BARCLAYS

Kontrollpflichten externer Lieferanten

Informations- und Cyber-Sicherheit (ICS)

Version 13.0 **September 2023**

Kontrollbereich / Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Genehmigte Verwendung	Der Lieferant muss sicherstellen, dass Informationen und andere zugehörige Ressourcen angemessen geschützt, verwendet und gehandhabt werden. Regeln für die akzeptable Nutzung und Verfahren für den Umgang mit Informationen und anderen zugehörigen Ressourcen müssen identifiziert, dokumentiert und implementiert werden. Mitarbeiter des Lieferanten samt Auftragnehmern, Unterauftragnehmern und Unterauftragsverarbeitern, die Informationen und andere zugehörige Ressourcen des Unternehmens verwenden oder Zugriff darauf haben, müssen über die Anforderungen an die Informationssicherheit zum Schutz und zur Handhabung der Informationen und anderer zugehöriger Ressourcen des Unternehmens informiert werden. Sie sind für ihre Nutzung der Einrichtungen zur Informationsverarbeitung verantwortlich. Das Unternehmen muss eine themenspezifische Richtlinie zur akzeptablen Nutzung von Informationen und anderen zugehörigen Ressourcen erstellen und diese an alle Personen weitergeben, die Informationen und andere zugehörige Ressourcen verwenden oder handhaben. Der Lieferant muss angemessene Schritte unternehmen, um die Konformität mit den allgemeinen Nutzungsbedingungen sicherzustellen. Folgende Themen können berücksichtigt werden: • 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 zur Verfügung gestellt werden. • Nutzung von IT-Geräten, die nicht vom Lieferanten zur Verfügung gestellt werden (z. B. eigene Geräte der Mitarbeiter [Bring Your Own Device]).	Allgemeine Nutzungsbedingungen helfen bei der Verstärkung der Kontrollumgebung zum Schutz von Informationsressourcen.

	• Nutzung tragbarer/wechselbarer Speichergeräte. • Verantwortlichkeiten bei Handhabung, Speicherung und Aufbewahrung der Informationsressourcen von Barclays. • Output von Datenleck-Kanälen, und • Risiken und Folgen des Missbrauchs der oben aufgeführten Gegenstände und/oder etwaige rechtswidrige, schädliche oder anstößige Folgen eines solchen Missbrauchs.	
2. Perimeter- und Netzwerksicherheit	Der Lieferant muss sicherstellen, dass alle vom Lieferanten und/oder dessen Unterauftragnehmer/Unterauftragsverarbeitern betriebenen Systeme und Anwendungen, die Barclays-Services unterstützen, vor eingehenden und ausgehenden Netzwerkbedrohungen geschützt sind. Es sollten Kontrollen implementiert werden, um die Sicherheit von Informationen in Netzwerken und den Schutz angeschlossener Dienste vor unbefugtem Zugriff zu gewährleisten. Der Lieferant muss Sicherheitswarnungen und -verletzungen identifizieren, schützen, erkennen und darauf reagieren. Die Netzwerksicherheitskontrollen gewährleisten den Schutz von Informationen in Netzwerken und ihren unterstützenden Informationsverarbeitungseinrichtungen. Zu ihnen zählen unter anderem folgende Bereiche: • Pflege und jährliche Überprüfung einer aktuellen Bestandsliste aller Netzwerkperimeter des Unternehmens (in Form eines Netzwerkplans/-diagramms). • Externe Verbindungen zum Lieferantennetzwerk werden vor ihrer Aktivierung dokumentiert, geprüft und genehmigt, um Sicherheitsverletzungen zu verhindern. • Lieferantennetzwerke müssen durch Anwendung von „Defense-in-Depth"-Prinzipien (z. B. Netzwerksegmentierung, Firewalls usw.) geschützt werden. • Der Lieferant muss über Technologien zur Verhinderung von Netzwerkeingriffen verfügen, um bösartigen Datenverkehr für den gesamten ein- und ausgehenden Datenverkehr zu erkennen und zu verhindern, sowie Signaturdatenbanken gemäß den besten branchenüblichen Best Practices aktualisieren und Updates vom Lösungsanbieter zeitnah anwenden. • Der Lieferant muss sicherstellen, dass die private Konnektivität zwischen Virtual Private Clouds (VPCs) und On-Premises-Netzwerken von Drittanbietern verschlüsselt ist und dass der Datenverkehr nicht dem öffentlichen Internet ausgesetzt ist. • Der Internet-Datenverkehr muss über einen Proxyserver laufen, der so konfiguriert ist, dass nicht autorisierte Verbindungen gefiltert werden.	Bei Nichtbeachtung dieser Grundsatzes könnten externe oder interne Netzwerke durch Angreifer unterwandert werden, die sich dadurch Zugang zum Dienst bzw. den damit verbundenen Daten verschaffen wollen.

	• Logische Trennung der Gerätemanagement-Ports/-Schnittstellen vom LAN-Datenverkehr der Benutzer, angemessene Authentifizierungskontrollen. • Sicherung der Kommunikation zwischen Geräten und Managementstationen/-konsolen. • Stellen Sie sicher, dass Protokollierung und Überwachung auch die Erkennung und Alarmierung verdächtiger Aktivitäten (anhand von Verhalten und Indikatoren für Kompromissauslöser), z. B. über ein SIEM, umfasst. • Die Netzwerkverbindung zwischen einzelnen Büros/Cloud-Serviceprovider/Datenzentren muss über ein sicheres Protokoll verschlüsselt werden. Barclays-Informationsressourcen/-Daten, die innerhalb des lieferantenseitigen Wide Area Network (WAN) übermittelt werden, sind zu verschlüsseln. • Der Lieferant muss die Firewall-Regeln (externe und interne Firewall) überprüfen und mindestens jährlich überprüfen. • Der Lieferant muss sicherstellen, dass der Zugriff auf das interne Netzwerk durch sachgerechte Netzwerkzugriffskontrollen überwacht wird. • Jeder drahtlose Zugang zum Netzwerk wird durch Protokolle zur Autorisierung, Authentifizierung, Segmentierung und starke Verschlüsselung überwacht, um Sicherheitsverletzungen zu vermeiden. • Der Lieferant muss über ein (logisch) getrenntes Netzwerk für die Dienstleistungen für Barclays verfügen. Der Lieferant muss gewährleisten, dass alle Server und Anwendungen, die zur Erbringung des Dienstes für Barclays genutzt werden, nicht über nicht vertrauenswürdige Netzwerke (Netzwerke außerhalb seiner Sicherheitsperimeter, die sich seiner 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, Unterauftragsverarbeiter), muss eine gültige Zertifizierung zum Sicherheitsmanagement in Übereinstimmung mit den bewährten Praktiken der Branche besitzen. 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/Last-Mile-Termination-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 Stellen Sie sicher, dass Protokollierung und Überwachung auch die Erkennung und Alarmierung verdächtiger Aktivitäten (anhand von Verhalten und Indikatoren für Kompromissauslöser), z. B. über ein SIEM, umfasst. **Der Drittanbieter muss sicherstellen, dass alle Systeme und Anwendungen, die Services erbringen, die Barclays als hohes Risiko betrachtet und dem Lieferanten als solche kommuniziert, netzwerksegmentiert werden. Die Partitionierung einer Geschäftsanwendung und ihrer grundlegenden Infrastrukturkomponenten (mit Ausnahme von gemeinsam genutzter und pervasiver kritischer Infrastruktur) in ihr eigenes Netzwerksegment unter Verwendung der zugelassenen Sicherheitstechnologien von Barclays (Firewalls oder andere gleichwertige Technologien) muss die nachstehenden Prinzipien erfüllen.** i. Ein Segmentierungsansatz muss verfolgt werden, um die Risikobelastung zu begrenzen, laterale Bewegungen im Netzwerk zu verhindern und das Übertragungsrisiko im Netzwerk zu senken. Anwendungen müssen in eigenständigen Segmenten stationiert werden, um das Risiko so weit wie mit vertretbarem Ausmaß möglich zu begrenzen. Beispiel: Faster-Payments-Zone Alle Infrastrukturen und Daten, die mit Geschäftsanwendungen in Verbindung stehen, müssen nach Möglichkeit in einer eigenständigen sicheren Anwendungszone bereitgestellt und vom internen Barclays-Netzwerk unter Verwendung einer CSO-genehmigten Durchsetzungstechnologie (z. B. Netzwerkfirewalls, genehmigte Segmentierungslösung) getrennt werden. Hinweis: In einigen Szenarios kann es erforderlich sein, Komponenten wie die Anwendung und die Datenbank auf mehrere Zonen aufzuteilen, z. B. wenn gemeinsam genutzte Plattformen genutzt werden. Jede Anwendung muss individuell beurteilt werden, wobei der zweckmäßigste Ansatz definiert und mit einem CSO-Sicherheitsberater vereinbart wird. ii. Die Dienste müssen physisch oder logisch getrennt sein. Das zugrunde liegende Netzwerkgefüge (z. B. Verkabelung/Switches) kann mit anderen Anwendungen und	

