Obligation de contrôle des fournisseurs (SCO)

Exigences en matière de contrôle de gestion –

Informations, cybersécurité et sécurité physique, technologie, plan de rétablissement, confidentialité des données, gestion des données et EUDA

MC 1.0 – Gouvernance et responsabilité

Le fournisseur doit avoir mis en place un cadre standard et homogène du secteur pour assurer la gouvernance de la technologie de l'information, de la sécurité de la technologie de l'information, de la sécurité physique, du plan de rétablissement, de la gestion des données et de la gestion des informations personnelles (protection des données/confidentialité des données) (NIST, ISO/CEI 27001, COBIT, BS10012, SSAE 18, ITIL) ou un cadre standard similaire en ce qui concerne les meilleures pratiques du secteur, afin de s'assurer que son procédé, sa technologie et son environnement physique fonctionnent efficacement grâce à des mesures de protection ou des contre-mesures. Un programme de gouvernance bien structuré à l'échelle de l'entreprise doit veiller à ce que les concepts fondamentaux de disponibilité, d'intégrité et de confidentialité soient renforcés par des contrôles adéquats. Les contrôles doivent être conçus pour atténuer ou réduire les risques de perte, de perturbation ou de corruption des informations et le fournisseur doit s'assurer que les contrôles des exigences de Barclays sont appliqués et fonctionnent efficacement pour protéger le ou les services dispensés à Barclays.

Un cadre de gouvernance doit être développé et doit inclure des mesures de protection administratives, techniques et physiques visant à protéger les actifs et les informations/données contre tout/toute perte accidentelle et/ou délibérée, divulgation, altération ou destruction, vol, utilisation inappropriée ou mauvaise utilisation et contre tout/toute accès, utilisation ou divulgation non autorisés.

Ce programme de gouvernance et de responsabilité doit inclure, mais sans s'y limiter, les éléments suivants :

- Politiques de gouvernance : un ensemble de politiques de gouvernance doit être défini, approuvé par la direction, publié et communiqué aux employés du fournisseur et aux parties concernées et maintenu à jour.
    - Des programmes énonçant des normes, des politiques et des procédures et créant efficacement, mettant en œuvre et mesurant en permanence l'efficacité de l'application des normes et politiques.
    - Un programme de gouvernance exhaustif présentant une structure de direction et un contrôle exécutif clairs pour faire émerger une culture de sensibilisation et de responsabilité.
    - Une communication continue sur les politiques et procédures approuvées dans l'ensemble de l'organisation.
    - Une adaptation des exigences juridiques aux politiques et pratiques, à la protection des données dès la conception et à d'autres contrôles pour garantir la mise en œuvre efficace des politiques et des procédés
- Les politiques de tous les domaines doivent être révisées à des intervalles planifiés ou en cas de modifications significatives afin de s'assurer qu'elles restent appropriées, adéquates et efficaces.
    - Ces politiques et procédures/normes doivent être révisées régulièrement (au moins une fois par an ou à chaque modification significative, selon le cas).

    - La nomination d'une personne ou une d'équipe expérimentée et qualifiée avec laquelle Barclays peut collaborer pour répondre aux exigences de SCO, y compris en ce qui concerne la sécurité physique et des bâtiments, la sécurité des informations et la cybersécurité, et la gestion des informations personnelles (confidentialité/protection des données), le plan de rétablissement, la gestion des données et de la personne qui veillera à ce que les exigences de contrôle de Barclays ou du fournisseur sont efficacement mises en œuvre et suivies.
    - Le fournisseur doit coordonner et aligner les rôles et responsabilités du personnel en mettant en œuvre, gérant et supervisant l'efficacité des contrôles avec les sous-traitants/sous-traitants ultérieurs internes.
- Le fournisseur doit mettre en œuvre une infrastructure sécurisée et un cadre de contrôle pour protéger l'organisation contre toute menace (incluant la cybersécurité)
- Le fournisseur doit mettre en place un ou plusieurs programmes d'audit indépendants pour vérifier que les contrôles du fournisseur sont mis en œuvre, maintenus, et qu'ils sont effectués au moins une fois par an.

