

Obligations de contrôle pour les fournisseurs externes

Sécurité physique

| Intitulé du contrôle | Description | Raisons de l'importance |
|---|---|---|
| 1. Évaluations des risques de sécurité | <p>Les fournisseurs doivent mener des évaluations des risques de sécurité afin de vérifier les processus et les mesures portant sur la sécurité physique.</p> <p>Les fournisseurs doivent s'assurer que les problèmes identifiés sont résolus selon un plan correctif (action, propriété, date de livraison) et signalés à Barclays de façon appropriée.</p> | <p>Garantir une évaluation précise de l'environnement, des contrôles et des processus liés à la sécurité physique du fournisseur, et s'assurer de leur efficacité. Mettre au jour les éventuelles vulnérabilités et déficiences en matière de contrôle qui ont été traitées de façon inappropriée, et réduire le risque de pertes ou d'atteinte aux actifs de Barclays, d'atteinte à la réputation de Barclays, et/ou d'amendes ou d'une censure.</p> |
| 2. Contrôle d'accès | <p>Les fournisseurs doivent documenter et déployer des systèmes et des processus de contrôle d'accès efficaces applicables à l'ensemble de leur personnel.</p> | <p>S'assurer que seul le personnel autorisé est habilité à accéder aux différentes installations des sites du fournisseur et ainsi réduire le risque de perte ou d'atteinte aux actifs de Barclays pouvant résulter en une perte financière, en une atteinte à la réputation de Barclays, et/ou en des amendes ou une censure.</p> |
| 3. Détection électronique d'intrusion et caméras de vidéosurveillance | <p>Les fournisseurs doivent déployer des mesures appropriées, telles que des alarmes, des capteurs de mouvement vidéo et des caméras de vidéosurveillance, afin de surveiller, détecter et identifier tout accès non autorisé et incident de sécurité. L'équipement doit être conforme aux normes nationales et du secteur en termes d'installation, de fonctionnement, de surveillance et de maintenance. Les images et données doivent être stockées dans des lieux sécurisés à l'accès limité, doivent pouvoir être recherchées en fonction de l'heure et de la date, et doivent être conservées pour une durée minimale de 30 jours, ou conformément aux réglementations et au droit locaux en vigueur.</p> | <p>S'assurer qu'aucun individu non autorisé n'accède aux sites et aux bâtiments contenant des données et des actifs de Barclays, et que tout accès non autorisé est détecté au plus tôt.</p> |

| | | |
|--|--|---|
| 4. Agents de sécurité | Les fournisseurs doivent déployer des agents de sécurité proportionnellement aux risques identifiés dont la prévention nécessite une présence physique et contre lesquels les systèmes électroniques et/ou surveillés à distance n'assurent pas une protection suffisamment efficace. Les agents de sécurité doivent avoir suivi une formation adaptée et être déployés conformément au droit, aux réglementations, et aux exigences en matière de licence locaux. | Le non-respect de cette exigence peut se traduire par l'intrusion de personnel non autorisé dans les différentes installations des sites du fournisseur et contenant des données et des actifs de Barclays, ou par la non-détection en temps opportun d'une telle intrusion, augmentant ainsi le risque de perte ou d'atteinte aux actifs de Barclays pouvant résulter en une perte financière, en une atteinte à la réputation de Barclays, et/ou en 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. Lorsque des incidents de sécurité affectent des actifs de Barclays, les rapports d'incidents et les détails de l'enquête doivent être partagés, y compris les données de contrôle d'accès et les images des caméras de vidéosurveillance si nécessaire, conformément au droit et aux réglementations locaux. | En cas de non-respect de cette exigence, Barclays est dans l'incapacité d'avoir la certitude que le fournisseur dispose des procédures testées et 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 toutes les données de Barclays sont transportés de manière sécurisée. | Protéger les données et les actifs de Barclays lors de leur transport entre les sites du fournisseur et/ou les sites de Barclays, et ainsi réduire le risque de pertes, de vol ou de dommages, et l'atteinte à la réputation de Barclays, et/ou le risque d'amendes ou de censure en résultant. |