	Diensten gemeinsam genutzt werden, d. h., Segmente können logisch definiert werden, ohne dass eine Segmentierung durch physische Trennung vom Rest des Barclays-Netzwerks erforderlich ist. iii. Anwendungszonen müssen den Datenverkehr zu und von anderen Zonen (einschließlich des internen CIPE-Netzwerks) auf der Grundlage der für den Betrieb des Dienstes erforderlichen und genehmigten Verwaltungs-, Überwachungs- und Sicherheitstools beschränken. Konfigurationen müssen bestimmte Ports, Protokolle und IP-Adressen für zulässige Kommunikationspfade festlegen, alle anderen Kommunikationswege müssen standardmäßig eingeschränkt sein. Regeln, die Bereiche enthalten, sollten vermieden und nur ausnahmsweise genehmigt werden, um sicherzustellen, dass nur die minimalen Konnektivitätsanforderungen aktiviert werden. iv. Container müssen robust und durch starke logische Kontrollen abgetrennt sein, die eine laterale Bewegung zwischen den Containern verhindern und so die Isolierung durchsetzen. Die Kompromittierung eines Containers darf nicht zu einer Gefährdung anderer Container führen, die auf demselben Host/Cluster ausgeführt werden. v. Alle Segmentierungsimplementierungen müssen eine zentralisierte Richtlinienverwaltung mit Funktionen (oder Integration) zur Überprüfung und Meldung der Richtlinienkonformität bieten (siehe Dokument zur Firewall-Compliance) und ein überprüfbares Änderungsprotokoll liefern. vi. Wo immer möglich/machbar, sind zustandsbezogene Inspektionen/Kontrollen zu betreiben. vii. Segmentierungsfunktionen müssen „ausfallsicher“ funktionieren, z. B. müssen genehmigte Regelsätze zum Blockieren/Zulassen von Datenverkehr durchgesetzt werden, wenn die Funktion ausfällt. viii. Jeglicher Verkehr zwischen Produktions- und Nicht-Produktionssystemen in Anwendungszonen darf nur ausnahmsweise erlaubt und muss protokolliert werden. **Anleitung für Cloud-Service-Kunden (-Anbieter), die für die Erbringung von Services für Barclays in Anspruch genommen werden** Der Cloud-Service-Kunde (CSC) muss sicherstellen, dass zweckgerechte Netzwerksicherheitskontrollen eingerichtet werden, um den Barclays-Service zu schützen. • Der Cloud-Service-Kunde (CSC) sollte seine Anforderungen für die Trennung von Netzwerken definieren, um eine Mandantenisolierung in der gemeinsamen Umgebung eines Cloud-Dienste zu erreichen, und er sollte überprüfen, ob der Cloud-Serviceprovider diese Anforderungen erfüllt.	

	• Die Zugriffskontrollrichtlinie des Cloud-Service-Kunden für die Nutzung von Netzwerkdiensten sollte die Anforderungen für den Benutzerzugriff auf jeden einzelnen verwendeten Cloud-Dienst festlegen. *Anm.: Als „Netzwerk" wird in dieser Kontrollrichtlinie jedes nicht zu Barclays gehörige Netzwerk bezeichnet, für das der Lieferant verantwortlich ist, darunter auch Netzwerke von Unterauftragnehmern des Lieferanten.*	
3. 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. Wenn der Lieferant **Dienste erbringende Systeme und Anwendungen** hostet, die Barclays-Daten speichern oder einen Ausfallsicherheitsdienst der Kategorien 0 oder 1 unterstützen, muss dieser mit einem hinreichenden DoS-Schutz versehen sein, um die Verfügbarkeit zu gewährleisten.	Wird dieser Grundsatz nicht umgesetzt, können Barclays und die Lieferanten von Barclays möglicherweise nicht verhindern, dass ein DoS-Angriff sein Ziel erreicht.
4. Arbeit außerhalb des Unternehmens (Remotezugriff)	Der Lieferant muss die Sicherheit von Informationen sicherstellen, während Mitarbeiter außerhalb des Unternehmens arbeiten. Es sind Sicherheitsmaßnahmen zu ergreifen, um Informationen zu schützen, auf die Personen während der Arbeit außerhalb des Unternehmensgeländes zugreifen und die sie verarbeiten. Der Lieferant muss den Mitarbeitern Anweisungen zum Arbeiten von zu Hause aus geben. **Remotezugriff auf das Barclays-Netzwerk** Der Remotezugriff auf das Barclays-Netzwerk über die Citrix-Anwendung von Barclays wird standardmäßig nicht zur Verfügung gestellt. Für den Zugriff auf das Barclays-Netzwerk von nicht genehmigten Standorten/von außerhalb des Büros/von zu Hause aus sowie für den Remotezugriff muss eine vorherige Genehmigung und Autorisierung von Barclays (Chief Security Office – ECAM Team (externalcyberassurance@barclayscorp.com) eingeholt werden. Der Lieferant sorgt dafür, dass für den Remotezugriff folgende Kontrollen eingerichtet sind:	Remotezugriffskontrollen helfen zu gewährleisten, dass sich keine nicht autorisierten und unsicheren Geräte aus der Ferne mit der Barclays-Umgebung verbinden.

	• Für den Zugriff auf das Barclays-Netzwerk sind ein RSA Token (Soft) und eine unterstützte Version der Citrix Workspace-App erforderlich. Einzelheiten werden von Barclays bereitgestellt. • Der Lieferant muss aktuelle und korrekte Aufzeichnungen über seine Mitarbeiter führen, die für die Remote-/Hybridarbeit genehmigt wurden, wobei für jeden genehmigten Mitarbeiter, einschließlich Unterauftragnehmer/Unterauftragsverarbeiter, eine geschäftliche Begründung erforderlich ist. • **Der Lieferant muss vierteljährlich eine Abstimmung aller Mitarbeiter für den Remotezugriff durchführen, gefolgt von einer Anzeige der Ergebnisse an Barclays (Chief Security Office – ECAM Team (externalcyberassurance@barclayscorp.com).** • Auf Benachrichtigung, dass kein Zugriff mehr benötigt wird (z. B. aufgrund von Mitarbeiterkündigung, Projektneuzuweisung usw.), deaktiviert Barclays Authentifizierungsdaten **innerhalb von vierundzwanzig (24) Stunden nach dem Tag des Ausscheidens/Last Day in Office (LDIO)**. • Darüber hinaus deaktiviert Barclays umgehend Authentifizierungsdaten, die über einen bestimmten Zeitraum hinweg nicht verwendet wurden (dieser Zeitraum der Nichtverwendung beträgt maximal einen Monat). • Der Lieferant muss sicherstellen, dass der Endpunkt, der für die Fernverbindung zu den Informationssystemen von Barclays verwendet wird, sicher konfiguriert ist (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 - **externalcyberassurance@barclayscorp.com**) genehmigt und autorisiert werden. Der Lieferant muss Protokoll führen und eine vierteljährliche Abstimmung durchführen. • **Persönlichen Geräten/BYOD (begrenzt auf Laptops/Desktops) darf kein Zugriff auf die Barclays-Umgebung und/oder Barclays-Daten gewährt werden, die in einer vom Lieferanten kontrollierten Umgebung aufbewahrt/gespeichert werden (eingeschlossen sind Mitarbeiter, Berater, Leiharbeiter, Auftragnehmer und Managed Service Partner, Unterauftragnehmer/Unterauftragsverarbeiter des Lieferanten).** Hinweis: Der Remotezugriff auf das Barclays-Netzwerk und Barclays-Daten ist nur mit ausdrücklicher Genehmigung und Autorisierung durch Barclays erlaubt.	

	Remotezugriff auf Lieferantenumgebung/-netzwerk Remotezugriff auf die vom Lieferanten verwaltete Umgebung für die Erbringung von Dienstleistungen, an der Barclays-Daten beteiligt sind, die sich in der Umgebung/im Netzwerk des Lieferanten befinden bzw. dort gespeichert sind und/oder dort verarbeitet werden. Der Lieferant sorgt dafür, dass für den Remotezugriff auf das Unternehmensnetzwerk des Lieferanten folgende Kontrollen eingerichtet sind. • Für den Remotezugriff auf das Lieferantennetzwerk müssen die übermittelten Daten stark verschlüsselt werden und es muss eine Multifaktor-Authentifizierung erfolgen. • Der Lieferant kann einen virtuellen Desktop für den Remotezugriff verwenden. • Der Lieferant muss Protokoll über Mitarbeiter führen, die Remote-/Hybridarbeit leisten. • **Der Lieferant muss eine Abstimmung aller Remotebenutzer gemäß den Zeitvorgaben des Lieferanten durchführen.** • Wenn kein Zugriff mehr benötigt wird (z. B. aufgrund von Mitarbeiterkündigung, Projektneuzuweisung usw.), deaktiviert der Lieferant Authentifizierungsdaten **innerhalb von vierundzwanzig (24) Stunden nach dem Tag des Ausscheidens/Last Day in Office (LDIO)**. • **Persönlichen Geräten/BYOD (begrenzt auf Laptops/Desktops) darf kein Zugriff auf 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).** Der Lieferant muss den Mitarbeitern Regeln für die Arbeit von zu Hause an die Hand geben, einschließlich Dos and Don'ts. Remote-Arbeit (auch von zu Hause aus) ist während des normalen Geschäftsablaufs verboten, soweit Dritte vertraglich verpflichtet sind, Dienstleistungen in banktechnischem Raum (Bank Dedicated Space) oder in den Räumlichkeiten des Lieferanten zu erbringen, oder wenn aufsichtsrechtliche Anforderungen gelten. In Business-Continuity-Plänen von Drittanbietern können jedoch für den Fall einer Notfallwiederherstellung/Krise/Pandemie in Abstimmung mit Barclays und im Einklang mit allen Sicherheitsanforderungen	