Conseils pour le client du service cloud (fournisseur)

Une politique de sécurité des informations pour le cloud computing doit être définie afin de servir de politique spécifique au client du service cloud. La politique de sécurité des informations du client du service cloud pour le cloud computing doit être conforme aux niveaux acceptables de risques de sécurité des informations de l'organisation pour ses informations et autres actifs. Lors de la définition de la politique de sécurité des informations pour le cloud computing, le client du service cloud doit prendre en compte les éléments suivants :

- Le prestataire de services cloud peut accéder aux informations stockées dans l'environnement de cloud computing et les gérer.
- Les actifs peuvent être gérés dans l'environnement de cloud computing, par exemple les programmes d'application.
- Les processus peuvent s'exécuter sur un service cloud virtualisé multi-tenant.
- Les utilisateurs du service cloud et le contexte dans lequel ils utilisent le service cloud.
- Les administrateurs de services cloud disposant d'un accès privilégié au client du service cloud.
- Les emplacements géographiques de l'organisation du prestataire de services cloud et les pays où le prestataire de services cloud peut stocker les données client du service cloud (y compris le stockage temporaire).

La politique de sécurité pertinente du client du service cloud doit identifier le prestataire de services cloud comme un type de fournisseur et le gérer conformément à la politique de sécurité. Cela devrait permettre de limiter les risques liés à l'accès et à la gestion des données des clients de services cloud associées au prestataire de services cloud.

Le client du service cloud doit tenir compte des lois et réglementations applicables des juridictions qui régissent le prestataire de services cloud, en plus de celles qui régissent le client du service cloud. Le client du service cloud doit obtenir la preuve de la conformité du prestataire

de services cloud aux réglementations et normes pertinentes requises pour l'activité du client du service cloud. Ces preuves peuvent également être des attestations/certificats produits par des auditeurs tiers.

Le fournisseur doit notifier Barclays par écrit dès qu'il est légalement tenu de le faire en cas de fusion, d'acquisition ou de tout autre changement de propriété l'affectant.

MC 2.0 - Gestion des risques

Le fournisseur doit mettre sur pied un programme de gestion des risques qui évalue, atténue et surveille efficacement les risques à travers son environnement contrôlé.

Ce programme doit inclure, mais sans s'y limiter, les éléments suivants :

- Le fournisseur doit disposer d'un cadre de gestion des risques dûment approuvé (par exemple, informations personnelles en cas de traitement de données personnelles, les informations, la cybersécurité et la sécurité physique, la technologie, les données et le plan de rétablissement) et être capable de démontrer son intégration à la stratégie commerciale
- Conformément au cadre de gestion des risques, des évaluations formelles des risques doivent être menées au moins une fois par an, à des intervalles planifiés, à l'aide d'une approche basée sur les risques, ou lors d'événements particuliers, (par ex. suite à un incident ou aux enseignements tirés de cet incident, conjointement à toute modification des systèmes d'informations ou des bâtiments ou espaces physiques) pour déterminer la probabilité et l'impact de tous les risques identifiés en utilisant des méthodes qualitatives et quantitatives. La probabilité et l'impact associé au risque inhérent et résiduel doivent être déterminés de façon indépendante, en tenant compte de toutes les catégories de risques (résultats d'audit, analyses de vulnérabilité et des menaces, et conformité réglementaire, par exemple).
- Établissement et maintien des critères de risque qui comprennent :
    - les critères d'acceptation des risques, et
    - les critères d'évaluation des risques,
- Identification des risques :
    - application du processus d'évaluation des risques pour identifier les risques associés à la perte de confidentialité, d'intégrité et de disponibilité des informations relevant du cadre des risques, et
    - identification des responsables des risques,
- Analyse des risques :
    - évaluation des conséquences potentielles qui en résulteraient si les risques étaient identifiés,
    - évaluation de la probabilité réaliste de l'occurrence des risques identifiés, et

