Obligations de contrôle pour les fournisseurs externes

Sécurité physique (contrôles techniques)

Version 12.0 – Octobre 2022

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Contrôle d'accès (TC 5.1)	Un contrôle d'accès électronique, mécanique ou numérique doit être déployé et géré sur tous les sites sur lesquels des activités liées aux contrats Barclays sont menées. Tous les systèmes de sécurité doivent être installés, exploités et entretenus conformément aux exigences légales et réglementaires. 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 peuvent être émis uniquement à réception de l'approbation appropriée. Tout accès aux zones à accès restreint doit être recertifié 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). Si un travail à distance s'impose lorsqu'un fournisseur ou ses sous-traitants accèdent aux informations de Barclays en format physique ou virtuel et dont la nature en limite la	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.

	diffusion, les stockent ou en assurent le traitement (incluant les données personnelles ou les informations à caractère sensible qui sont fournies au fournisseur lorsqu'il a besoin d'en avoir connaissance), ces arrangements pris avec Barclays doivent être approuvés par le fournisseur avant qu'un accès à ces données ne lui soit accordé.	
2. Système de détection des intrusions et caméras de sécurité (TC 5.2)	Des systèmes de détection des intrusions et des caméras de sécurité doivent être déployés pour dissuader, détecter, surveiller et identifier tout accès inapproprié ou toute activité criminelle. L'équipement déployé doit être adapté aux menaces de sécurité physiques dominantes identifiées par l'évaluation des risques de sécurité pour chaque site. Tous les systèmes de vidéosurveillance et de détection des intrusions doivent être installés, exploités et entretenus conformément aux normes actuelles du secteur (par ex. de l'Organisation internationale de normalisation (ISO), le contrôle des systèmes et des organisations (SOC), les exigences légales et réglementaires en vigueur et les spécifications actuelles des fabricants). Des procédures doivent être mises en place pour veiller à ce que les alarmes des systèmes de détection des intrusions et des caméras de sécurité soient surveillées et gérées efficacement. L'accès au système de sécurité doit être limité au personnel autorisé.	Les systèmes de détection des intrusions et de vidéosurveillance font partie des contrôles qui protègent un site contre tout accès non autorisé et assurent la sécurité des actifs. Si ces systèmes ne sont pas installés, exploités, surveillés et entretenus correctement, il est possible qu'un individu non autorisé accède aux sites et aux bâtiments contenant des données et des actifs de Barclays, et qu'un accès non autorisé ne soit pas détecté à temps.
3. Centres de données, halls et installations de communication (TC 5.3)	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. Des couches de contrôles techniques, physiques et humains, ainsi que des procédures propres au site doivent être en place dans tous les	Pour protéger les actifs et données de Barclays conservés dans des centres de données, des halls de données et d'autres sites critiques similaires 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.

	centres de données afin de protéger efficacement le périmètre, le bâtiment, l'intégrité des halls de données et tous les autres espaces critiques. Ces contrôles incluent, sans s'y limiter, les caméras de sécurité, les systèmes de détection des intrusions, les contrôles d'accès et les agents de sécurité. Lorsque les installations se trouvent dans des emplacements partagés, une sécurité efficace doit être déployée autour de leur séparation discrète.	

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.