<table>
<tr><td></td><td>Vorkehrungen für die Remote-Arbeit im Rahmen der vertraglichen Vereinbarung getroffen werden.</td><td></td></tr>
<tr><td>5. Management von Sicherheitsprotokollen</td><td>Der Lieferant muss über ein gut etabliertes und unterstützendes Rahmenkonzept für das Audit- und Protokollmanagement verfügen. Das Rahmenkonzept muss wichtige IT-Systeme umfassen, einschließlich Anwendungen, Netzwerkausrüstung, Sicherheitsgeräte und Server, die für die Protokollierung wichtiger Ereignisse eingerichtet sind. Zur Aufzeichnung von Ereignissen, Erbringung von Nachweisen und Gewährleistung der Integrität von Protokollinformationen müssen Protokolle fälschungssicher sein, Schutz vor unbefugtem Zugriff bieten und die Identifizierung von Informationssicherheitsereignissen ermöglichen, die zu einem Informationssicherheitsvorfall führen können, und Untersuchungen unterstützen. Der Lieferant muss sicherstellen, dass die Protokolle zentralisiert, angemessen gegen Manipulation und/oder Löschung geschützt und vom Lieferanten mindestens 12 Monate lang oder über einen den behördlichen Auflagen entsprechenden längeren Zeitraum 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>
Das Rahmenkonzept des Sicherheitsprotokollmanagements sollte die folgenden Bereiche abdecken:

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, damit es möglich ist, Angriffe zu überwachen, zu erkennen, zu verstehen und/oder 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 können folgende Informationen enthalten:
</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>

	○ IDS/IPS, Router, Firewall, Web-Proxy, Remotezugriffssoftware (VPN), Authentifizierungsserver, Anwendungen, Datenbankprotokolle. ○ Erfolgreiche Anmeldungen, fehlgeschlagene Anmeldeversuche (beispielsweise falsche Benutzerkennung oder falsches Passwort), Erstellung, Änderung und Löschung von Benutzerkonten. ○ Konfiguration von Änderungsprotokollen. • Barclays-Dienste in Bezug auf Geschäftsanwendungen und technische Infrastruktursysteme, auf denen angemessene und den bewährten Praktiken der Branche entsprechende Protokollierung aktiviert werden muss, einschließlich ausgelagerter oder „in der Cloud" befindlicher Lösungen. • Synchronisierung der Zeitstempel in Ereignisprotokollen anhand einer gemeinsamen, vertrauenswürdigen Quelle. • Schutz sicherheitsspezifischer Ereignisprotokolle (z. B. durch Verschlüsselung, MFA, Zugriffskontrolle und Sicherungskopien). • 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. • Die Protokollanalyse sollte die Analyse und Interpretation von Informationssicherheitsereignissen umfassen, damit ungewöhnliche Aktivitäten oder ungewöhnliches Verhalten erkannt werden, die auf Gefährdungen hinweisen können. • Zu den wichtigen protokollierten Ereignissen müssen jene gehören, die potenziell die Vertraulichkeit, Integrität und Verfügbarkeit der für Barclays zur Verfügung gestellten Dienste beeinflussen könnten und die zur Identifizierung oder Untersuchung von Vorfällen und/oder Zugriffsrechtsverletzungen bezüglich der Lieferantensysteme beitragen können. • Prüfen Sie regelmäßig, ob das Rahmenkonzept weiterhin die oben genannten Anforderungen erfüllt. **Anleitung für Cloud-Service-Kunden (-Anbieter), die für die Erbringung von Services für Barclays in Anspruch genommen werden**	

	Der Cloud-Service-Kunde (CSC) muss sicherstellen, dass zweckgerechte Kontrollen für das Sicherheitsprotokollmanagement implementiert werden, um den Barclays-Service zu schützen - • Der Cloud-Service-Kunde sollte seine Anforderungen für die Ereignisprotokollierung definieren und dokumentieren sowie überprüfen, ob der Cloud-Dienst diese Anforderungen erfüllt. • Wenn eine privilegierte Funktion an den Cloud-Service-Kunden delegiert wird, sollten der Betrieb und das Ergebnis dieser Funktionen protokolliert werden. Der Cloud-Service-Kunde sollte entscheiden, ob die vom Cloud-Serviceprovider zur Verfügung gestellten Protokollierungsfunktionen zweckgerecht sind oder ob der Cloud-Service-Kunde zusätzliche Protokollierungsfunktionen implementieren sollte. • Der Cloud-Service-Kunde sollte Informationen über die für die Systeme des Cloud-Serviceproviders verwendete Zeitsynchronisierung anfordern. • Der Cloud-Service-Kunde sollte vom Cloud-Serviceprovider Informationen über die für jeden Cloud-Dienst verfügbaren Überwachungsfunktionen anfordern.	
6. Malware-Abwehr	In Übereinstimmung mit den bewährten Praktiken der Branche muss der Lieferant etablierte Richtlinien und Verfahren einführen sowie unterstützende Geschäftsprozesse und technische Maßnahmen umsetzen, um die Ausführung von Malware in der gesamten IT-Umgebung zu verhindern. 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 unter anderem Folgendes beinhalten: • Zentral verwaltete Anti-Malware-Software, um die gesamte IT-Umgebung des Unternehmens kontinuierlich zu überwachen und zu schützen. • Gewährleistung, dass die Anti-Malware-Software der Organisation ihre Scan-Engine aktualisiert • Regelmäßige Aktualisierung der Signatur-Datenbank • Versendung aller erkannten Malware-Ereignisse zur Analyse und Warnung an die unternehmenseigenen Anti-Malware-Administrationstools und Ereignisprotokollserver. • Der Lieferant sollte zweckgerechte Kontrollen implementieren, um sich vor Malware und Angriffen auf mobile Geräte zu schützen, die für Barclays-Dienste genutzt werden.	Anti-Malware-Lösungen sind für den Schutz der Informationsressourcen von Barclays vor Schadcode unerlässlich.

	• Das E-Mail-Gateway überprüft alle eingehenden, ausgehenden und internen E-Mail-Nachrichten, einschließlich Anhängen und URLs, auf Anzeichen bösartiger oder schädlicher Inhalte. Hinweis: Anti-Malware muss (unter anderem) unerlaubten mobilen Code, Viren, Spyware, Key-Logger-Software, Botnetze, Würmer, Trojaner usw. erkennen.	
8. Endpunkt-Sicherheit	Der Lieferant muss einen einheitlichen Ansatz für die Endpunktverwaltung verfolgen, um sicherzustellen, dass die für den Zugriff auf das Barclays-Netzwerk oder für den Zugriff auf bzw. die Verarbeitung von Barclays-Informationsressourcen/-Daten verwendeten Endpunkte zum Schutz vor bösartigen Angriffen verstärkt werden. Bewährte Praktiken der Branche müssen umgesetzt werden und die Endpunktsicherheit muss unter anderem folgende Punkte umfassen: • Vollständige Festplattenverschlüsselung. • Deaktivierung aller nicht benötigten Softwareprogramme/Dienste/Ports. • Deaktivierung der Administratorrechte für lokale Benutzer. • Die Mitarbeiter des Lieferanten dürfen grundlegenden Einstellungen wie Standard-Service-Pack, Systempartition, Standarddienste, Antivirus-Dienste usw. nicht ändern. • Die Aktivierung von USB für das Kopieren von Barclays-Informationen/Daten auf externe Medien • Virenschutzsignaturen und Sicherheitspatches sind stets auf die neueste Version zu aktualisieren. • Deaktivierung des Druckspoolerdiensts • Tool zum Schutz vor Datenverlust, um Datenschutzverletzungen bei Barclays zu verhindern • Der Lieferant muss sicherstellen, dass die Exfiltration von Barclays-Daten auf Websites sozialer Netzwerke, Webmail-Services und Websites, auf denen Informationen wie z. B. Google Drive, Dropbox oder iCloud gespeichert werden können, blockiert wird. • Deaktivierung der Weitergabe/Übermittlung von Barclays-Daten über Instant-Messaging-Tools/-Software. • Erkennen, Stoppen und Beheben des Vorhandenseins und/oder der Verwendung nicht autorisierter Software, einschließlich schädlicher Software.	Wird diese Kontrolle nicht umgesetzt, sind das Netzwerk und Endpunkte von Barclays und dem Lieferanten möglicherweise für Cyber-Angriffe anfällig.