- détermination des niveaux de risque
- Évaluation des risques :
  - comparaison des résultats de l'analyse des risques avec les critères de risque établis, et
  - hiérarchisation des risques analysés pour le traitement des risques
- Gestion des risques :
  - un régime approprié d'options de gestion des risques doit être sélectionné, en tenant compte des résultats de l'évaluation des risques,
  - tous les contrôles nécessaires à la mise en œuvre de la ou des options de gestion des risques choisies doivent être déterminés,
  - une déclaration d'applicabilité qui contient les contrôles nécessaires et la justification des inclusions, qu'elles soient mises en œuvre ou non, doit être produite et
  - Le fournisseur doit s'assurer que les risques identifiés sont réduits à un minimum ou éliminés de l'environnement en hiérarchisant les risques et en mettant en place des contre-mesures. Le fournisseur doit surveiller en permanence les contre-mesures pour qu'elles soient efficaces.
- Le fournisseur doit effectuer au minimum une évaluation annuelle des risques en ce qui concerne la sécurité des informations, la cybersécurité, la sécurité physique, la gestion des informations personnelles (confidentialité des données/protection des données) et le plan de rétablissement. En fonction des environnements spécifiques présentant des menaces actuelles et émergentes, le fournisseur doit envisager une cadence plus fréquente.
  - Les sites essentiels au fonctionnement des processus/services fournis à Barclays (y compris les centres de données) doivent être évalués au moins une fois par an.
- L'organisation doit conserver des informations documentées sur le processus d'évaluation des risques liés à la sécurité des informations.
- Les évaluations des risques associées aux exigences de gouvernance des données (y compris les informations personnelles en cas de traitement des données personnelles) doivent tenir compte des éléments suivants :
  - Classification et protection des données contre toute utilisation, perte, destruction et falsification non autorisées, ou contre tout accès non autorisé.
  - Connaissance des emplacements où les données sensibles sont stockées et transmises à travers les applications, les bases de données, les serveurs et l'infrastructure réseau.
  - Respect des périodes de rétention définies et des exigences de mise au rebut en fin de vie.
- Le fournisseur, lorsqu'il agit en tant que responsable du traitement ou sous-traitant, doit évaluer le risque potentiel en matière de confidentialité lors du traitement de volumes sensibles ou importants de données de Barclays afin de s'assurer que toute modification apportée au traitement des données de Barclays n'entraîne pas de risque pour la confidentialité

- Le fournisseur doit développer et mettre en œuvre la structure de gouvernance organisationnelle afin de permettre une compréhension continue des priorités de l'organisation en matière de gestion des risques en tenant compte du risque d'atteinte à la vie privée

MC 3.0 - Rôles et responsabilités

Il incombe au fournisseur de s'assurer que tous ses employés, y compris, mais sans s'y limiter, les entrepreneurs, sous-traitants, sous-traitants ultérieurs impliqués dans la prestation de services à Barclays, connaissent les exigences de contrôle de Barclays, et les respectent. Le fournisseur doit s'assurer qu'une équipe appropriée de spécialistes et/ou de personnes ayant les compétences requises, ainsi que des rôles et des responsabilités définis pour soutenir et/ou gérer les exigences de contrôle de Barclays, est en place de manière à intervenir efficacement pour assurer la protection du ou des services de Barclays.

Le fournisseur doit définir et communiquer les rôles et les responsabilités pour soutenir efficacement les exigences de contrôle de Barclays. Ces rôles et responsabilités doivent être révisés régulièrement (et dans tous les cas au moins une fois tous les 12 mois) et après chaque modification significative apportée à l'activité ou au modèle d'exploitation du fournisseur.

Il appartient au fournisseur de s'assurer que ses employés, entrepreneurs, sous-traitants/sous-traitants ultérieurs connaissent les exigences de contrôle énoncées par cette norme ainsi que par les politiques et normes connexes, et les respectent. Le fournisseur doit désigner un point de contact pour assurer la liaison avec Barclays en cas de signalement découlant du non-respect des exigences de contrôle. Les exigences contractuelles spécifiques doivent être transmises par écrit aux sous-traitants/sous-traitants ultérieurs du fournisseur.

