Übermittlung von Barclays-Daten außerhalb des BDS-Netzwerks muss vor Datenleckagen geschützt werden:
	  • E-Mail
	  • Internet-/Web-Gateway (einschließlich Online-Speicher und Webmail).
	• Durchsetzung Netzwerk-basierter URL-Filter, welche die Fähigkeiten eines Systems darauf beschränken, sich nur mit internen oder Internet-Websites des Lieferantenunternehmens zu verbinden.

	• Sämtliche Anhänge und/oder Upload-Funktionen auf Websites müssen blockiert werden. • Es dürfen nur vollständig unterstützte Webbrowser und E-Mail-Clients erlaubt werden.	
25.10 BDS – BYOD/persönliche Geräte	**Persönlichen Geräten/BYOD darf es nicht erlaubt werden, auf die Barclays-Umgebung und/oder Barclays-Daten zuzugreifen**	
Inspektionsrecht	Zur Überprüfung der Erfüllung der Vertragspflichten des Lieferanten muss der Lieferant Barclays erlauben, nachdem Barclays dies mindestens zehn (10) Geschäftstage zuvor schriftlich angekündigt hat, eine Sicherheitsüberprüfung jedes Standorts oder jeder Technologie vorzunehmen, der bzw. die vom Lieferanten oder von dessen Subunternehmen dazu genutzt wird, die in den Diensten verwendeten Lieferantensysteme zu entwickeln, zu testen, zu verbessern, zu pflegen oder zu betreiben. Der Lieferant muss Barclays zudem erlauben, mindestens ein Mal pro Jahr oder unmittelbar nach einem Sicherheitsvorfall eine Inspektion durchzuführen. Zu jeder von Barclays bei einer Inspektion identifizierten Nichterfüllung von Kontrollen führt Barclays eine Risikobewertung durch und gibt einen Zeitrahmen für Abstellmaßnahmen vor. Anschließend muss der Lieferant etwaige geforderte Abstellmaßnahmen innerhalb dieses Zeitrahmens ausführen. Soweit von Barclays angefordert, muss der Lieferant bei jeder Inspektion Unterstützung in angemessener Weise leisten, und die im Rahmen der Inspektion vorgelegten Dokumente müssen ausgefüllt und an Barclays zurückgesendet werden.	Sofern dies nicht vereinbart wurde, sind Lieferanten nicht in der Lage, die Einhaltung dieser Sicherheitspflichten vollumfänglich abzusichern.

Anhang A: Glossar

Definitionen	
Konto	Ein Satz von Anmeldedaten (z. B. eine Benutzerkennung und ein Passwort), durch die der Zugriff auf ein IT-System mithilfe logischer Zugriffssteuerungen verwaltet wird.
Backup	Ein Backup oder Backup-Prozess ist die Erstellung von Datenkopien, damit diese zusätzlichen Kopien zur Wiederherstellung des Originals nach einem Datenverlust-Ereignis verwendet werden können.
Banktechnischer Raum	Banktechnischer Raum (Bank Dedicated Space, BDS) sind im Besitz oder unter der Kontrolle einer Konzerngesellschaft des Lieferanten oder von Subunternehmen befindliche Räumlichkeiten, die nur für Barclays zur Verfügung gestellt werden und von denen aus die Dienste erbracht oder bereitgestellt werden.
BYOD	Eigene Geräte der Mitarbeiter (Bring Your Own Devices)
Kryptografie	Die Anwendung mathematischer Grundlagen zur Entwicklung von Techniken und Algorithmen, die sich auf Daten anwenden lassen, damit Ziele wie Vertraulichkeit, Datenintegrität und/oder Authentifizierung erreicht werden.
Daten	Aufgezeichnete Fakten, Konzepte oder Anweisungen auf einem Speichermedium zur Kommunikation, zum Abruf und zur Verarbeitung durch automatisierte Mittel und Wiedergabe als für den Menschen verständliche Informationen.
DoS(-Angriff) (Denial of Service)	Versuch, die Verfügbarkeit einer Computerressource für ihre vorgesehenen Benutzer aufzuheben.
Vernichtung/ Löschung	Das Überschreiben, Auslöschen oder physische Zerstören von Informationen auf eine solche Art und Weise, dass sie nicht wiederherstellbar sind.
ECAM	„External Cyber Assurance & Monitoring"-Team, das die Sicherheitsaufstellung des Lieferanten beurteilt.
Verschlüsselung	Die Umwandlung einer Nachricht (Daten-, Sprach- oder Videonachricht) in eine nichtssagende, für unbefugte Mitleser unverständliche Form. Diese Umwandlung erfolgt aus dem Klartextformat in Chiffretext.
HSM	Hardware Security Module. Ein spezifisches Gerät zur sicheren kryptografischen Schlüsselgenerierung, -speicherung und -nutzung, einschließlich Beschleunigung kryptografischer Prozesse.