	• Timeout bei Sperrbildschirm, Beschränkung der TCP/IP-Verbindung auf das Unternehmensnetzwerk, Advanced EPS-Sicherheitsagent zur Erkennung verdächtiger Verhaltensweisen Hinweis: Wechseldatenträger/tragbare Geräte sollten standardmäßig deaktiviert und nur zu legitimen Geschäftszwecken erlaubt werden. Gemäß den genehmigten Konfigurationsstandards eines Unternehmens muss der Lieferant sichere Abbildungen oder Vorlagen für alle Systeme im Unternehmen aufbewahren. Jedes neu eingerichtete oder bestehende System, das kompromittiert wurde, sollte mithilfe genehmigter Abbildungen oder Vorlagen konfiguriert werden. Wenn der Zugriff über die Endpunkte (Laptops/Desktops) auf das Barclays-Netzwerk mithilfe von Barclays Citrix-Anwendungen über das Internet zugelassen wird, muss der Lieferant das von Barclays zur Verfügung gestellte Tool zur Endpunktanalyse (EPA) installieren, um die Konformität der Endpunktsicherheit und des Betriebssystems zu überprüfen. Nur Geräte, die die Endpunktanalyse erfolgreich durchlaufen haben, erhalten über die Barclays Citrix-Anwendung Fernzugriff auf das Barclays-Netzwerk. Wenn der Lieferant das EPA-Tool nicht installieren oder verwenden kann, muss dies mit dem Barclays Relationship Manager/IT-Supportteam von Barclays/ECAM-Team geklärt werden. Mobile Geräte, die für Barclays-Dienste genutzt werden – • Um das Risiko einer Datenkompromittierung zu senken, muss der Lieferant einheitliche Endpunktverwaltungsfunktionen (UEM-Funktionen) oder 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. • Der Lieferant muss sicherstellen, dass mobile Geräte Möglichkeiten zur Remotesperrung und -löschung besitzen, um die Informationen im Falle von Verlust, Diebstahl oder Kompromittierung eines Geräts zu schützen. • Verschlüsselung von Barclays-Daten, die auf den Daten des mobilen Geräts gespeichert sind und/oder verarbeitet werden • Der Lieferant muss sicherstellen, dass Mobilgeräte keine vollen Administratorrechte (Root) haben und eine strenge Authentifizierungsrichtlinie aktiviert ist.	
9. Verhinderung von Datenleckagen	Der Lieferant muss die vom Management genehmigten effektiven Rahmenkonzepte nutzen, um Barclays-Daten vor Leckage/Exfiltration zu schützen. Dazu gehören unter anderem folgende Kanäle für Datenleckagen: -	Es sind angemessene, effektiv durchgeführte Kontrollen nötig, damit Informationen

	• Unzulässige Übertragung von Informationen außerhalb des internen Netzwerks bzw. außerhalb des Lieferantennetzwerks.
	  o E-Mail
	  o Internet-/Web-Gateway (einschließlich Online-Speicher und Webmail).
	  o DNS
	• 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 über Kabelverbindung (z. B. seriell, USB) oder drahtlos (z. B. Bluetooth, WLAN).
	• Unsicherer Informationsaustausch mit Dritten (Unterauftragnehmer, Unterauftragsverarbeiter).
	• Unangebrachtes Ausdrucken oder Kopieren von Informationen.
	
	Auf Systeme, Netzwerke und andere Geräte, die Daten/Informationen von Barclays verarbeiten, speichern oder übertragen, müssen Maßnahmen zur Vermeidung von Datenlecks angewendet werden.
		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 Geschäftsprozessen zur Folge haben kann.

10. Datensicherheit	Der Lieferant muss Barclays-Daten, die von ihm gespeichert und/oder verarbeitet werden, durch eine Kombination aus technischen Verfahren für Verschlüsselung, Integritätsschutz und Vorbeugung von Datenverlust sichern. Der Zugriff auf Barclays-Daten muss ausschließlich auf seine autorisierten Mitarbeiter beschränkt und vor Kontamination, Aggregationsangriffen, Inferenzangriffen und Speicherbedrohungen, wie unter anderem Bedrohungen aus Cloud-Computing-Umgebungen, geschützt werden. Die Maßnahmen für die Datensicherheit sollten unter anderem folgende Bereiche abdecken: 1. Der Lieferant ist verpflichtet, jederzeit alle geltenden Datenschutzgesetze einzuhalten. 2. Festlegung von Richtlinien, Prozessen und Verfahren zur Unterstützung von Geschäftsprozessen und technischen Maßnahmen. Dokumentation und Pflege von Datenflüssen für Daten, die sich am (physischen und virtuellen) geografischen Standort des Dienstes befinden. Sie sollten Details zu Anwendungen und Systemkomponenten im Datenfluss abdecken. 3. Pflege der Datenflussdiagramme von Barclays-Daten, die sich an geografischen (auch physischen und virtuellen) Standorten in Anwendungen und Systemkomponenten befinden.	

	4. Pflege eines Bestandsverzeichnisses aller vom Lieferanten gespeicherten, verarbeiteten oder übermittelten sensiblen/vertraulichen Barclays-Informationen (Barclays-Daten). 5. Gewährleistung, dass alle Barclays-Daten gemäß diesem Standard zu der vom Management genehmigten Datenklassifizierung und zum Datenschutz klassifiziert und gekennzeichnet werden. 6. Schutz von Daten im Ruhezustand a. Starke Verschlüsselung ruhender Daten, um die Gefährdung von Barclays-Informationsressourcen zu verhindern 7. Überwachung der Datenbank-Aktivitäten. a. Datenbank-Zugriff und -Aktivitäten sind zu überwachen und zu protokollieren, um bösartige Aktivitäten schnell und effektiv zu erkennen. 8. Schutz der verwendeten Daten; a. Sicherstellen, dass die Zugriffsverwaltungsfunktion die Verarbeitung vertraulicher Informationen steuert, um sie vor der Ausbeutung vertraulicher Informationen zu schützen 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 Daten während der Übertragung a. Nutzung effektiver Verschlüsselungstechniken, um den Schutz der Daten während ihrer Übermittlung zu gewährleisten. b. Die starke 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: 10. Transport Layer Security (TLS) (gemäß der bewährten Branchenpraxis der modernen Kryptografie, einschließlich der Verwendung/Ablehnung von Protokollen und Schlüsseln) 11. Alle Daten, die in Produktions- und Nicht-Produktionsumgebungen gespeichert sind, sind durch Verschlüsselung zu schützen (siehe Kontrolle 16 Kryptografie).	
11. Sicherheit von Anwendungssoftware	Der Lieferant muss mithilfe sicherer Codierungsverfahren und in einer sicheren Umgebung Anwendungen entwickeln. Wenn der Lieferant Anwendungen zur Verwendung durch Barclays entwickelt oder zur Unterstützung des Services für Barclays verwendet, muss der Lieferant ein Rahmenkonzept für die sichere Softwareentwicklung einrichten, um die	Kontrollen zum Schutz der Anwendungsentwicklung helfen, dafür zu sorgen, dass

	Sicherheit in den Lebenszyklus der Softwareentwicklung einzubauen. Der Lieferant muss Schwachstellen in der Software testen und beheben, bevor er sie an Barclays liefert. Die Sicherheit von Anwendungssoftware sollte unter anderem die folgenden Bereiche abdecken: • Festlegung und Übernahme von vom Management genehmigten Standards für sichere Codierung, die an den besten Branchenpraktiken ausgerichtet sind, um Schwachstellen und Serviceunterbrechungen zu vermeiden. • 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. • Es dürfen keine vertraulichen Informationen in die Entwicklungs- und Testsystemumgebung kopiert werden, es sei denn, es werden entsprechende Kontrollen für die Entwicklungs- und Testsysteme bereitgestellt. • 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 bewährten Branchenstandards (z. B. OWASP für Webanwendungen) gestaltet, entwickelt, zum Einsatz gebracht und getestet werden. • Verbot der Nutzung öffentlicher Code-Repositorys, Der Lieferant sollte Webanwendungen mithilfe von Web Application Firewalls (WAF) schützen, die den gesamten Datenverkehr, der die Webanwendung erreicht, auf aktuelle und geläufige Webanwendungsangriffe prüfen. Für nicht-webbasierte Anwendungen müssen	Anwendungen beim Einsatz geschützt sind.

	spezifische Anwendungsfirewalls genutzt werden, sofern für die Art der Anwendung 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 praktikabel, muss eine Host-basierte Web Application Firewall verwendet werden. Der Lieferant muss sicherstellen, dass alle internetfähigen SaaS-basierten (Software as a Service) Anwendungslösungen, die für Barclays-Dienste verwendet werden, außer einer herkömmlichen Authentifizierungskontrolle (Benutzername/Passwort) über eine zusätzliche Zugangskontrolle (Authentifizierungskontrolle) verfügen. Der Lieferant muss unter anderem folgende Bereiche abdecken: • Multi-Faktor-Authentifizierung (z. B. Token, SMS) • SSO (Single Sign-On) • Zugangskontrolle auf Basis von IP-Adressen Zusätzliche Zugangskontrollen müssen für Mitarbeiter des Lieferanten/Unterauftragnehmer/Unterauftragsverarbeiter/Mitarbeiter von Barclays/Kunden von Barclays eingerichtet werden.	
12. Logische Zugriffsverwaltung (Logical Access Management (LAM))	Der Zugriff auf Informationsressourcen (einschl. Software, Hardware und Daten) darf nur auf Need-to-Know-Basis nach dem Least-Privilege-Prinzip (Prinzip der Minimalberechtigung) gewährt werden. Der Verantwortliche für IT-Systeme/Informationsressourcen ist für die Bereitstellung einer Liste aller Konten verantwortlich, die Zugriff auf das System/die Informationsressource haben, sowie für die Definition des Logical Access Security Model (Modell für logischen Zugriffsschutz), einschließlich Zugriffsprofilen und Regeln für die Aufgabentrennung (Segregation of Duties, SoD). Die vom Lieferanten gehosteten Web-Anwendungen fallen in den Geltungsbereich von Barclays LAM Onboarding, und dafür sind Barclays LAM-Kontrollen zu implementieren. • Der Need-to-Know-Grundsatz des Wissensbedarfs besagt, dass Mitarbeiter nur auf die Informationen Zugriff haben sollten, die sie zur Erfüllung der ihnen ordnungsgemäß übertragenen Aufgaben benötigen. Wenn zum Beispiel ein Mitarbeiter nur Umgang mit Kunden in Großbritannien hat, benötigt er keine Informationen zu Kunden in den USA. • Das Prinzip der Minimalberechtigung besagt, dass Mitarbeiter nur den Mindestumfang an Berechtigungen haben sollten, die zur Erfüllung der ihnen ordnungsgemäß übertragenen Aufgaben erforderlich sind. Wenn zum Beispiel ein Mitarbeiter die	Angemessene LAM-Kontrollen helfen dabei, sicherzustellen, dass Informationsressourcen vor unangemessener Verwendung geschützt werden. Zugriffsverwaltungskontrollen sorgen mit dafür, dass nur zugelassene Benutzerkonten auf die Informationsressourcen zugreifen können.