Conseils pour le client du service cloud (fournisseur)

Le client du service cloud doit convenir avec le prestataire de services cloud d'une attribution appropriée des rôles et responsabilités en matière de sécurité des informations, et confirmer qu'il peut remplir les rôles et responsabilités qui lui sont attribués. Les rôles et responsabilités des deux parties doivent être énoncés dans un accord. Le client du service cloud doit identifier et gérer sa relation avec la fonction d'assistance et de support client du prestataire de services cloud.

Le client du service cloud doit définir ou étendre ses politiques et procédures existantes conformément à son utilisation des services cloud, et informer ses utilisateurs du service cloud de leurs rôles et responsabilités dans l'utilisation du service cloud.

MC 4.0 - Formation et sensibilisation

Le fournisseur doit exécuter en permanence un programme de formation de sensibilisation pour tous les employés du fournisseur, y compris les entrepreneurs, les personnes embauchées à court terme et les consultants. Toutes les personnes ayant accès aux informations ou données de Barclays ou encore à d'autres actifs physiques doivent suivre une formation appropriée et bénéficier de mises à jour régulières

de leur connaissance des politiques, processus et procédures de l'organisation liées à leur fonction au sein de celle-ci. Les niveaux de formation et de mise à jour doivent préparer les employés du fournisseur à remplir leurs fonctions en toute sécurité et s'assurer que les employés du fournisseur comprennent leurs responsabilités lorsqu'ils accèdent à ou traitent des données de Barclays, y compris des données personnelles. Les registres du programme entrepris doivent être consignés dans une plate-forme adaptée de gestion de l'apprentissage ou par le biais d'un processus manuel.

Le fournisseur doit s'assurer que tous ses employés suivent une formation obligatoire complète portant sur la sensibilisation et la formation, et qui inclut la cybersécurité, la sécurité physique, le plan de rétablissement, la gestion des informations personnelles (confidentialité des données/protection des données), la gestion des données, la gestion des services informatiques, l'EUDA et la protection des données de Barclays dans le mois suivant leur arrivée dans l'organisation et/ou après leur arrivée au(x) service(s) de Barclays. En plus d'une remise à niveau chaque année, le fournisseur doit s'assurer de tester ses employés afin de vérifier qu'ils comprennent leurs responsabilités et connaissent les risques associés aux données. Toutes les formations dispensées doivent être enregistrées et tenues à jour pour tous les employés du fournisseur travaillant sur le(s) service(s) de Barclays et produites pour inspection par Barclays sur demande.

Le fournisseur doit s'assurer que son programme de formation à la sensibilisation comprend les sujets de cybersécurité suivants : ingénierie sociale et menaces internes. Il est recommandé au fournisseur d'effectuer des tests de simulation d'attaques d'ingénierie sociale à l'aide de techniques telles que des tests de simulation d'hameçonnage pour tous les employés au niveau de l'entreprise, avec une surveillance continue pour s'assurer que la menace de tels risques est clairement comprise et pour réduire à un minimum les problèmes identifiés.

Les groupes à haut risque, par exemple les personnes disposant d'un accès à un ou des systèmes privilégiés, d'un accès à un espace critique ou à haut risque ou à des postes sensibles pour l'entreprise (y compris les utilisateurs privilégiés, notamment les développeurs et l'assistance, les cadres supérieurs, le personnel en charge de la sécurité des informations, et les parties prenantes tierces) doivent suivre une formation de sensibilisation situationnelle sur la sécurité des informations et la sécurité physique adaptée à leurs rôles et responsabilités.