Informationsressource	Alle Informationen, denen ein Wert im Hinblick auf ihre Anforderungen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit beigemessen wird. Oder jegliche Einzelinformation oder Gruppe von Informationen, die einen Wert für die Organisation hat.
Verantwortlicher für Informationsressourcen	Die Einzelperson innerhalb des Unternehmens, die für die Kategorisierung einer Ressource verantwortlich ist sowie dafür, dass der korrekte Umgang mit der Ressource sichergestellt wird.
Minimalberechtigung	Der Mindestumfang an Zugriffsrechten/Genehmigungen, mit denen einem Benutzer oder Konto die Erfüllung seiner geschäftlichen Funktion ermöglicht wird.
Netzwerkgerät/Netzwerkausrüstung	Sämtliche IT-Geräte, die mit einem Netzwerk verbunden sind und mit denen ein Netzwerk verwaltet, unterstützt oder kontrolliert wird. Dazu zählen beispielsweise Router, Switches, Firewalls oder Lastverteiler.
Schadcode	Software, die in der Absicht erstellt wurde, die Sicherheitsrichtlinien eines IT-Systems, eines IT-Geräts oder einer IT-Anwendung zu umgehen. Beispiele sind Computerviren, Trojaner und Würmer.
Multi-Faktor-Authentifizierung	Authentifizierung mit zwei oder mehr unterschiedlichen Authentifizierungstechniken. Ein Beispiel ist die Verwendung eines Sicherheits-Tokens. Erforderlich für eine erfolgreiche Authentifizierung ist dabei etwas, das sich im Besitz der betreffenden Einzelperson befindet (d. h. das Sicherheits-Token), und etwas, das dem Benutzer bekannt ist (d. h. die Sicherheits-Token-PIN).
Privilegiertes Konto	Ein Konto, das ein höheres Maß an Kontrolle über ein spezifisches IT-System bietet. Solche Konten werden in der Regel für Systemwartung, Sicherheitsverwaltung oder Konfigurationsänderungen an einem IT-System verwendet. Beispiele sind „Administrator", „Stammverzeichnis", Unix-Konten mit uid=0, Supportkonten, Sicherheitsadministratorkonten, Systemadministratorkonten und lokale Administratorkonten.
Gemeinsam genutztes Konto	Konto, das mehreren Mitarbeitern, Beratern, Auftragnehmern oder Zeitarbeitskräften mit Zugriffsberechtigung überlassen wird, wenn Einzelkonten aufgrund der Art des Systems, auf das zugegriffen wird, keine zur Verfügung gestellte Option sind.
System	Ein System im Kontext dieses Dokuments sind Personen, Verfahren, IT-Geräte und Software. Die Elemente dieses zusammengesetzten Gebildes werden zusammen in der vorgesehenen Betriebs- oder Support-Umgebung verwendet, um eine bestimmte Aufgabe zu verrichten oder einem bestimmten Zweck gerecht zu werden, Support zu leisten oder eine Einsatzanforderung zu erfüllen.

Sollte	Diese Definition bedeutet, dass die Auswirkungen vollumfänglich verstanden und sorgfältig beurteilt werden, bevor eine andere Option gewählt wird.
Sicherheitsvorfall	Bei Sicherheitsvorfällen handelt es sich laut Definition um Ereignisse, die gegen eine ausdrückliche oder stillschweigende Sicherheitsrichtlinie verstoßen. • Versuche (ob fehlgeschlagen oder erfolgreich), sich unbefugten Zugang zu einem System oder den darauf befindlichen Daten zu verschaffen. • Ungewollte Unterbrechungen oder Überlastangriffe. • Unbefugte Nutzung eines Systems zur Verarbeitung oder Speicherung von Daten. • Änderungen an den Eigenschaften der System-Hardware, -Firmware oder -Software, ohne Wissen, Anweisung oder Zustimmung des Eigentümers. • Eine Anwendungsschwachstelle, die unbefugten Zugriff auf Daten ermöglicht.

Anhang B: Barclays-Kennzeichnungsschema für Informationen

Tabelle B1: Barclays-Kennzeichnungsschema für Informationen

Kennzeichnung	Definition	Beispiele
Geheim	Informationen müssen als **Geheim** kategorisiert werden, wenn ihre unbefugte Offenlegung negative Auswirkungen auf Barclays haben würde, mit der Einschätzung im Rahmen des Enterprise Risk Management Framework (ERMF) als „Kritisch" - „Critical" (finanziell oder nicht finanziell). Diese Informationen sind auf eine spezifische Zielgruppe beschränkt und dürfen ohne Erlaubnis des Urhebers nicht	• Informationen über mögliche Firmenzusammenschlüsse oder -übernahmen • Informationen zur strategischen Planung – das Geschäft und die Organisation betreffend. • Bestimmte Informationen über die Sicherheitskonfiguration. • Bestimmte Befunde und Berichte einer Betriebsprüfung. • Vorstandsprotokolle.

	weiterverbreitet werden. Auf ausdrückliche Genehmigung des Verantwortlichen für die Informationen können zur Zielgruppe auch externe Empfänger gehören.	• Angaben zur Authentifizierung oder Identifizierung und Verifizierung (ID&V) – Kunden/Klienten und Kollegen. • Große Mengen an Informationen über Karteninhaber. • Gewinnprognosen oder Jahresbilanzen (vor deren Veröffentlichung) • Im Rahmen einer formellen Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA) behandelte Punkte.
Eingeschränkt - Intern	Informationen müssen als **Eingeschränkt – Intern** kategorisiert werden, wenn es sich bei den voraussichtlichen Empfängern nur um authentifizierte Mitarbeiter von Barclays und Managed Service Providers (MSPs) von Barclays mit einem bestehenden aktiven Vertrag handelt und sie auf eine spezifische Zielgruppe beschränkt sind. Eine unbefugte Offenlegung würde negative Auswirkungen auf Barclays haben, mit der Einschätzung im Rahmen des ERMF als „Bedeutend" - „Major" oder „Begrenzt" - „Limited" (finanziell oder nicht finanziell). Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	• Strategien und Budgets • Leistungsbeurteilungen • Vergütung und personenbezogene Daten von Mitarbeitern. • Schwachstellenbewertungen
Nur für den Dienstgebrauch – Extern	Informationen müssen als **Eingeschränkt – Extern** kategorisiert werden, wenn es sich bei den voraussichtlichen Empfängern um authentifizierte Mitarbeiter von Barclays und MSPs von Barclays mit einem bestehenden aktiven Vertrag handelt und sie auf eine spezifische Zielgruppe oder auf vom Verantwortlichen für die Informationen genehmigte externe Personen beschränkt sind.	• Neue Produktpläne • Klientenverträge • Rechtsgültige Verträge • Für die externe Versendung vorgesehene Kunden-/Klienteninformationen individueller Art bzw. geringen Umfangs. • Kunden-/Klientenmitteilungen.