	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. • Die **Aufgabentrennung (Segregation of Duties, SoD)** ist ein Ansatz zur Strukturierung von Aufgaben auf eine Weise, die verhindert, dass eine Aufgabe nur von einer einzelnen Person erledigt werden kann. Das dient in erster Linie dazu, das Betrugsrisiko zu mindern. Wenn zum Beispiel ein Mitarbeiter die Erstellung eines Kontos beantragt, sollte der Antrag nicht von ihm, sondern von einem anderen genehmigt werden. Es sind Zugriffsmanagementprozesse gemäß den Best Practices der Branche zu definieren, zu dokumentieren und durchzusetzen. Nach der Informations- und Cyber-Sicherheitsrichtlinie und dem IAM-Standard (Identity & Access Management, Identitäts- und Zugriffsmanagement) der Barclays Group ist dazu Folgendes erforderlich ist: • **Barclays LAM Onboarding:** Der Lieferant muss sicherstellen, dass für die Zugriffsmanagementprozesse das zentrale IAM-Toolset von Barclays genutzt wird, um die LAM-Kontrollen zu erleichtern. IT-System-Zugriffskontrolllisten (Access Control Lists, ACLs) müssen dem IAM-Team im Rahmen des Onboardings des IT-Systems im IAM-Toolset vorgelegt werden. Um einen möglichst effektiven Betrieb nachgeschalteter LAM-Kontrollen zu gewährleisten, ist die optimale Feed-Frequenz ein täglicher automatisierter Feed. Die Mindestanforderung ist ein monatlich bereitgestellter Feed. • **Kontrollen für Neuangestellte**: Alle Zugriffsmöglichkeiten müssen angemessen sein und vor der Bereitstellung genehmigt werden. • **Kontrollen für Personen, die in eine neue Position wechseln**: Zugriffsmöglichkeiten sind vor dem Transfertag zu überprüfen, um zu bestätigen, welche beibehalten, entzogen oder aktiviert werden müssen. Zugriffsmöglichkeiten, die entzogen werden müssen, sind vor dem Transfertag aufzuheben. • **Kontrollen für Ausscheidende**: Alle Zugriffsmöglichkeiten, die für den Zugriff auf Informationsressourcen von Barclays und/oder die Erbringung von Diensten für Barclays verwendet werden, müssen zu dem Datum entfernt werden, an dem der Vertrag des Mitarbeiters mit dem Lieferanten endet. • **Kontoverantwortung**: Eindeutiges Konto muss einem einzelnen Mitarbeiter zugeordnet sein, der für sämtliche mit dem Konto durchgeführten Aktivitäten verantwortlich ist. Kontodaten und Passwörter dürfen nicht an andere Mitarbeiter weitergegeben werden.	

	• **Ruhende Konten**: Konten, die 60 Tage in Folge oder länger nicht verwendet wurden, müssen gesperrt/deaktiviert werden (und entsprechende Aufzeichnungen sind aufzubewahren). • **Erneuerung der Zugriffsrechte**: Alle Zugriffsberechtigungen müssen überprüft werden – alle 12 Monate (bei nicht privilegiertem Zugriff) und alle 6 Monate (bei privilegiertem Zugriff), um sicherzustellen, dass der Zugriff angemessen bleibt. • **Überprüfung der Identität (ID&V)**: Es sind Kontrollen einzurichten, die gewährleisten, dass die Zugriffsmanagementprozesse Mechanismen zur Überprüfung der Identität beinhalten. • **Authentifizierung**: Alle Konten müssen authentifiziert werden, bevor der logische Zugriff gewährt wird. Anwendungen und Authentifizierungsmechanismen dürfen keine Passwörter oder PINs anzeigen. Angemessen lange und komplexe Passwörter, Passwortverlauf, Häufigkeit von Passwortänderungen, Multi-Faktor-Authentifizierung und sichere Verwaltung von Anmeldedaten müssen gewährleistet sein. • **Nicht persönliche Anmeldeinformationen**: Nicht persönliche Anmeldeinformationen (d. h. Passwörter und Geheimnisse) müssen in ein zweckgerechtes Tool zur Verwaltung von Anmeldedaten (z. B. CyberArk) integriert werden. Wo dies nicht möglich ist, müssen die Anmeldeinformationen gesichert werden, damit sie von keinem Menschen jemals verwendet werden können. Wenn eine menschliche Nutzung des Kontos erforderlich ist, muss der Zugriff temporär und zeitgebunden sein, und die Anmeldeinformationen müssen anschließend zurückgesetzt werden. • **Verwaltung von Anmeldedaten**: Passwörter für persönliche Konten müssen mindestens alle 90 Tage geändert werden. Passwörter für privilegierte und interaktive Konten müssen alle 90 Tage oder nach jeder menschlichen Nutzung geändert werden, damit kein Mensch das Passwort kennt. Wenn das Passwort aus 50 oder mehr Zeichen besteht, muss es alle 365 Tage oder nach jeder menschlichen Nutzung geändert werden, damit kein Mensch das Passwort kennt. Passwörter für interaktive Konten müssen sich von den zwölf (12) vorangegangenen Passwörtern unterscheiden. • **Zeitgebundener Zugriff**: Persönlicher privilegierter Zugriff auf Produktions- und Notfallwiederherstellungsinfrastruktur, die von Mitarbeitern von Barclays oder nicht ständigen Mitarbeitern von Barclays verwendet wird, muss zeitlich gebunden sein und bedarf entsprechender Genehmigungen. • **Überwachung privilegierter Aktivitäten**: Es muss eine Überwachung von privilegierten Aktivitäten durchgeführt werden. Anleitung für Cloud-Service-Kunden (-Anbieter), die für die Erbringung von Services für Barclays in Anspruch genommen werden	

	Der Cloud-Service-Kunde (CSC) muss sicherstellen, dass zweckgerechte Kontrollen für das logische Zugriffsmanagement implementiert werden, um den Barclays-Service zu schützen - • Der Cloud-Service-Kunde sollte ausreichende Authentifizierungstechniken (z. B. Multifaktor-Authentifizierung) verwenden, um die Cloud-Service-Administratoren des Cloud-Service-Kunden gemäß den identifizierten Risiken gegenüber den administrativen Fähigkeiten eines Cloud-Dienste zu authentifizieren. • Der Cloud-Service-Kunde sollte sicherstellen, dass der Zugriff auf Informationen im Cloud-Dienst gemäß seiner Zugangskontrollrichtlinie eingeschränkt werden kann und dass solche Einschränkungen realisiert werden. Dazu gehört auch die Einschränkung des Zugriffs auf Cloud-Dienste, Cloud-Service-Funktionen und Cloud-Service-Kundendaten, die im Service gepflegt werden. • Wenn die Nutzung von Hilfsprogrammen erlaubt ist, sollte der Cloud-Service-Kunde die in seiner Cloud-Computing-Umgebung zu verwendenden Hilfsprogramme identifizieren und sicherstellen, dass sie die Kontrollen des Cloud-Diensts nicht beeinträchtigen.	
13. Schwachstellenmanagement	Der Lieferant muss ein effektives Schwachstellenmanagement-Programm durch Richtlinien und Verfahren sowie unterstützende Prozesse/organisatorische Maßnahmen und technische Maßnahmen durchführen, um eine effektive Überwachung zu gewährleisten, Schwachstellen innerhalb von unternehmenseigenen oder vom Unternehmen verwalteten Anwendungen oder entwickelten Anwendungen/Code, Infrastrukturnetzwerk- und Systemkomponenten rechtzeitig zu erkennen und zu beheben, und so die Effizienz der implementierten Sicherheitskontrollen zu gewährleisten. Das Schwachstellenmanagement sollte unter anderem die folgenden Bereiche abdecken: • Definierte Rollen, Verantwortlichkeiten und Zuständigkeiten für Überwachung, Berichterstattung, Eskalation und Abhilfe. • Geeignete Tools und Infrastrukturen zur Suche nach Schwachstellen. • Der Service-Anbieter wird regelmäßig (Intervalle entsprechend den bewährten Praktiken der Branche) Schwachstellenprüfungen vornehmen, die innerhalb sämtlicher Ressourcenklassen in der Umgebung effektiv bekannte und unbekannte Schwachstellen aufdecken. • Anwendung eines Risikobewertungsprozesses, um die Behebung der festgestellten Schwachstellen zu priorisieren.	Wird diese Kontrolle nicht umgesetzt, könnten Angreifer Schwachstellen innerhalb von Systemen für Cyber-Angriffe ausnutzen, was rechtliche Probleme und Rufschädigung nach sich ziehen kann.