Tout le personnel de sécurité physique (qu'il soit employé par le fournisseur, un propriétaire ou un fournisseur externe) doit être engagé ou sous contrat par l'intermédiaire d'un prestataire de services accrédité et agréé conformément à la législation locale et, lorsque la juridiction l'exige, être personnellement autorisé à exercer des fonctions de sécurité. Le personnel de sécurité physique doit suivre une formation à la sécurité adaptée à son rôle et à ses responsabilités. Toutes les formations dispensées doivent être documentées et un dossier de formation doit être tenu à jour pour l'ensemble du personnel de sécurité et présenté à Barclays pour inspection sur demande

Le fournisseur doit s'assurer que son personnel tiers ayant accès aux données contenant des informations personnelles est conscient des risques liés à la vie privée et qu'il assume ses fonctions et responsabilités conformément aux politiques, processus, procédures, accords et valeurs de confidentialité organisationnelles connexes. Toutes les formations dispensées doivent être documentées et un dossier de formation doit être tenu à jour pour l'ensemble du personnel et présenté à Barclays pour inspection sur demande

Le fournisseur doit former ses employés à l'exécution efficace de leurs tâches de gestion des données (gestion des éléments de données critiques ou applications gérées par des tiers).

Le propriétaire EUDA du fournisseur doit identifier les employés du fournisseur ayant des responsabilités EUDA et s'assurer qu'ils suivent au moins une fois par an la formation et la sensibilisation correspondant à leur rôle et conserver les preuves qui doivent démontrer la conformité au contrôle.

Conseils pour le client du service cloud (fournisseur)

Le client du service cloud doit ajouter les éléments suivants aux programmes de sensibilisation, d'éducation et de formation destinés aux responsables métiers du service cloud, aux administrateurs de services cloud, aux intégrateurs de services cloud et aux utilisateurs de services cloud, y compris les employés et entrepreneurs concernés :

- Les normes et procédures relatives à l'utilisation des services cloud.
- Les risques de sécurité des informations liés aux services cloud et la façon dont ces risques sont gérés.
- Les risques liés aux systèmes et à l'environnement réseau liés à l'utilisation de services cloud.
- Les considérations légales et réglementaires applicables.

Des programmes de sensibilisation, d'éducation et de formation à la sécurité des informations sur les services cloud doivent être fournis à la direction et aux responsables de la supervision, y compris ceux des unités commerciales. Ces efforts soutiennent une coordination efficace des activités de sécurité des informations.

MC 5.0 - Gestion des incidents

Le fournisseur doit disposer d'un cadre de gestion des incidents établi pour gérer, limiter et supprimer/atténuer efficacement un incident et sa cause sous-jacente de l'environnement du fournisseur.

Le fournisseur doit disposer d'une procédure de Gestion des Incidents et des Crises qui comprend le processus de signalement des incidents/crises à Barclays. Le fournisseur doit s'assurer que les équipes de réponse en cas d'Incident/Crise et les processus pertinents sont contrôlés au moins une fois par an pour démontrer sa capacité à répondre efficacement à des Incidents. Le fournisseur doit également contrôler sa capacité à notifier un incident aux personnes concernées dans un délai défini et à le prouver à Barclays sur demande.

Le fournisseur doit disposer de plans de réponse aux incidents bien documentés, qui définissent les rôles de ses employés ainsi que les phases de la gestion et du traitement des incidents :

- Responsabilités et procédures : les responsabilités et procédures de gestion doivent être établies pour garantir une réponse rapide, efficace et ordonnée aux incidents.

- Signalement d'incidents : les incidents doivent être signalés le plus rapidement possible par les canaux de gestion appropriés et le mécanisme de signalement doit être aussi facile et accessible pour tous les employés et entrepreneurs du fournisseur.
- Évaluation d'incidents : les incidents doivent être évalués afin de déterminer la criticité, la classification et la réponse appropriées requises.
    - Classification des incidents : établissement d'une échelle de classification des incidents pour déterminer si l'événement doit être classé comme incident. La classification et la hiérarchisation des incidents peuvent aider à identifier l'impact et l'étendue d'un incident.
- Réponse aux incidents : les incidents doivent être traités conformément aux procédures documentées de gestion des incidents du fournisseur.
    - Endiguement des incidents : utilisation du personnel, des processus et des technologies disponibles pour endiguer rapidement et efficacement un incident dans l'environnement.
    - Élimination/Atténuation des incidents : utilisation du personnel, des processus et des technologies disponibles pour éliminer ou atténuer efficacement une menace de sécurité et/ou ses composants de l'environnement.
- Leçons tirées des incidents : les connaissances acquises lors de l'analyse et de la résolution des incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents futurs.
- Collecte de preuves : le fournisseur doit définir et appliquer des procédures d'identification, de collecte, d'acquisition et de conservation des informations, qui peuvent servir de preuves.