	Eine unbefugte Offenlegung würde negative Auswirkungen auf Barclays haben, mit der Einschätzung im Rahmen des ERMF als „Bedeutend" - „Major" oder „Begrenzt" - „Limited" (finanziell oder nicht finanziell). Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	• Angebotsunterlagen für Neuemissionen (z. B. Emissions-, Verkaufsprospekt). • Abschließende Forschungsdokumente. • Nicht zu Barclays gehörige wesentliche nicht öffentliche Informationen (Material Non-Public Information; MNPI). • Sämtliche Forschungsberichte • Bestimmte Marketingmaterial • Marktkommentare • Befunde und Berichte einer Betriebsprüfung
Uneingeschränkt	Informationen müssen als **Uneingeschränkt** kategorisiert werden, wenn sie entweder für die allgemeine Verbreitung bestimmt sind oder wenn sie im Falle ihrer Verbreitung keine negativen Auswirkungen auf die Organisation haben würden.	• Marketingmaterial • Veröffentlichungen • Öffentliche Ankündigungen • Stellenausschreibungen • Informationen ohne Auswirkungen auf Barclays

Tabelle B2: Barclays-Kennzeichnungsschema für Informationen – Anforderungen an die Handhabung

*** Informationen über Systemsicherheitskonfigurationen, Ergebnisse von Betriebsprüfungen und personenbezogene Datensätze können, je nach den Auswirkungen ihrer unbefugten Offenlegung auf das Geschäft, als „Eingeschränkt – Intern" oder „Geheim" eingestuft werden.

Phase des Lebenszyklus	Geheim	Eingeschränkt – Intern	Eingeschränkt – Extern
Erstellen und Einführen	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.

Speichern	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten abgelegt werden, an denen unbefugte Personen in der Lage sein könnten, sie einzusehen oder auf sie zuzugreifen. • Elektronische Ressourcen in Speichermedien müssen durch Verschlüsselung oder geeignete Ausgleichskontrollen geschützt werden, wenn ein erhebliches Risiko des unbefugten Zugriffs besteht. • Alle zum Schutz der Daten, der Identität und/oder Reputation von Barclays verwendeten privaten Schlüssel müssen durch zertifizierte HSMs (Hardware Security Modules), d. h. FIPS 140-2 Level 3 oder höher, geschützt sein.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen abgelegt werden (einschließlich öffentlicher Bereiche innerhalb der Räumlichkeiten, in die Besucher ohne Überwachung gelangen könnten). • Informationen dürfen nicht in öffentlichen Bereichen innerhalb von Räumlichkeiten gelassen werden, in die Besucher ohne Überwachung gelangen könnten.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten abgelegt werden, an denen unbefugte Personen in der Lage sein könnten, sie einzusehen oder auf sie zuzugreifen. • Elektronische Ressourcen in Speichermedien müssen durch Verschlüsselung oder geeignete Ausgleichskontrollen geschützt werden, wenn ein erhebliches Risiko des unbefugten Zugriffs besteht.
Zugriff und Verwendung	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten bearbeitet oder unbeaufsichtigt gelassen werden, an denen unbefugte Personen sie einsehen oder auf sie zugreifen könnten. Ressourcen können bearbeitet werden, wenn geeignete Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente).	• Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen außerhalb der Räumlichkeiten gelassen werden. • Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen innerhalb der Räumlichkeiten gelassen werden, in die Besucher ohne Überwachung gelangen könnten.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten bearbeitet oder unbeaufsichtigt gelassen werden, an denen unbefugte Personen sie einsehen oder auf sie zugreifen könnten. Ressourcen können bearbeitet werden, wenn geeignete Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente).

	• Für den Druck vorgesehene Ressourcen müssen mithilfe sicherer Druckprogramme gedruckt werden. • Elektronische Ressourcen müssen durch geeignete LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.	• Falls erforderlich, müssen elektronische Ressourcen durch geeignete LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.	• Gedruckte Ressourcen müssen sofort aus dem Drucker entnommen werden. Ist dies nicht möglich, müssen sichere Druckprogramme verwendet werden. • Elektronische Ressourcen müssen durch geeignete LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.
Weitergabe	• Ausgedruckte Ressourcen müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen. • Umschläge, in denen sich ausgedruckte Ressourcen befinden, müssen an der Vorderseite eine sichtbare Informationsbeschriftung tragen und mit einem manipulationssicheren Siegel versehen werden. Vor der Verteilung müssen diese in einen unbeschrifteten zweiten Umschlag gesteckt werden.	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung erhalten. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. • Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden. • Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen.	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung tragen. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein. • Umschläge, in denen sich ausgedruckte Ressourcen befinden, müssen an der Vorderseite eine sichtbare Informationsbeschriftung tragen. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. Elektronische Kopien mehrseitiger Dokumente müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen.

	• Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. Elektronische Kopien mehrseitiger Dokumente müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen. • Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden. • Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen. • Ressourcen dürfen nur an Personen verteilt werden, denen vom Verantwortlichen für die Informationen ausdrücklich die Befugnis erteilt wurde, sie in Empfang zu nehmen. • Ressourcen dürfen nicht per Fax gesendet werden.		• Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden. • Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen. • Ressourcen dürfen nur an Personen verteilt werden, die diese aus geschäftlichen Gründen benötigen. • Ressourcen dürfen nicht per Fax gesendet werden, es sei denn, der Absender hat sich vergewissert, dass die Empfänger zum Abruf der Ressource bereitstehen. • Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübertragung außerhalb des internen Netzwerks verläuft.

	• Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübertragung außerhalb des internen Netzwerks verläuft. • Für elektronische Ressourcen muss eine Kontrollkette gepflegt werden.		
Archivieren und Entsorgen	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben" des Systems und ähnlichen Ablagen gelöscht werden. • Medien, auf denen als „Geheim" eingestufte elektronische Ressourcen gespeichert wurden, müssen vor oder während der Entsorgung entsprechend bereinigt werden.	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben" des Systems und ähnlichen Ablagen gelöscht werden.	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben" des Systems und ähnlichen Ablagen gelöscht werden.

Bankgeheimnis

Zusätzliche Kontrollen nur für Länder mit Bankgeheimnis (Schweiz/Monaco)

Restricted - External

Kontrollbereich / Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Funktionen und Verantwortlichkeiten	Der Lieferant muss Funktionen und Verantwortlichkeiten für die Handhabung von Daten, durch die Kunden identifiziert werden (Client Identifying Data, nachfolgend CID genannt), definieren und kommunizieren. Der Lieferant muss nach jeder am Betriebsmodell (oder Geschäft) des Lieferanten vorgenommenen Änderung oder mindestens einmal im Jahr die Dokumente überprüfen, in denen die Funktionen und Verantwortlichkeiten für CID näher beschrieben sind, und er muss sie in dem betreffenden Land mit Bankgeheimnis verteilen. Wesentliche Funktionen sind unter anderem ein leitender Angestellter, der für den Schutz und die Aufsicht über sämtliche mit CID zusammenhängenden Aktivitäten zuständig ist (Definition von CID ist Anhang A zu entnehmen). Unter Berücksichtigung der Grundsätze des Wissensbedarfs muss die Anzahl der Mitarbeiter mit CID-Zugriff auf dem absoluten Minimum gehalten werden.	Durch die klare Definition von Funktionen und Verantwortlichkeiten wird die Umsetzung des Vertragsanhangs „Kontrollpflichten externer Lieferanten" unterstützt.