	• Gewährleistung, dass Schwachstellen durch solide Korrekturmaßnahmen und Patchmanagement effektiv behoben werden, um das Risiko einer Ausnutzung von Schwachstellen zu verringern (die Abhilfemaßnahmen müssen zeitnah und in Übereinstimmung mit den bewährten Praktiken der Branche oder mithilfe eines Patchmanagementprogramms erfolgen). • Aufstellung eines Prozesses zur Validierung der Schwachstellenbehebung, um innerhalb sämtlicher Ressourcenklassen in der Umgebung schnell und effektiv die Behebung der festgestellten Schwachstellen zu prüfen. • Regelmäßiger Abgleich der Ergebnisse aufeinanderfolgender Schwachstellenprüfungen, um zu überprüfen, ob die Schwachstellen rechtzeitig behoben wurden. Für Dienstleistungen des Anbieters im Zusammenhang mit **Hosting-Infrastruktur/Anwendungen** im Auftrag von Barclays (einschließlich kommunizierter **Hochrisiko-Dritter)** • Der Lieferant muss Barclays unverzüglich benachrichtigen, wenn kritische/hochgradige Schwachstellen gefunden werden. • Der Lieferant muss die Schwachstellen entsprechend der nachstehenden Tabelle oder in Abstimmung mit Barclays (Chief Security Office – ECAM-Team) beheben. **Priorität** / **Einstufung** / **Tage für Behebung (maximal)** P1 / Kritisch / 15 (max. 30 Tage) P2 / Hoch / 60 P3 / Mittel / 180 P4 / Gering / Kein SLA Alle Sicherheitsprobleme und Schwachstellen, die wesentliche Auswirkungen auf die Hosting-Infrastruktur von Barclays oder auf die vom Lieferanten zur Verfügung gestellten 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 - externalcyberassurance@barclayscorp.com) schriftlich abgestimmt werden. **Anleitung für Cloud-Service-Kunden (-Anbieter), die für die Erbringung von Services für Barclays in Anspruch genommen werden** Der Cloud-Service-Kunde (CSC) muss sicherstellen, dass zweckgerechte Sicherheitskontrollen für das Schwachstellenmanagement implementiert werden, um den Barclays-Service zu schützen - • Der Cloud-Service-Kunde sollte vom Cloud-Serviceprovider Informationen über das Management technischer Schwachstellen anfordern, die sich auf die zur Verfügung gestellten Cloud-Dienste auswirken können. Der Cloud-Service-Kunde sollte die technischen Schwachstellen identifizieren, für die er verantwortlich ist, und einen Prozess für ihre Verwaltung klar definieren.	
14. Patchmanagement	Der Lieferant muss über ein durch etablierte Unternehmensprozesse/organisatorische Maßnahmen und technische Maßnahmen unterstütztes Patchmanagementprogramm verfügen, um den Bedarf an Patches zu überwachen/zu verfolgen und Sicherheitspatches für die gesamte Umgebung/den gesamten Bestand des Lieferanten zu installieren. Der Lieferant muss sicherstellen, dass Server, Netzwerkgeräte, Anwendungen und Endpunktgeräte mit den neuesten Sicherheitspatches und den bewährten Praktiken der Branche entsprechend auf dem neuesten Stand gehalten werden, um Folgendes zu gewährleisten: • Bevor er einen Patch auf Produktionssystemen installiert, muss der Lieferant alle Patches auf Systemen beurteilen und testen, die genau der Konfiguration der Ziel-Produktionssysteme entsprechen. Darüber hinaus ist nach jedem Patching die 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 künftige Anforderungen an Audits, Untersuchungen, Fehlerbehebung und Analysen zu unterstützen. • Der Lieferant muss dafür sorgen, dass Patches in Produktions- und Notfallwiederherstellungs-Umgebungen angewendet werden.	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.

<table>
<tr>
<td>15. Penetrationstests/IT-Sicherheitsbewertung</td>
<td>
Der Lieferant muss unter Einbeziehung eines unabhängigen qualifizierten Sicherheitsdienstleisters eine IT-Sicherheitsbewertung/Penetrationstests durchführen, die sich auf die IT-Infrastruktur, einschließlich Disaster-Recovery-Standort und Webanwendungen im Zusammenhang mit dem (den) vom Lieferanten für Barclays erbrachten Dienst(en) bezieht.

Dies muss mindestens einmal jährlich erfolgen, um ausnutzbare Schwachstellen zu identifizieren, die die Vertraulichkeit der Daten von Barclays durch Cyberangriffe verletzen könnten. 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 Dienstleistungen des Anbieters im Zusammenhang mit Hosting-Infrastruktur/Anwendungen im Auftrag von Barclays (einschließlich kommunizierter Hochrisiko-Dritter)

Der Lieferant muss ECAM über den Umfang der Sicherheitsbewertung mit Barclays informieren und diesen Umfang 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.
Der Lieferant muss Barclays (Chief Security Office/ECAM-Team - - externalcyberassurance@barclayscorp.com) jährlich den aktuellen Bericht zur Sicherheitsbewertung vorlegen.
Der Lieferant muss Barclays unverzüglich benachrichtigen, wenn kritische/hochgradige Schwachstellen gefunden werden.
Der Lieferant muss die Schwachstellen entsprechend der nachstehenden Tabelle oder in Abstimmung mit Barclays (Chief Security Office – ECAM-Team) beheben.

<table>
<tr><th>Priorität</th><th>Einstufung</th><th>Tage für Behebung (maximal)</th></tr>
<tr><td>P1</td><td>Kritisch</td><td>15 (max. 30 Tage)</td></tr>
<tr><td>P2</td><td>Hoch</td><td>60</td></tr>
</table>
</td>
<td>
Wird diese Kontrolle nicht umgesetzt, ist de Lieferant möglicherweise nicht in der Lage, die Cyber-Bedrohungen, mit denen er es zu tun haben, und die Angemessenheit und Stärke seiner Abwehrmaßnahmen einzuschätzen.

Die Informationen von Barclays könnten offengelegt werden und/oder Dienste ausfallen, was wiederum regulatorische Probleme sowie Rufschädigung zur Folge haben kann.
</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td>P3</td><td>Mittel</td><td>180</td><td></td><td></td></tr>
<tr><td></td><td></td><td>P4</td><td>Gering</td><td>Kein SLA</td><td></td><td></td></tr>
<tr><td>16. Kryptografie</td><td colspan="4">Der Lieferant muss die ordnungsgemäße und effektive Nutzung von Kryptografie sicherstellen, um die Vertraulichkeit, Authentizität oder Integrität von Daten/Informationen von Barclays gemäß den geschäftlichen Anforderungen und den Anforderungen an die Informationssicherheit zu schützen, und die rechtlichen, gesetzlichen, aufsichtsrechtlichen und vertraglichen Anforderungen in Bezug auf Kryptografie berücksichtigen.

Bei der Verwendung von Kryptografie sind folgende Punkte zu berücksichtigen:

• die themenspezifische Kryptografierichtlinie, die von der Organisation festgelegt wurde, einschließlich der allgemeinen Grundsätze zum Schutz von Informationen. Eine themenspezifische Richtlinie zur Verwendung von Kryptografie ist notwendig, um den Nutzen der Verwendung kryptografischer Techniken zu maximieren, die Risiken zu minimieren und eine unangemessene oder falsche Verwendung zu vermeiden.
• Identifizierung des erforderlichen Schutzniveaus und der Kategorisierung der Informationen und somit Festlegung von Art, Stärke und Qualität der erforderlichen kryptografischen Algorithmen.
• Verwendung von Kryptografie zum Schutz von Informationen, die auf Speichermedien gespeichert und über Netzwerke an solche Geräte oder Speichermedien übertragen werden.
• Ansatz für das Schlüsselmanagement, einschließlich Methoden zur Generierung und zum Schutz von kryptografischen Schlüsseln und zur Wiederherstellung verschlüsselter Informationen bei Verlust, Kompromittierung oder Beschädigung von Schlüsseln.
• 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 zweckgerecht 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. Der Lieferant muss seine Schlüssel nach Ablauf des Servicezeitraums außer Betrieb nehmen oder ein obligatorisches Schlüsselrotationsprogramm einrichten.</td><td>Ein aktueller und angemessener Schutz durch Verschlüsselung sowie aktuelle und angemessene Verschlüsselungsalgorithmen stellen den kontinuierlichen Schutz der Informationsressourcen von Barclays sicher.</td></tr>
</table>

	• 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. • 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. • 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 bewährten Branchenstandards geschehen. • 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.	