Post-incident : suite à une perturbation du ou des services de Barclays, un rapport post-incident doit être soumis à Barclays dans les quatre semaines civiles suivant le rétablissement du service à des niveaux de fonctionnement normaux. Ce rapport doit comprendre, au minimum, un examen de ce qui suit :

- Les événements entourant la situation.
- La manière dont l'incident/la crise a été géré(e) ;
- Une analyse de ses causes profondes ;
- S'il est classé comme « événement à risque » par le fournisseur ou Barclays (à savoir, jugé suffisamment important pour devoir être notifié/signalé aux parties prenantes concernées conformément aux politiques applicables connues du fournisseur) ;
- S'il représente un « risque de conduite » (par ex. si le fournisseur traite directement avec des clients de Barclays).
- Toute voie de recours des clients de Barclays dont le fournisseur a connaissance,
- Amélioration continue pour prévenir toute récurrence, et
- Le fournisseur doit chercher à améliorer les réponses lorsque cela est possible en intégrant les leçons tirées des mesures de détection/réponses actuelles et antérieures.

Communication : le fournisseur doit nommer un contact, lequel communiquera avec Barclays en cas d'incident/crise. Le fournisseur doit communiquer à Barclays les coordonnées de ce contact, ainsi que tout changement le concernant, y compris son numéro de téléphone et les heures auxquelles il est joignable.

Les informations suivantes doivent être incluses : - Nom, responsabilités au sein de l'organisation, rôle, adresse e-mail et numéro de téléphone

Si, à tout moment, le fournisseur confirme qu'un incident a un impact sur les Services de Barclays, les Systèmes de Barclays ou les Données de Barclays, le fournisseur doit en informer Barclays immédiatement, et, dans tous les cas, au plus tard 2 heures après la découverte de l'incident.

Dès que le fournisseur a connaissance d'un Cyber-incident, y compris par notification d'une entité Barclays, le fournisseur doit immédiatement, mais en aucun cas plus tard que ce qui est requis par la loi en vigueur ou, en l'absence d'une telle exigence, dans les 48 heures après avoir pris connaissance du cyber-incident, informer Barclays en envoyant un e-mail à l'adresse gcsojoc@barclays.com, et fournir toutes les informations pertinentes, y compris, si possible (a) les catégories et le nombre approximatif de données de Barclays concernées, et, le cas échéant, les catégories et le nombre approximatif de personnes concernées affectées ; (b) l'impact et les conséquences probables du cyber-incident pour Barclays et, le cas échéant, sur les personnes concernées ; et (c) les mesures correctives et d'atténuation prises ou à prendre par le fournisseur.

En cas de vol réel, suspecté ou allégué, d'utilisation ou de divulgation non autorisée de Données personnelles protégées en raison d'une défaillance des mesures de sécurité du fournisseur (ou de tout Personnel du fournisseur) ou d'un accès non autorisé aux Données personnelles protégées depuis ou par l'intermédiaire du fournisseur (ou de tout membre du Personnel du fournisseur), ou de perte, d'endommagement ou de destruction des Données personnelles protégées en possession ou sous le contrôle de tout Personnel du fournisseur, ou de tout autre Traitement non autorisé de Données personnelles protégées, le fournisseur doit en informer Barclays dès que possible, et, dans tous les cas, dans les 24 heures suivant la prise de connaissance de l'événement concerné, en envoyant un e-mail à l'adresse gcsojoc@barclays.com, et doit coopérer et fournir une assistance complète à Barclays en ce qui concerne cet événement, y compris en fournissant toutes les informations pertinentes telles que les données, l'heure, le lieu, le type d'incident, l'impact, le statut et les mesures d'atténuation prises.

