Obligations de contrôle pour les fournisseurs externes

Sécurité physique (contrôles techniques)

V14.0 – Octobre 2024

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Contrôle d'accès (TC 5.1)	Des règles de contrôle d'accès doivent être définies pour toutes les zones sécurisées, soutenues par des procédures officielles approuvées et des responsabilités définies. Les zones sécurisées doivent être protégées par des contrôles d'entrée et des points d'accès appropriés à l'aide de contrôles d'accès électroniques, mécaniques ou numériques. L'accès logique et administratif aux systèmes de contrôle d'accès électronique doit être limité au personnel autorisé, et l'accès aux clés physiques et combinaisons doit être géré et contrôlé de manière stricte. Une piste d'audit des détenteurs d'identifiants/de clés/de combinaisons doit être tenue à jour et couvrir l'octroi, la modification et la révocation des autorisations d'accès. Tous les identifiants d'accès doivent être gérés efficacement pour réduire le risque d'accès non autorisé. Tous les identifiants d'accès doivent être gérés conformément aux procédures de contrôle d'accès du fournisseur. Tous les identifiants d'accès uniques peuvent être émis uniquement à réception de l'approbation appropriée. Tous les identifiants d'accès aux zones à accès restreint doivent être recertifiés à intervalle approprié. Si l'accès à un local ou à une zone à accès restreint n'est plus nécessaire, les identifiants d'accès doivent être désactivées par la fonction responsable de l'administration des identifiants d'accès dans les 24 heures suivant la réception de la notification de l'unité commerciale ou de la fonction concernée informant du changement d'exigences pour l'employé en question (par ex. changement de rôle ou de responsabilités, licenciement ou embauche).	Le maintien d'un système de contrôle d'accès efficace et de processus et procédures de gestion des accès est un élément essentiel de la combinaison de contrôles à plusieurs niveaux requise pour protéger les locaux contre les accès non autorisés et assurer la sécurité des actifs. En l'absence de mesures de contrôle d'accès efficaces, il est possible que des individus non autorisés entrent sur les sites du fournisseur ou dans les zones à accès restreint de ces sites. Cela accroît le risque de perte ou d'atteinte aux actifs de Barclays, ce qui peut causer des pertes financières, porter atteinte à la réputation de Barclays et/ou entraîner des amendes ou une censure.

2. Sécurité des périmètres, bâtiments et espaces (TC 5.2)	Des périmètres de sécurité doivent être définis et mis en œuvre pour protéger les zones contenant des informations et d'autres actifs associés, en fonction de l'environnement de risque et de menace identifié et anticipé. La sécurité physique des bureaux, des salles, et des installations (y compris les systèmes de contrôle d'accès, les caméras de sécurité, les systèmes de détection des intrusions et autres contrôles techniques appropriés) doit être conçue et mise en œuvre selon une approche basée sur les niveaux de menace actuels et anticipés et doit être en adéquation avec les processus d'entreprise réalisés, ainsi que les informations et la valeur des actifs. Des processus de sécurité pour travailler dans des zones sécurisées doivent être conçus et mis en œuvre. Des règles de rangement pour les papiers et supports de stockage amovibles et des règles de verrouillage des écrans pour les installations de traitement des informations doivent être définies et appliquées de manière appropriée. Tous les centres de données tiers (autonomes ou en colocation), fournisseurs de services cloud, halls de données et installations de communication (y compris les salles de serveurs et les armoires de communication autonomes) doivent être sécurisés de manière efficace pour prévenir tout accès non autorisé, vol ou dommage des actifs ou données de Barclays. Lorsque les installations se trouvent dans des emplacements partagés, des contrôles de sécurité efficaces doivent être mis en place pour assurer une séparation et une surveillance discrètes	Pour protéger les actifs et données de Barclays conservés dans des centres de données, des halls de données et d'autres sites du fournisseur (gérés par le fournisseur ou par des tiers) contre le risque de perte, d'atteinte ou de vol suite à un accès non autorisé à un espace faisant l'objet d'une restriction d'accès.
3. Protection contre les menaces physiques pesant sur l'infrastructure et les ressources (TC 5.3)	La protection contre les menaces physiques pesant sur l'infrastructure et les actifs doit être conçue et mise en œuvre par le déploiement de caméras de sécurité, de systèmes de détection des intrusions et/ou d'autres contrôles de sécurité multi-niveaux adaptés à l'environnement de menaces existant et anticipé. Les locaux doivent être surveillés en permanence pour détecter tout accès physique non autorisé.	Le déploiement et l'utilisation de contrôles de sécurité physiques adaptés aux menaces actuelles et anticipées limiteront ou empêcheront l'impact d'un accès non autorisé, d'un vol ou de dommages intentionnels sur les locaux et les actifs.

	L'équipement doit être sécurisé et protégé sur le site. Les câbles transportant de l'électricité, des données ou des informations doivent être protégés contre les interceptions physiques, les interférences ou les dommages. Les équipements et installations de sécurité doivent être installés et entretenus conformément aux exigences du fabricant, et surveillés afin de garantir la disponibilité, l'intégrité et la confidentialité des informations. Les actifs de Barclays détenus hors site doivent être protégés au repos et en transit. Les équipements doivent être installés et entretenus correctement et conformément aux normes en vigueur de l'industrie afin de garantir la disponibilité, l'intégrité et la confidentialité des informations. L'installation et le fonctionnement de tous les systèmes de sécurité doivent être conformes aux exigences légales et réglementaires en vigueur. Le cas échéant, les zones de livraison et de chargement doivent être correctement contrôlées et isolées des installations opérationnelles afin d'éviter tout accès non autorisé et toute menace potentielle provenant de livraisons non vérifiées.	

Cette norme doit être lue conjointement avec la norme suivante, lorsque les contrôles de gestion identifiés comme entrant dans le champ d'application doivent être appliqués :

Obligation de contrôle pour les fournisseurs de services tiers (TPSPCO), exigences de contrôle de la gestion - informations, cybersécurité et sécurité physique, technologie, plan de rétablissement, confidentialité des données, gestion des données, PCI DSS et EUDA.