	○ Zertifikate von CAs, die Barclays repräsentieren. ○ Root-, Issuing-, OCSP- und RA-Zertifikate (Registrierungsstelle) werden zur Ausstellung von Zertifikaten zum Schutz der Barclays-Dienste genutzt. ○ 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: • IT-Supportteam • Verbundene Ressourcen • 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. • 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 bewährten Branchenstandards entsprechen.	
17. Cloud-Computing	Der Lieferant (Cloud-Service-Kunde, CSC) muss sicherstellen, dass der für Barclays-Dienste genutzte Cloud-Dienst über ein klar definiertes Rahmenkonzept für Sicherheitskontrollen verfügt, um die Ziele von Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen und um zu gewährleisten, dass Sicherheitskontrollen vorhanden sind und die Dienste von Barclays wirksam schützen. Der Lieferant sollte nach ISO/IEC 27017 oder 27001 oder SOC 2 oder einem ähnlichen Rahmenkonzept für Cloud-Sicherheit oder nach der bewährten Praxis der Branche zertifiziert sein. So wird sichergestellt, dass Sicherheitsmaßnahmen vorhanden sind und umgesetzt werden, mit denen eine sichere Nutzung der Cloud-Technologie gewährleistet wird. Es ist sicherzustellen, dass der Cloud-Serviceprovider nach der bewährten Praxis der Branche zertifiziert ist, einschließlich geeigneter Kontrollen, die der neuesten Version der Cloud Security Alliance, Cloud Controls Matrix (CCM), entsprechen. Der Lieferant ist für die Gewährleistung von Datensicherheitskontrollen in Bezug auf Barclays-Informationsressourcen/-Daten, einschließlich personenbezogener Daten, innerhalb der Cloud verantwortlich, und der Cloud-Serviceprovider (CSP) ist für die Sicherheit der Cloud-Computing-Umgebung verantwortlich. Der Lieferant ist weiterhin für die	Eine fehlende Umsetzung dieser Cloud-Kontrolle könnte dazu führen, dass Daten von Barclays gefährdet werden, was wiederum regulatorische Probleme sowie Rufschädigung zur Folge haben kann.

	Konfiguration und Überwachung der Sicherheitsmaßnahmen zum Schutz vor Sicherheitsvorfällen, einschließlich Datenschutzverletzungen, verantwortlich. Der Lieferant muss Sicherheitsmaßnahmen für alle Aspekte des bereitgestellten Dienstes umsetzen, einschließlich des Modells der geteilten Verantwortung für die Cloud, um die Vertraulichkeit, Integrität, Verfügbarkeit und Zugänglichkeit zu gewährleisten, indem er die Möglichkeit des Zugriffs von Unbefugten auf Barclays-Informationen und die von Barclays genutzten Dienste auf ein Minimum reduziert. Cloud-Sicherheitskontrollen sollten unter anderem die folgenden Bereiche für Bereitstellungsmodelle (IaaS/PaaS/SaaS) abdecken: • Mechanismen für Steuerung und Rechenschaftspflicht • Identitäts- und Zugriffsmanagement • Netzwerksicherheit (einschließlich Konnektivität) • Datensicherheit (Übermittlung/Archivierung/Speicherung) • Sicheres Löschen/Entfernen von Daten • Kryptografie, Verschlüsselung und Schlüsselmanagement • Protokollierung und Überwachung • Virtualisierung • Abgrenzung der Dienste Barclays-Informationsressourcen/-Daten, einschließlich personenbezogener Daten, die im Rahmen des für Barclays erbrachten Dienstes in der Cloud gespeichert werden, müssen von Barclays (Chief Security Office – ECAM-Team) genehmigt werden. Der Lieferant stellt Barclays Standorte von Datenzonen und Failover-Datenzonen zur Verfügung, in denen Barclays-Daten gespeichert oder aufbewahrt werden.	

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 und 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**-Extranet-Gateways verbunden – LAN, WAN und 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 und Desktop-Geräte gehören dem Lieferanten und werden von diesem verwaltet.

18.1 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.
18.2 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 geregelt und überwacht werden, um sicherzustellen, dass nur autorisierten Mitarbeitern (rollenspezifisch) Zutritt gewährt wird und der Zutritt genehmigt wurde (vom BDS-Serviceeigentümer). • 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, versetzt werden oder untergetaucht sind, sind innerhalb von 24 Stunden zu löschen (und entsprechende Aufzeichnungen dazu sind aufzubewahren). • 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 Anti Passback (Verhinderung von zweimaligem Zutritt ohne vorhergehenden Austritt) wird aktiviert und überwacht • Der Lieferant muss über Prozesse und Verfahren zur Kontrolle und Überwachung externer Personen verfügen, einschließlich Unterauftragnehmern, Unterauftragsverarbeitern, denen zu Wartungs- oder Reinigungsarbeiten physischer Zugang zu BDS-Bereichen gewährt wird.
18.3 BDS – Videoüberwachung	• Installation von Videoüberwachung in BDS-Bereichen, um unbefugten Zugang und/oder böswillige Aktivitäten zuverlässig aufzuzeichnen oder zu warnen und Ermittlungen zu unterstützen. • Alle Zugangs- und Ausgangspunkte eines BDS-Bereichs müssen videoüberwacht werden. • Kameras sind auf Funktion und Qualität zu testen. 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.
18.4 BDS – Zugang zum Barclays-Netzwerk und zu Barclays-Authentifizierungstoken	• 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 (RSA-Token) erhalten haben, und in vierteljährlichen Abständen eine Abstimmung vornehmen. • Auf Benachrichtigung, dass kein Zugriff mehr benötigt wird (z. B. aufgrund von Mitarbeiterkündigung, Projektneuzuweisung usw.), deaktiviert Barclays die Authentifizierungsdaten innerhalb von 24 Stunden nach dem Tag des Ausscheidens/letzten Arbeitstag/LDIO-Datum. • 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 Kontrolle - 4. Arbeit außerhalb des Unternehmens (Remotezugriff)
18.5 BDS – Unterstützung außerhalb des Unternehmens	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. Remote-Arbeit (auch von zu Hause aus) ist während des normalen Geschäftsablaufs verboten, soweit Dritte vertraglich verpflichtet sind, Dienstleistungen in banktechnischem Raum (Bank Dedicated Space) oder in den Räumlichkeiten des Lieferanten zu erbringen, oder wenn aufsichtsrechtliche Anforderungen gelten. In Business-Continuity-Plänen von Drittanbietern können jedoch für den Fall einer Notfallwiederherstellung/Krise/Pandemie in Abstimmung mit Barclays und im Einklang mit allen Sicherheitsanforderungen Vorkehrungen für die Remote-Arbeit im Rahmen der vertraglichen Vereinbarung getroffen werden.
18.6 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 werden, und durch angemessene Netzwerkzugriffskontrollen dürfen nur Geräte mit entsprechender Berechtigung erlaubt werden. Siehe Kontrolle - 2. Perimeter- und Netzwerksicherheit
18.7 BDS – Drahtlosnetzwerk	Deaktivieren des Wireless-Netzwerks zur BDS-Netzwerkbereitstellung für Barclays-Services
18.8 BDS – Endpunkt-Sicherheit	Computer innerhalb des BDS-Netzwerks müssen einen sicheren Desktop (einschließlich Laptops) haben, der in Übereinstimmung mit den bewährten Praktiken der Branche konfiguriert ist. Bewährte Praktiken der Branche müssen umgesetzt werden und die Sicherheit von BDS-Endpunktgeräten muss unter anderem folgende Punkte umfassen: • Vollständige Festplattenverschlüsselung. • 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. • Die Aktivierung von USB für das Kopieren von Barclays-Informationen/Daten auf externe Medien • Aktualisiert mit den neuesten Anti-Malware-Signaturen und Sicherheitspatches. • Deaktivierung des Druckspoolerdienstes • Der Austausch/die Übertragung von Barclays-Informationsressourcen/-Daten über Instant-Messaging-Tools/-Software sollte deaktiviert werden. • Erkennen, Stoppen und Beheben des Vorhandenseins und/oder der Verwendung nicht autorisierter Software, einschließlich schädlicher Software. • Timeout bei Sperrbildschirm, Beschränkung der TCP/IP-Verbindung auf das Unternehmensnetzwerk, Advanced EPS-Sicherheitsagent zur Erkennung verdächtiger Verhaltensweisen Siehe Kontrolle - 8. Endpunkt-Sicherheit
18.9 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.
18.10 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 gegenüber Barclays 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 Unterauftragnehmer/Unterauftragsverarbeiter 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 Nichtkonformität von Kontrollen muss Barclays eine Risikobewertung durchführen und einen Zeitrahmen für Abstellmaßnahmen vorgeben. Anschließend muss der Lieferant etwaige verlangte Abstellmaßnahmen innerhalb dieses Zeitrahmens ausführen.

Der Lieferant muss Barclays in Bezug auf die Inspektion und die bei der Inspektion vorgelegten Unterlagen in angemessener Weise unterstützen. Die Dokumentation muss ausgefüllt und umgehend an Barclays zurückgesendet werden. Der Lieferant muss Barclays außerdem mit einem Beurteilungs-Fragesteller sowie mit den im Zuge einer Sicherheitsrisikoüberprüfung verlangten Nachweisen unterstützen.