Si un sous-traitant/sous-traitant ultérieur est utilisé pour fournir le service, et qu'il détient ou traite des données/informations ou actifs de Barclays, le fournisseur doit obtenir l'accord de Barclays. Le fournisseur doit avoir une relation contractuelle avec les sous-traitants/sous-traitants ultérieurs et doit s'assurer que les sous-traitants/sous-traitants ultérieurs sont accrédités par un cadre standard similaire concernant les meilleures pratiques du secteur fonctionnant efficacement pour protéger les données/informations de Barclays qu'ils traitent

et/ou détiennent. En cas d'incident avec le sous-traitant/sous-traitant ultérieur, il doit s'assurer que la notification d'incident ci-dessus sera suivie.

Conseils pour le client du service cloud (fournisseur)

Le client du service cloud doit vérifier l'attribution des responsabilités pour la gestion des incidents et s'assurer qu'elle répond aux exigences du client du service cloud. Le client du service cloud doit demander au prestataire de services cloud des informations sur les mécanismes suivants :
– le client du service cloud doit signaler un incident/événement détecté au prestataire de services cloud.
– le client du service cloud doit recevoir des rapports concernant un incident/événement détecté par le prestataire de services cloud.
– le client du service cloud doit suivre l'état d'un événement de sécurité signalé sur les informations.

MC 6.0 – Gestion des actifs informatiques (matériels et logiciels)

Le fournisseur doit disposer d'un programme de gestion des actifs efficace pour toute la durée de vie des actifs. La gestion des actifs doit régir le cycle de vie des actifs, depuis leur acquisition jusqu'à leur mise au rebut et/ou l'élimination en sécurité, et fournir une visibilité et une sécurité pour toutes les classes d'actifs dans l'environnement.

Le fournisseur doit tenir un inventaire précis, complet et à jour de tous les actifs critiques présents sur tous les sites et/ou pour tous les sites géographiques dans le cadre des services fournis à Barclays, y compris l'équipement Barclays hébergé sur les sites du fournisseur, et les sous-traitants/sous-traitants ultérieurs fournis par Barclays. Le fournisseur doit vérifier cet inventaire des actifs informationnels au moins une fois par an pour s'assurer qu'il est à jour, complet et exact, et présenter les résultats à Barclays sur demande.

Le processus de gestion des actifs doit couvrir les éléments suivants :

- Inventaire des actifs : les actifs associés aux informations et aux installations de traitement des informations doivent être identifiés et un inventaire de ces actifs doit être établi et tenu à jour.
    - Le fournisseur doit tenir un inventaire précis et à jour de tous les actifs matériels informatiques pouvant stocker ou traiter des informations.
    - Le fournisseur doit disposer d'un inventaire exact et à jour des actifs informationnels concernant l'équipement Barclays hébergé par le fournisseur et/ou concernant les actifs informatiques de Barclays fournis au fournisseur.
    - Les fournisseurs des niveaux 1, 2 et 3 doivent conserver des inventaires à jour, complets et précis des actifs (y compris des ordinateurs portables et de bureau, de l'équipement réseau, des jetons RSA ou de tout autre actif fourni par Barclays).
    - Le fournisseur doit effectuer le rapprochement de tous les actifs de Barclays (matériels et logiciels) chaque année et informer Barclays (Bureau de la sécurité, équipe ECAM) de ses résultats.

- La tenue à jour d'un inventaire de tous les logiciels déployés et autorisés requis pour fournir le service à Barclays et la conformité aux conditions générales des licences respectives.
- L'inventaire des actifs du client du service cloud doit tenir compte des informations et des actifs associés stockés dans l'environnement de cloud computing. Les registres de l'inventaire doivent indiquer où les actifs sont conservés, par exemple l'identification du service cloud.