2. Berichterstattung über Verstöße im Zusammenhang mit CID	Um sicherzustellen, dass Verstöße mit Auswirkungen auf CID gemeldet und verwaltet werden, müssen dokumentierte Kontrollmechanismen und Prozesse vorhanden sein. Der Lieferant muss auf jede Nichteinhaltung der (in Tabelle B2 definierten) Anforderungen an die Handhabung reagieren und die Nichteinhaltung muss der entsprechenden Entität von Barclays, die dem Bankgeheimnis unterliegt, umgehend (spätestens innerhalb von 24 Stunden) gemeldet werden. Es muss ein Vorfallbehandlungsprozess für die zeitnahe Abwicklung und regelmäßige Meldung von Ereignissen, die CID betreffen, eingerichtet werden. Der Lieferant muss dafür sorgen, dass die festgelegten Abhilfemaßnahmen nach einem Vorfall gemäß einem Abhilfeplan (Aktion, Zuständigkeit, Frist) ausgeführt und mit dem entsprechenden Land mit Bankgeheimnis abgesprochen und vereinbart werden. Falls der externe Lieferant Beratungsdienste erbringt und ein Mitarbeiter dieses Lieferanten Auslöser eines Datenverlustvorfalls war, meldet die Bank den Vorfall dem Lieferanten und ist gegebenenfalls berechtigt, den Austausch des Mitarbeiters zu verlangen.	Mit Hilfe eines Vorfallbehandlungsprozesses wird sichergestellt, dass Vorfälle schnell eingedämmt werden und verhindert wird, dass sie sich ausweiten. Jede Nichteinhaltung mit Auswirkungen auf CID könnte Barclays schwere Rufschädigungen zufügen sowie Geldbußen und den Verlust der Banklizenz in der Schweiz oder in Monaco nach sich ziehen.

3. Weiterbildung und Awareness	Mitarbeiter des Lieferanten, die Zugriff auf CID haben und/oder diese handhaben, müssen nach jeder Änderung der Vorschriften oder mindestens einmal im Jahr eine Schulung* absolvieren, in der die Anforderungen des Bankgeheimnisses an CID behandelt werden. Der Lieferant muss dafür sorgen, dass alle neuen Mitarbeiter des Lieferanten (die Zugriff auf CID haben und/oder diese handhaben) innerhalb eines angemessenen Zeitraums (ca. 3 Monate) eine Schulung absolvieren, mit der sichergestellt wird, dass sie sich über ihre Verantwortlichkeiten in Bezug auf CID im Klaren sind. Der Lieferant muss den Überblick darüber behalten, welche Mitarbeiter die Schulung absolviert haben. * Länder mit Bankgeheimnis geben noch Anleitungen zu den erwarteten Inhalten der Schulung.	Durch Weiterbildung und Awareness werden alle anderen Kontrollen im Rahmen dieses Vertragsanhangs unterstützt.

4. Kennzeichnungsschema für Informationen	***Gegebenenfalls**** muss der Lieferant für sämtliche im Auftrag des betreffenden Landes mit Bankgeheimnis gehaltenen oder verarbeiteten Informationsressourcen das Barclays-Kennzeichnungsschema für Informationen (Tabelle E1 von Anhang E) anwenden, oder ein mit dem Land mit Bankgeheimnis vereinbartes alternatives Schema. Die Anforderungen an die Handhabung bei CID-Daten sind in Tabelle E2 von Anhang E festgelegt. * *Der Ausdruck „**gegebenenfalls**" bezieht sich auf den Nutzen der Kennzeichnung im Vergleich zu den damit verbundenen Kosten. Beispielsweise kann die Beschriftung eines Dokuments unangemessen sein, wenn diese einen Verstoß gegen etwaige Manipulationsschutzvorschriften bedeuten würde.*	Eine vollständige und genaue Bestandsliste der Informationsressourcen ist unverzichtbar, um sicherzustellen, dass die Kontrollen angemessen sind.
5. Cloud-Computing / externe Speicherung	Jede Nutzung von Cloud-Computing und/oder externer Speicherung von CID (auf Servern außerhalb des Landes mit Bankgeheimnis oder außerhalb der Infrastruktur des Lieferanten), die im Rahmen des Dienstes für das betreffende Land verwendet werden, bedarf der Genehmigung durch die entsprechenden relevanten lokalen Teams (einschließlich des Chief Security Office, der Abteilung Compliance und der Rechtsabteilung); und damit CID im Hinblick auf ihr hohes Risikoprofil geschützt sind, müssen Kontrollen im Einklang mit den Vorschriften im betreffenden Land mit Bankgeheimnis umgesetzt werden.	Wird dieses Prinzip nicht umgesetzt, könnten unangemessen geschützte Kundendaten (CID) gefährdet werden, was rechtliche und behördliche Strafmaßnahmen oder Rufschädigung zur Folge haben kann.

Anhang C: Glossar

** Daten, durch die Kunden identifiziert werden, sind spezielle Daten auf Grund der in der Schweiz und in Monaco gültigen Gesetze zum Bankgeheimnis. Deshalb verstehen sich die Kontrollen, die hier aufgeführt sind, als Ergänzung zu den oben aufgeführten Kontrollen.