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 Unterauftragnehmern, Unterauftragsverarbeitern befindliche Räumlichkeiten, die nur für Barclays zur Verfügung gestellt werden und von denen aus die Dienste erbracht oder zur Verfügung gestellt werden.
Bewährte Praktiken der Branche	Verwendung der bewährten und derzeit auf dem Markt führenden Praktiken, Verfahren, Standards und Zertifizierungen. Gewährleistung des Maßes an Fachkenntnis und Sorgfalt, das von einem professionellen Unternehmen mit hoher Fachkompetenz, Erfahrung und Marktpräsenz erwartet werden kann, das Dienstleistungen erbringt, die mit den für Barclays erbrachten Dienstleistungen identisch oder vergleichbar sind.
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.
Cyber-Sicherheit	Die Anwendung von Technologien, Prozessen, Kontrollen und organisatorischen Maßnahmen zum Schutz von Computersystemen, Netzwerken, Programmen, Geräten und Daten vor digitalen Angriffen, bei denen es unter anderem zu unbefugter Offenlegung, Zerstörung, Verlust, Änderung, Diebstahl oder Beschädigung von Hardware, Software oder Daten kommen kann.
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.
Multifaktor-Authentifizierung (MFA)	Authentifizierung, für die zwei oder mehr unterschiedliche Authentifizierungstechniken erforderlich sind. Ein Beispiel ist die Verwendung eines Sicherheitstokens. Erforderlich für eine erfolgreiche Authentifizierung ist dabei etwas, das sich im Besitz der betreffenden Einzelperson befindet (d. h. das Sicherheitstoken), und etwas, das dem Benutzer bekannt ist (d. h. die Sicherheitstoken-PIN).
Personenbezogene Daten	Alle Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Privilegierter Zugriff	Zuweisung von speziellen (über den Standard hinausgehenden) Zugriffsrechten, Berechtigungen oder Kompetenzen an einen Benutzer, Prozess oder Computer.
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.
Remotezugriff	Technologie und Techniken, mit denen autorisierte Benutzer von einem externen Standort aus Zugang zu den Netzwerken und Systemen eines Unternehmens erhalten.
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.
Sicherheitsvorfall	Bei Sicherheitsvorfällen handelt es sich laut Definition unter anderem um folgende Ereignisse: • 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.
Virtuelle Maschine:	Die vollständige Umgebung, die die Ausführung von Gastsoftware unterstützt. HINWEIS: Eine virtuelle Maschine ist eine vollständige Verkapselung der virtuellen Hardware, der virtuellen Laufwerke und der zugehörigen Metadaten. Virtuelle Maschinen ermöglichen das Multiplexing der zugrunde liegenden physischen Maschine über eine Softwareschicht, die als Hypervisor bezeichnet wird.

Bankgeheimnis

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

Kontrollbereich / Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Funktionen und Verantwortlichkeiten	Der Lieferant muss Funktionen, Verantwortlichkeiten und Haftung 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, Verantwortlichkeiten und Haftung 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, Prozesse und Verfahren 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 und regelmäßig getestet 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. Der Lieferant muss zeitnah Abhilfemaßnahmen ergreifen. 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 zum damit verbundenen Risiko. 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 geltenden Gesetzen und Vorschriften im betreffenden Land mit Bankgeheimnis umgesetzt werden.	Wird dieser Grundsatz nicht umgesetzt, könnten unangemessen geschützte Kundendaten (CID) gefährdet werden, was rechtliche und behördliche Strafmaßnahmen oder Rufschädigung zur Folge haben kann.

Anhang B: Glossar

** Daten, durch die Kunden identifiziert werden, sind spezielle Daten auf Grund der in der Schweiz und in Monaco geltenden 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 Mitarbeiter direkt zuzuordnende Einzelpersonen, oder jegliche Einzelpersonen, die dem Lieferanten zeitlich begrenzt Leistungen erbringen (z. B. Berater)
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	Ein 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 C: 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 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	Name des Kunden/Interessenten	Container-Nummer / Container-Kennung	Geburtsort	Jede strikt interne Kennung einer CID-Hosting-/-Verarbeitungsanwendung
	Firmenname	Nummer des MACC (Geldkonto unter einer Avaloq-Container-Kennung)	Geburtsdatum	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. Großbritannien) ansässig sind, eine E-Mail senden oder Dokumente an sie weitergeben.

1. Kundenname

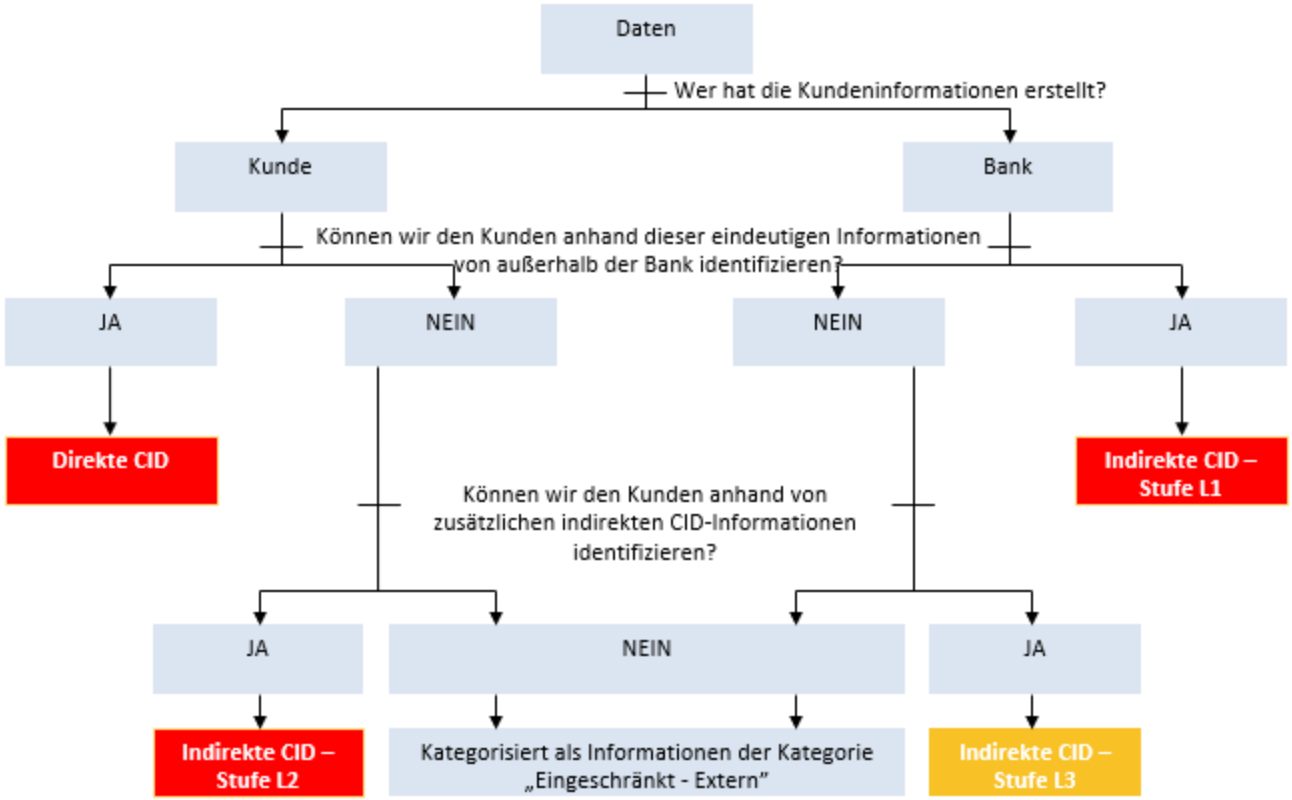
   (DCID) = Verletzung des Bankgeheimnisses

2. Container-Kennung

   (ICID der Stufe L1) = Verletzung des Bankgeheimnisses

3. Vermögensverhältnisse + Staatsangehörigkeit

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


Daten
Wer hat die Kundeninformationen erstellt?
Kunde
Bank
Können wir den Kunden anhand dieser eindeutigen Informationen von außerhalb der Bank identifizieren?
JA
NEIN
NEIN
JA
Direkte CID
Indirekte CID – Stufe L1
Können wir den Kunden anhand von zusätzlichen indirekten CID-Informationen identifizieren?
JA
NEIN
JA
Indirekte CID – Stufe L2
Kategorisiert als Informationen der Kategorie „Eingeschränkt - Extern"
Indirekte CID – Stufe L3

Anhang D: Barclays-Kennzeichnungsschema für Informationen

Tabelle D1: 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 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.	• Kundenname • Adresse des Kunden • Unterschrift • IP-Adresse des Kunden (weitere Beispiele in Anhang D)

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 Rahmenkonzept (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).	• Strategien und Budgets. • Leistungsbeurteilungen. • Löhne und personenbezogene Daten von Mitarbeitern • Schwachstellenbewertungen. • Befunde und Berichte einer Betriebsprüfung.

	Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	
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 D2: 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-Datenübermittlungen 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 Arbeit außerhalb des Unternehmens eingehalten werden. Es muss gewährleistet sein, dass einem bei der Arbeit niemand in die Dokumente schauen kann, 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.
Anteil	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 Informationsressource zugewiesen sein.	• Ressourcen müssen einem Verantwortlichen für die Informationsressource zugewiesen sein.	• Ressourcen müssen einem Verantwortlichen für die Informationsressource 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 zweckgerechte 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 zweckgerechte 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 zweckgerechte 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 zweckgerechte 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 zweckgerechte 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 zweckgerechte Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente). • Für den Druck vorgesehene Ressourcen müssen mithilfe sicherer Druckprogramme gedruckt werden. • Elektronische Ressourcen müssen durch zweckgerechte LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.
Anteil	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung erhalten. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen.	• 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.	• Ausgedruckte Ressourcen 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.	• 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, 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.	• 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 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.

		• Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübermittlung außerhalb des internen Netzwerks verläuft.	• Ressourcen dürfen nur an Personen verteilt werden, denen vom Verantwortlichen für die Informationsressource 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 Datenübermittlung 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.