Kontrollpflichten externer Lieferanten

Physische Sicherheit (technische Kontrollen)

V14.0 Oktober 2024

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Zugangskontrolle (TC 5.1)	Für alle gesicherten Bereiche sind Regeln für die Zugangskontrolle zu definieren, die durch formal genehmigte Verfahren und definierte Verantwortlichkeiten unterstützt werden. Gesicherte Bereiche sind durch geeignete Zutrittskontrollen und Zugangspunkte mittels elektronischer, mechanischer oder digitaler Zugangskontrollen zu schützen. Der logische und administrative Zugriff auf elektronische Zutrittskontrollsysteme muss auf autorisiertes Personal beschränkt werden, und der Zugriff auf physische Schlüssel und Kombinationen muss streng verwaltet und kontrolliert werden. Es muss ein Audit-Trail mit Inhabern von Anmeldeinformationen/Schlüsseln/Kombinationen geführt werden, der die Erteilung, Änderung und Aufhebung von Zugangsberechtigungen umfasst. Alle Zugangsdaten müssen effektiv verwaltet werden, um das Risiko eines unbefugten Zugriff zu verringern. Zugangsdaten müssen in Übereinstimmung mit den Zugriffssteuerungsverfahren des Lieferanten verwaltet werden. Individuelle Zugangsdaten können nur nach Eingang der entsprechenden Genehmigung ausgegeben werden. Alle Zugangsdaten für Bereiche mit Zugangsbeschränkung müssen in angemessenen Abständen erneut zertifiziert werden. Wenn der Zugang zu einem Gelände oder einem eingeschränkten Bereich nicht mehr erforderlich ist, muss die für die Verwaltung der Zugangsdaten zuständige Funktion die Zugangsdaten innerhalb von 24 Stunden nach Erhalt der Benachrichtigung der jeweiligen Geschäftseinheit oder Funktion über die Änderung der Anforderungen für den betreffenden	Die Aufrechterhaltung eines effektiven Zutrittskontrollsystems und der Prozesse und Verfahren für das Zugriffsmanagement ist eine wichtige Komponente innerhalb der mehrschichtigen Kombination von Kontrollen, die erforderlich sind, um das Gelände vor unbefugtem Zugriff zu schützen und die Sicherheit von Ressourcen zu gewährleisten. Sind keine effektiven Maßnahmen zur Zugangskontrolle vorhanden, besteht das Risiko, dass unbefugte Personen in die Standorte oder in Bereiche mit Zugangsbeschränkungen an den Standorten des Lieferanten gelangen. Dies kann das Risiko für Verluste von oder Schäden an Ressourcen von Barclays erhöhen, woraus sich wiederum finanzielle Einbußen und damit verbundenen Rufschädigungen bzw. Konventionalstrafen oder Zensur ergeben.

	Mitarbeiter (z. B. Wechsel der Rolle oder der Verantwortlichkeiten oder Kündigung des Beschäftigungsverhältnisses) deaktivieren.	
2. Perimeterschutz und Sicherheit von Gebäuden und Flächen (TC 5.2)	Entsprechend dem identifizierten und erwarteten Risiko- und Bedrohungsumfeld sind Sicherheitszonen zu definieren und zu implementieren, um Bereiche zu schützen, die Informationen und andere zugehörige Ressourcen enthalten. Physische Sicherheit für Büros, Räume und Einrichtungen (einschließlich Zugangskontrollsystemen, Sicherheitskameras, Einbruchserkennungssystemen und anderer geeigneter technischer Kontrollen) ist auf der Grundlage des aktuellen und erwarteten Bedrohungsniveaus risikoorientiert zu gestalten und zu implementieren und muss den ausgeführten Geschäftsprozessen sowie dem Informations- und Anlagenwert entsprechen. Sicherheitsprozesse für das Arbeiten in gesicherten Bereichen müssen entwickelt und implementiert werden. Es sind Clear Desk-Regeln (Regeln für einen aufgeräumten Arbeitsplatz) für Papiere und Wechselspeichermedien sowie Clear Screen-Regeln für Einrichtungen zur Informationsverarbeitung zu definieren und entsprechend durchzusetzen. Alle eigenständigen Rechenzentren, Cloud-Anbieter, Datenzentren und Kommunikationseinrichtungen (einschließlich Serverräumen und eigenständiger Kommunikationsschränke) müssen wirksam gesichert werden, um unbefugten Zugriff und Diebstahl oder Beschädigung von Ressourcen oder Daten von Barclays zu verhindern. Wenn sich Installationen an gemeinsam genutzten Standorten befinden, müssen wirksame Sicherheitskontrollen eingerichtet sein, um diskrete Trennung und Überwachung zu bewirken.	Damit sollen die in Datenzentren, Rechenzentren und in Räumlichkeiten des Lieferanten (unterhalten vom Lieferanten oder Dritten) aufbewahrten Ressourcen bzw. Daten von Barclays vor dem Risiko von Verlusten, Schäden oder Diebstahl infolge des unbefugten Zugangs zu Bereichen mit Zugangsbeschränkungen geschützt werden.

3. Schutz vor physischen Gefahren für Infrastruktur und Ressourcen (TC 5.3)	Entsprechend der aktuellen und erwarteten Bedrohungsumgebung ist der Schutz vor physischen Gefahren für Infrastruktur und Ressourcen durch den Einsatz von Sicherheitskameras, Einbruchserkennungssystemen und/oder anderen mehrstufigen Sicherheitskontrollen zu entwickeln und zu implementieren. Räumlichkeiten sind kontinuierlich auf unbefugten physischen Zugang zu überwachen. Die Ausrüstung muss sicher aufgestellt und geschützt werden. Kabel für die Stromversorgung, die Übertragung von Daten oder die Unterstützung von Informationsdiensten müssen vor dem Abfangen durch physischen Zugriff, Störungen oder Beschädigungen geschützt werden. Sicherheitseinrichtungen und -anlagen müssen in Übereinstimmung mit den Anforderungen des Herstellers installiert und gewartet sowie überwacht werden, um die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen sicherzustellen. Die außerhalb des Standorts aufbewahrten Ressourcen von Barclays müssen sowohl bei der Lagerung als auch während des Transports geschützt werden. Die Ausrüstung ist korrekt zu installieren und zu warten und muss den geltenden Branchenstandards entsprechen, damit die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen gewährleistet sind. Installation und Betrieb aller Sicherheitssysteme müssen den geltenden gesetzlichen und aufsichtsrechtlichen Anforderungen entsprechen. Wo vorhanden, müssen Anliefer- und Ladebereiche angemessen kontrolliert und von den Betriebsanlagen isoliert werden, um unbefugten Zugang und potenzielle Gefahren durch unbestätigte Lieferungen zu vermeiden.	Durch Bereitstellung und Betrieb physischer Sicherheitskontrollen, die den aktuellen und erwarteten Bedrohungen entsprechen, werden die Auswirkungen von unbefugtem Zugang, Diebstahl oder vorsätzlichen Schäden an Räumlichkeiten und Vermögenswerten begrenzt oder verhindert.

Dieser Standard muss in Verbindung mit dem folgenden Standard gelesen werden, in dem die als innerhalb des Geltungsbereichs liegenden identifizierten Managementkontrollen angewendet werden müssen:

Kontrollpflicht für Drittanbieter (TPSPCO), Managementkontrollanforderungen – Informationen, Cyber- und physische Sicherheit, Technologie, Wiederherstellungsplanung, Datenschutz, Datenmanagement, PCI DSS und EUDA.