Ausdruck	Definition
CID	Daten, durch die Kunden identifiziert werden (Client Identifying Data)
CIS	Cyber- und Informationssicherheit
Mitarbeiter des Lieferanten	Jegliche dem Lieferanten als festangestellte(r) Mitarbeiter(in) direkt zuzuordnende Einzelperson, oder jegliche Einzelperson, die dem Lieferanten zeitlich begrenzt Leistungen erbringt (z. B. Berater(in))
Ressource	Jegliche Einzelinformation oder Gruppe von Informationen, die einen Wert für die Organisation hat
System	Ein System im Kontext dieses Dokuments sind Personen, Verfahren, IT-Geräte und Software. Die Elemente dieses zusammengesetzten Gebildes werden zusammen in der vorgesehenen Betriebs- oder Support-Umgebung verwendet, um eine bestimmte Aufgabe zu verrichten oder einem bestimmten Zweck gerecht zu werden, Support zu leisten oder eine Einsatzanforderung zu erfüllen.
Benutzer	Konto ohne besondere Rechte, das einem Mitarbeiter, einem Berater, einem Auftragnehmer oder einer Zeitarbeitskraft des Lieferanten zugeteilt wurde, der bzw. die zum Zugriff auf ein im Eigentum von Barclays befindliches System berechtigt ist.

Anhang D: DEFINITION VON DATEN, DURCH DIE KUNDEN IDENTIFIZIERT WERDEN (CLIENT IDENTIFYING DATA, CID)

Direkte CID (DCID) lassen sich definieren als (im Eigentum des Kunden befindliche) eindeutige Kennungen, die es in der vorhandenen Form und auf sich allein gestellt ermöglichen, einen Kunden zu identifizieren, ohne dass auf Daten in Bankanwendungen von Barclays zugegriffen wird. Dies muss unzweideutig sein, keine Auslegungssache, und mögliche Beispiele hierfür sind Informationen wie der Vorname, der Nachname, der Firmenname, die Unterschrift, die Kennung in sozialen Netzwerken usw. Direkte CID sind Kundendaten, die sich weder im Eigentum der Bank befinden noch von ihr erstellt wurden.

Indirekte CID (ICID) werden in drei Stufen unterteilt

- **ICID der Stufe L1** lassen sich definieren als (im Eigentum der Bank befindliche) eindeutige Kennungen, die es ermöglichen, einen Kunden eindeutig zu identifizieren, falls Zugriff auf Bankanwendungen oder sonstige **Anwendungen Dritter** gewährt wird. Die Kennung muss unzweideutig sein, keine Auslegungssache, und mögliche Beispiele hierfür sind Kennungen wie die Kontonummer, die IBAN, Kreditkartennummer usw.

- **ICID der Stufe L2** lassen sich definieren als (im Eigentum des Kunden befindliche) Informationen, die in Kombination mit einer anderen Information auf die Identität eines Kunden schließen lassen würden. Zwar lassen sich diese Informationen auf sich allein gestellt nicht zur Identifizierung eines Kunden verwenden, sie können aber mit anderen Informationen verwendet werden, um einen Kunden zu identifizieren. ICID der Stufe L2 müssen ebenso streng wie DCID geschützt und verwaltet werden.
- **ICID der Stufe L3** lassen sich definieren als (im Eigentum der Bank befindliche) eindeutige, aber anonymisierte Kennungen, die es ermöglichen, einen Kunden zu identifizieren, wenn Zugriff auf Bankanwendungen gewährt wird. Der Unterschied zu ICID der Stufe L1 besteht in der Kategorisierung der Informationen als Eingeschränkt – Extern und nicht als Bankgeheimnis, sie unterliegen also nicht den gleichen Kontrollen.

Eine Übersicht zur Methode der Kategorisierung ist der Abbildung 1, Entscheidungsbaum für CID, zu entnehmen.

Direkte CID und ICID der Stufe L1 dürfen nicht an Personen außerhalb der Bank weitergegeben werden und bei ihnen muss jederzeit der Grundsatz des Wissensbedarfs beachtet werden. ICID der Stufe L2 dürfen je nach Wissensbedarf weitergegeben werden, ihre Weitergabe darf jedoch nicht in Verbindung mit jeglichen anderen Bestandteilen von CID erfolgen. Durch die Weitergabe mehrerer Bestandteile von CID besteht die Möglichkeit, dass eine „toxische Kombination" entsteht und die Identität eines Kunden so potenziell offenbart wird. Eine toxische Kombination definieren wir ausgehend von mindestens zwei ICID der Stufe L2. ICID der Stufe L3 dürfen weitergegeben werden, da sie nicht als Informationen auf der Stufe des Bankgeheimnisses kategorisiert sind, es sei denn, die wiederholte Verwendung derselben Kennung kann zur Erfassung von ausreichend ICID-Daten der Stufe L2 führen, so dass die Identität des Kunden offenbart wird.

Kategorisierung von Informationen	Bankgeheimnis			Eingeschränkt - Intern
Kategorie	**Direkte CID (DCID)**	**Indirekte CID (ICID)**		
		Indirekt (Stufe L1)	**Potenziell Indirekt (Stufe L2)**	**Unpersönliche Kennung (Stufe L3)**
Art der Information	Kundenname	Container-Nummer / Container-Kennung	Geburtsort	Jede strikt interne Kennung einer CID-Hosting-/-Verarbeitungsanwendung
	Firmenname	Nummer des MACC (Geldkonto unter einer Avaloq-Container-Kennung)	Geburtstag	Dynamische Kennung
	Kontoauszug	SDS-ID	Staatsangehörigkeit	Funktionskennung CRM-Partei
	Unterschrift	IBAN	Titel	Externe Container-Kennung
	Kennung für soziales Netzwerk	Anmeldedaten E-Banking	Familienverhältnisse	
	Reisepass-Nummer	Nummer der Depotverwahrung	Postleitzahl	

	Telefonnummer	Kreditkartennummer	Vermögensverhältnisse	
	E-Mail-Adresse	SWIFT-Nachricht	Große Position/Transaktionswert	
	Tätigkeitsbezeichnung oder PEP-Titel	Interne Geschäftspartner-Kennung	Letzter Kundenbesuch	
	Künstlername		Sprache	
	IP-Adresse		Geschlecht	
	Faxnummer		Ablaufdatum der Kreditkarte	
			Hauptansprechpartner	
			Geburtsort	
			Datum der Kontoeröffnung	

Beispiel: Wenn Sie an externe Personen (einschließlich Dritte in der Schweiz / in Monaco) oder interne Kollegen in anderen verbundenen Unternehmen / Tochtergesellschaften, die in der Schweiz / in Monaco oder anderen Ländern (z. B. Vereinigtes Königreich) ansässig sind, eine E-Mail senden oder Dokumente an sie weitergeben.

