Obligations de contrôle pour les fournisseurs externes

Sécurité physique

Version 10.0 - Octobre 2020

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Évaluations des risques de sécurité	Les fournisseurs doivent mener des évaluations des risques de sécurité afin de vérifier les processus et les mesures portant sur la sécurité physique. Les évaluations doivent être réalisées par un individu qualifié ayant l'expérience adéquate. Elles doivent tenir compte de l'adéquation et de l'efficacité des contrôles de sécurité physique pour atténuer à la fois le profil de menace actuel du bâtiment et tout problème émergent susceptible d'avoir un impact sur le site. La fréquence de l'évaluation des risques doit être adaptée aux fins et à la criticité du site. Les sites critiques pour le fonctionnement des processus Barclays (y compris les centres de données) doivent être évalués au moins une fois par an. Les résultats des évaluations des risques de sécurité doivent être documentés, des plans d'action doivent être développés, et les problèmes et risques identifiés doivent être affectés à un propriétaire et suivis jusqu'à leur résolution. Barclays doit être tenu informé de tous les résultats significatifs dans les 10 jours ouvrés suivant leur découverte.	Les évaluations des risques de sécurité constituent une exigence clé pour évaluer avec précision l'environnement, les contrôles et les processus liés à la sécurité physique du fournisseur, et s'assurer de leur efficacité. Elles mettent au jour les vulnérabilités et les déficiences nouvelles ou existantes en matière de contrôle, et réduisent le risque de pertes ou d'atteinte aux actifs de Barclays, d'atteinte à la réputation de Barclays, et/ou d'amendes ou de censure.
2. Contrôle d'accès	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 au système doit être limité au personnel autorisé, et l'accès aux clés et combinaisons doit être géré et contrôlé de manière stricte.	Un contrôle d'accès efficace fait partie des contrôles qui protègent le site contre tout accès non autorisé et assurent 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.

	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 sont émis à réception de l'approbation appropriée. Tout accès aux zones à accès restreint doit être recertifié à intervalle approprié. Si l'accès à un site ou à une zone à accès restreint n'est plus nécessaire, les identifiants d'accès doivent être désactivés dans les 24 heures qui suivent notification.	
3. Système de détection des intrusions et caméras de sécurité	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 vidéosurveillance et de détection des intrusions doivent être installés, exploités et entretenus conformément aux normes acceptées du secteur. L'accès au système 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 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.
4. Personnel de sécurité	Le personnel de sécurité déployé doit être adapté aux menaces de sécurité physiques dominantes pour chaque site. Tout le personnel de sécurité (qu'il soit employé par le fournisseur, un propriétaire ou un fournisseur externe) doit être embauché via un fournisseur de service agréé et disposant des licences adéquates, et conformément à la législation locale. Le personnel doit suivre une formation sur la sécurité adaptée à son rôle et à ses responsabilités. Toute formation dispensée doit être documentée, et un registre des formations doit être tenu pour tout le personnel de sécurité.	Le personnel de sécurité fait partie des contrôles qui protègent un site contre tout accès non autorisé et assurent la sécurité des actifs. Si le personnel de sécurité déployé n'est pas adapté aux menaces de sécurité dominantes ou n'est pas formé correctement, il est possible qu'un individu non autorisé accède aux sites contenant des données et des actifs de Barclays, ou qu'un accès non autorisé ne soit pas détecté à temps. 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.

5. Gestion des incidents de sécurité et niveaux de réponse	Les fournisseurs doivent mettre en place des procédures de gestion des incidents de sécurité et d'enquête le cas échéant. Tout incident de sécurité affectant des actifs de Barclays doit être signalé à Barclays dans les 48 heures. Les rapports officiels et les détails de l'enquête doivent être partagés dès que techniquement possible, mais au plus tard dans les 10 jours ouvrés qui suivent l'incident. Cela inclut les données du contrôle d'accès et les images des caméras de sécurité, conformément au droit et aux réglementations locaux.	Le non-respect de cette exigence prive Barclays de la certitude que le fournisseur dispose des procédures documentées adéquates pour gérer les incidents de sécurité. Le non-respect de cette exigence peut se traduire par l'application de mesures inappropriées suite à un incident, augmentant ainsi le risque de pertes ou d'atteinte aux actifs de Barclays, d'atteinte à la réputation de Barclays, et/ou d'amendes ou de censure.
6. Transport	Les fournisseurs doivent s'assurer que tous les actifs et données de Barclays sont transportés de manière sécurisée, avec des contrôles adaptés en place, proportionnels à la valeur des actifs et données transportés (aussi bien d'un point de vue financier que d'atteinte à la réputation) et à l'environnement de menaces dans lequel ils sont transportés.	Pour protéger les données et les actifs de Barclays en transit entre les sites du fournisseur et/ou les sites de Barclays, et ainsi réduire le risque de pertes, de vol ou de dommages, d'atteinte à la réputation de Barclays, et/ou d'amendes ou de censure en résultant.
7. Halls et centres de données	Tous les centres de données tiers (autonomes ou en colocation), fournisseurs de service de cloud et halls de données doivent être efficacement sécurisés 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 centres de données afin de protéger efficacement le périmètre, le bâtiment et l'intégrité des halls de données. Ces contrôles incluent, sans s'y limiter, les caméras de sécurité, les systèmes de détection des intrusions et les contrôles d'accès.	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.