1. Kundenname

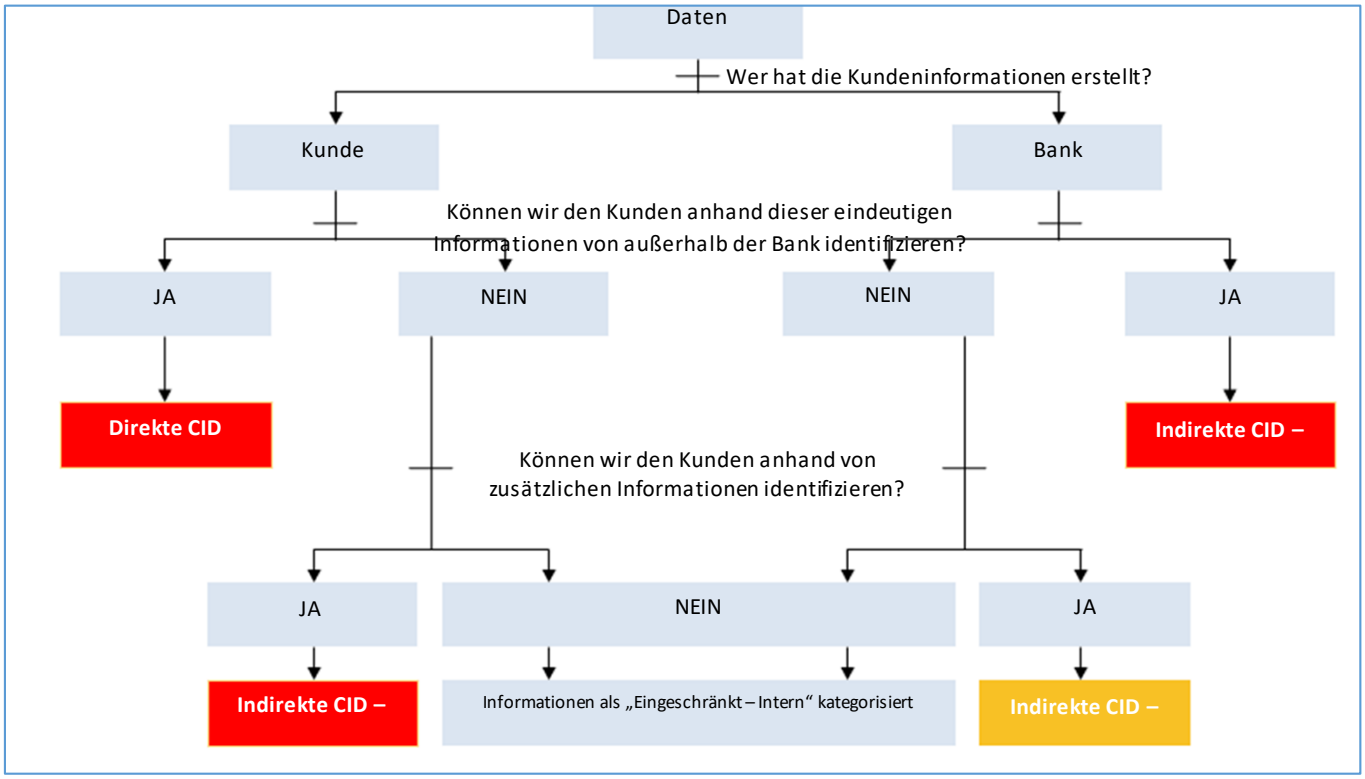
   (DCID) = Verletzung des Bankgeheimnisses

2. Container-Kennung

   (ICID der Stufe L1) = Verletzung des Bankgeheimnisses

3. Vermögensverhältnisse + Staatsangehörigkeit

(ICID der Stufe L2) + (ICID der Stufe L2) = Verletzung des Bankgeheimnisses



Anhang E: Barclays-Kennzeichnungsschema für Informationen

Tabelle E1: Barclays-Kennzeichnungsschema für Informationen

** Die Kennzeichnung „Bankgeheimnis" ist spezifisch für Länder mit Bankgeheimnis.

Kennzeichnung	Definition	Beispiele
Bankgeheimnis	Informationen, die im Zusammenhang mit schweizerischen, Direkten oder Indirekten Daten, durch die Kunden identifiziert werden (CID), stehen. Die Kategorisierung „Bankgeheimnis" gilt für Informationen, die im Zusammenhang mit Direkten oder Indirekten Daten, durch die Kunden identifiziert werden, stehen. Deshalb ist ein Zugriff durch sämtliche Mitarbeiter, auch wenn sie im Land der Verantwortlichkeit bzw. Verarbeitung der Informationen ansässig sind, nicht angemessen. Der Zugriff auf diese Informationen wird nur von denjenigen benötigt, die zur Erfüllung ihrer ordnungsgemäßen Aufgaben oder vertraglichen Pflichten diesbezüglich Wissensbedarf haben. Die unbefugte Offenlegung, der unbefugte Zugriff oder die unbefugte Weitergabe dieser Informationen, sowohl intern als auch außerhalb der Organisation, kann kritische Auswirkungen haben und zu strafrechtlichen	• Kundenname • Adresse des Kunden • Unterschrift • IP-Adresse des Kunden (weitere Beispiele in Anhang D)

	Verfahren führen sowie zivilrechtliche und administrative Konsequenzen wie beispielsweise Geldbußen und den Verlust der Banklizenz nach sich ziehen, wenn die Informationen unbefugtem Personal gegenüber offengelegt werden, sowohl intern als auch extern.	

Kennzeichnung	Definition	Beispiele
Geheim	Informationen müssen als Geheim kategorisiert werden, wenn ihre unbefugte Offenlegung negative Auswirkungen auf Barclays haben würde, mit der Einschätzung im Rahmen des Enterprise Risk Management Framework (ERMF) als „Kritisch" - „Critical" (finanziell oder nicht finanziell). Diese Informationen sind auf eine spezifische Zielgruppe beschränkt und dürfen ohne Erlaubnis des Urhebers nicht weiterverbreitet werden. Auf ausdrückliche Genehmigung des Verantwortlichen für die Informationen können zur Zielgruppe auch externe Empfänger gehören.	• Informationen über potenzielle Firmenzusammenschlüsse oder -übernahmen. • Informationen zur strategischen Planung – das Geschäft und die Organisation betreffend. • Bestimmte Informationen über die Sicherheitskonfiguration. • Bestimmte Befunde und Berichte einer Betriebsprüfung. • Vorstandsprotokolle. • Angaben zur Authentifizierung oder Identifizierung und Verifizierung (ID&V) – Kunden/Klienten und Kollegen. • Große Mengen an Informationen über Karteninhaber.

		• Gewinnprognosen oder Jahresergebnisse (vor deren Veröffentlichung). • Im Rahmen einer formellen Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA) behandelte Punkte.
Eingeschränkt – Intern	Informationen müssen als Eingeschränkt – Intern kategorisiert werden, wenn es sich bei den voraussichtlichen Empfängern nur um authentifizierte Mitarbeiter von Barclays und Managed Service Providers (MSPs) von Barclays mit einem bestehenden aktiven Vertrag handelt und sie auf eine spezifische Zielgruppe beschränkt sind. Eine unbefugte Offenlegung würde negative Auswirkungen auf Barclays haben, mit der Einschätzung im Rahmen des ERMF als „Bedeutend" - „Major" oder „Begrenzt" - „Limited" (finanziell oder nicht finanziell). Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	• Strategien und Budgets. • Leistungsbeurteilungen. • Vergütung und personenbezogene Daten von Mitarbeitern. • Schwachstellenbewertungen. • Befunde und Berichte einer Betriebsprüfung.

Eingeschränkt – Extern	Informationen müssen als Eingeschränkt – Extern kategorisiert werden, wenn es sich bei den voraussichtlichen Empfängern um authentifizierte Mitarbeiter von Barclays und MSPs von Barclays mit einem bestehenden aktiven Vertrag handelt und sie auf eine spezifische Zielgruppe oder auf vom Verantwortlichen für die Informationen genehmigte externe Personen beschränkt sind. Eine unbefugte Offenlegung würde negative Auswirkungen auf Barclays haben, mit der Einschätzung im Rahmen des ERMF als „Bedeutend" - „Major" oder „Begrenzt" - „Limited" (finanziell oder nicht finanziell). Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	• Neue Produktpläne. • Klientenverträge. • Rechtsgültige Verträge. • Für die externe Versendung vorgesehene Kunden-/Klienteninformationen individueller Art bzw. geringen Umfangs. • Kunden-/Klientenmitteilungen. • Angebotsunterlagen für Neuemissionen (z. B. Emissions-, Verkaufsprospekt). • Abschließende Forschungsdokumente. • Nicht zu Barclays gehörige wesentliche nicht öffentliche Informationen (Material Non-Public Information; MNPI). • Sämtliche Forschungsberichte. • Bestimmtes Marketingmaterial. • Marktkommentare.
Uneingeschränkt	Informationen, die entweder für die allgemeine Verbreitung bestimmt sind oder die im Falle ihrer Verbreitung keine Auswirkungen auf die Organisation haben würden.	• Marketingmaterial. • Veröffentlichungen. • Öffentliche Bekanntgaben. • Stellenausschreibungen.

		• Informationen ohne Auswirkungen auf Barclays.

Tabelle E2: Kennzeichnungsschema für Informationen – Anforderungen an die Handhabung

** Spezifische Anforderungen an die Handhabung bei CID-Daten, um deren Vertraulichkeit gemäß den behördlichen Vorschriften sicherzustellen

Phase des Lebenszyklus	Anforderungen des Bankgeheimnisses
Erstellung und Kennzeichnung	Wie bei „Eingeschränkt – Extern" sowie: • Ressourcen müssen einem Verantwortlichen für CID zugewiesen sein.
Speichern	Wie bei „Eingeschränkt – Extern" sowie: • Ressourcen dürfen auf wechselbaren Medien nur so lange gespeichert werden, wie dies aufgrund eines spezifischen geschäftlichen Erfordernisses ausdrücklich notwendig ist oder von Aufsichtsbehörden oder externen Prüfern ausdrücklich verlangt wird. • Große Umfänge von Informationsressourcen, die dem Bankgeheimnis unterliegen, dürfen nicht auf tragbaren Geräten/Medien gespeichert werden. Weitere Informationen erteilt auf Anfrage das lokale Team für Cyber-Sicherheit und Informationssicherheit (nachstehend CIS genannt). • Gemäß dem Grundsatz des Wissensbedarfs bzw. dem Grundsatz der Erforderlichkeit des Besitzes dürfen Ressourcen (ob physisch oder elektronisch) nicht an Orten abgelegt werden, an denen unbefugte Personen in der Lage sein könnten, sie einzusehen oder auf sie zuzugreifen. • Sichere Praktiken am Arbeitsplatz, beispielsweise ein aufgeräumter Arbeitsplatz (Clear Desk) und eine Desktop-Sperre, müssen zur sicheren Aufbewahrung von Ressourcen (ob physisch oder elektronisch) eingehalten werden.

	• Informationsressourcen auf wechselbaren Medien dürfen für die Speicherung nur so lange verwendet werden, wie dies ausdrücklich erforderlich ist, und bei Nichtverwendung müssen sie weggeschlossen werden. • Für Ad-hoc-Datenübertragungen auf tragbare Geräte/Medien ist die Genehmigung des Verantwortlichen für die Daten, der Abteilung Compliance und der CIS erforderlich.
Zugriff und Verwendung	Wie bei „Eingeschränkt – Extern" sowie: • Ohne die formelle Genehmigung vom Verantwortlichen für CID (oder dessen Stellvertreter) dürfen Ressourcen nicht an einen Ort außerhalb des Standorts (Räumlichkeiten von Barclays) verbracht bzw. dort eingesehen werden. • Ohne die formelle Genehmigung vom Verantwortlichen für CID (oder dessen Stellvertreter) und vom Kunden (Verzichtserklärung/beschränkte Vollmacht) dürfen Ressourcen nicht an einen Ort außerhalb des Buchungslandes des Kunden verbracht bzw. dort eingesehen werden. • Es müssen sichere Praktiken für die Telearbeit eingehalten werden, wobei sichergestellt wird, dass einem bei der Arbeit niemand über die Schulter sehen kann (kein Shoulder-Surfing), wenn physische Ressourcen an einen Ort außerhalb des Standorts verbracht werden.
	• Es muss sichergestellt werden, dass unbefugte Personen die elektronischen Ressourcen, auf denen sich CID befinden, über einen beschränkten Zugriff auf Geschäftsanwendungen weder beobachten noch darauf zugreifen können.
Weitergabe	Wie bei „Eingeschränkt – Extern" sowie: • Ressourcen dürfen nur gemäß dem „Grundsatz des Wissensbedarfs" UND innerhalb der Informationssysteme und unter den Mitarbeitern des Landes mit Bankgeheimnis, in dem sie entstanden sind, verteilt werden. • Für die Ad-hoc-Übertragung von Ressourcen mittels wechselbarer Medien ist die Genehmigung des Verantwortlichen für die Informationsressource und der CIS erforderlich.

	• Elektronische Mitteilungen müssen bei der Übertragung verschlüsselt sein. • Per Post (als Ausdruck) gesendete Ressourcen müssen mit einem Dienst zugestellt werden, bei dem eine Empfangsbestätigung verlangt wird. • Ressourcen dürfen nur nach dem „Grundsatz des Wissensbedarfs" verteilt werden.
Archivieren und Entsorgen	Wie bei „Eingeschränkt – Extern"

*** Informationen über Systemsicherheitskonfigurationen, Ergebnisse von Betriebsprüfungen und personenbezogene Datensätze können, je nach den Auswirkungen ihrer unbefugten Offenlegung auf das Geschäft, als „Eingeschränkt – Intern" oder „Geheim" eingestuft werden.

Phase des Lebenszyklus	Eingeschränkt – Intern	Eingeschränkt – Extern	Geheim
Erstellen und Einführen	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.

Speichern	• Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen abgelegt werden (einschließlich öffentlicher Bereiche innerhalb der Räumlichkeiten, in die Besucher ohne Überwachung gelangen könnten). • Informationen dürfen nicht in öffentlichen Bereichen innerhalb von Räumlichkeiten gelassen werden, in die Besucher ohne Überwachung gelangen könnten.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten abgelegt werden, an denen unbefugte Personen in der Lage sein könnten, sie einzusehen oder auf sie zuzugreifen. • Elektronische Ressourcen in Speichermedien müssen durch Verschlüsselung oder geeignete Ausgleichskontrollen geschützt werden, wenn ein erhebliches Risiko des unbefugten Zugriffs besteht.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten abgelegt werden, an denen unbefugte Personen in der Lage sein könnten, sie einzusehen oder auf sie zuzugreifen. • Elektronische Ressourcen in Speichermedien müssen durch Verschlüsselung oder geeignete Ausgleichskontrollen geschützt werden, wenn ein erhebliches Risiko des unbefugten Zugriffs besteht. • Alle zum Schutz der Daten, der Identität und/oder Reputation von Barclays verwendeten privaten Schlüssel müssen durch zertifizierte HSMs (Hardware Security Modules), d. h. FIPS 140-2 Level 3 oder höher, geschützt sein.

Zugriff und Verwendung	• Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen außerhalb der Räumlichkeiten gelassen werden. • Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen innerhalb der Räumlichkeiten gelassen werden, in die Besucher ohne Überwachung gelangen könnten. • Falls erforderlich, müssen elektronische Ressourcen durch geeignete LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten bearbeitet oder unbeaufsichtigt gelassen werden, an denen unbefugte Personen sie einsehen oder auf sie zugreifen könnten. Ressourcen können bearbeitet werden, wenn geeignete Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente). • Gedruckte Ressourcen müssen sofort aus dem Drucker entnommen werden. Ist dies nicht möglich, müssen sichere Druckprogramme verwendet werden. • Elektronische Ressourcen müssen durch geeignete LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten bearbeitet oder unbeaufsichtigt gelassen werden, an denen unbefugte Personen sie einsehen oder auf sie zugreifen könnten. Ressourcen können bearbeitet werden, wenn geeignete Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente). • Für den Druck vorgesehene Ressourcen müssen mithilfe sicherer Druckprogramme gedruckt werden. • Elektronische Ressourcen müssen durch geeignete LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.

Weitergabe	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung erhalten. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. • Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden. • Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen.	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung tragen. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein. • Umschläge, in denen sich ausgedruckte Ressourcen befinden, müssen an der Vorderseite eine sichtbare Informationsbeschriftung tragen. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. Elektronische Kopien mehrseitiger Dokumente müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen. • Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden.	• Ausgedruckte Ressourcen müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen. • Umschläge, in denen sich ausgedruckte Ressourcen befinden, müssen an der Vorderseite eine sichtbare Informationsbeschriftung tragen und mit einem manipulationssicheren Siegel versehen werden. Vor der Verteilung müssen diese in einen unbeschrifteten zweiten Umschlag gesteckt werden. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. Elektronische Kopien mehrseitiger Dokumente müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen.

		• Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen. • Ressourcen dürfen nur an Personen verteilt werden, die diese aus geschäftlichen Gründen benötigen. • Ressourcen dürfen nicht per Fax gesendet werden, es sei denn, der Absender hat sich vergewissert, dass die Empfänger zum Abruf der Ressource bereitstehen.	• Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden. • Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen. • Ressourcen dürfen nur an Personen verteilt werden, denen vom Verantwortlichen für die Informationen ausdrücklich die Befugnis erteilt wurde, sie in Empfang zu nehmen. • Ressourcen dürfen nicht per Fax gesendet werden.

		• Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübertragung außerhalb des internen Netzwerks verläuft.	• Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübertragung außerhalb des internen Netzwerks verläuft. • Für elektronische Ressourcen muss eine Kontrollkette gepflegt werden.
Archivieren und Entsorgen	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben" des Systems und ähnlichen Ablagen gelöscht werden.	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben" des Systems und ähnlichen Ablagen gelöscht werden.	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben" des Systems und ähnlichen Ablagen gelöscht werden.

			• Medien, auf denen als „Geheim" eingestufte elektronische Ressourcen gespeichert wurden, müssen vor oder während der Entsorgung entsprechend bereinigt werden.