- Utilisation acceptable des actifs : des règles d'utilisation acceptable des informations et des actifs associés aux informations et installations de traitement des informations doivent être identifiées, documentées et mises en œuvre.
  - Les actifs non autorisés doivent être retirés du réseau.
  - Le fournisseur doit s'assurer que des procédures efficaces sont mises en place pour atténuer les problèmes liés aux technologies non prises en charge, et en fin de vie des actifs, au retrait et à l'élimination sécurisée des actifs et des données, afin d'éliminer le risque.
  - Les logiciels et matériels non pris en charge doivent être identifiés comme tels dans le système d'inventaire.
- Restitution des actifs : tous les employés et sous-traitants/sous-traitants ultérieurs du fournisseur (dans le champ d'application des services fournis à Barclays) doivent restituer tous les actifs du fournisseur en leur possession à la fin de leur emploi, contrat ou accord.
  - Les actifs de Barclays « perdus ou volés » doivent faire l'objet d'une enquête appropriée et être signalés à Barclays conformément au contrôle de gestion des incidents.
  - En cas de « perte ou vol » des actifs du fournisseur contenant des informations de Barclays, ces informations doivent être signalées à Barclays conformément au contrôle de gestion des incidents.

Le fournisseur doit informer promptement Barclays des changements dont il a connaissance concernant sa capacité à prendre en charge, directement ou indirectement, les actifs informatiques utilisés dans le cadre de la prestation de services à Barclays, y compris lorsque des produits présentent des vulnérabilités de sécurité ; il doit en outre s'assurer de la mise à niveau ou de la suppression, en temps opportun, de ces actifs informatiques.

Transport des actifs de Barclays : le fournisseur devra s'assurer que tous les actifs et données de Barclays sont transportés de manière sécurisée, avec des contrôles adaptés, proportionnels à la classification et la valeur des actifs et données transportés (aussi bien d'un point de vue financier que d'atteinte à la réputation) incorporant l'impact de l'environnement de menaces dans lequel ils sont transportés.

Gestion du soutien (fournisseur)

Le fournisseur doit informer promptement Barclays des changements dont il a connaissance concernant sa capacité à prendre en charge, directement ou indirectement, les actifs informatiques utilisés dans le cadre de la prestation de services à Barclays, y compris lorsque des produits présentent des vulnérabilités de sécurité ; il doit en outre s'assurer de la mise à niveau ou de la suppression, en temps opportun, de ces actifs informatiques.

Le fournisseur doit s'assurer que toute modification potentielle des principaux accords de support aux tiers est identifiée et communiquée à Barclays pour les actifs concernés, afin de s'assurer que les informations sur le produit sont à jour.

Conseils pour le client du service cloud (fournisseur)

L'inventaire des actifs du client du service cloud doit tenir compte des informations et des actifs associés stockés dans l'environnement de cloud computing. Les registres de l'inventaire doivent indiquer où les actifs sont conservés, par exemple l'identification du service cloud.

L'installation de logiciels sous licence commerciale dans un service cloud peut entraîner une violation des conditions de licence du logiciel. Le client du service cloud doit disposer d'une procédure permettant d'identifier les exigences de licence spécifiques au cloud avant d'autoriser l'installation d'un logiciel sous licence dans un service cloud. Une attention particulière doit être portée aux cas où le service cloud est flexible et évolutif et où le logiciel peut être exécuté sur un nombre de systèmes ou de cœurs de processeur supérieur à celui autorisé par les conditions de licence.

MC 7.0 – Suppression/Destruction sécurisée des actifs physiques et rémanence des données venant des informations électroniques

La destruction ou l'effacement sécurisé des actifs informationnels de Barclays, y compris les images utilisées pour la maintenance, qui sont sauvegardés dans un format physique et/ou électronique, doit être effectué selon une méthode sécurisée et adaptée et il convient de vérifier que les données Barclays ne sont pas récupérables.

Le fournisseur doit élaborer des procédures et mettre en place les processus métiers et mesures techniques s'y rapportant pour éliminer de manière sécurisée les données selon des méthodes de protection appropriées, y compris, mais sans s'y limiter, la suppression, le nettoyage et la destruction pour garantir la suppression/l'effacement et la récupération sécurisés des données Barclays à partir de tous les supports de stockage, rendant les données Barclays irrécupérables par des moyens d'investigation informatique connus.

Les données de Barclays sauvegardées sur un support doivent être supprimées afin de les rendre irrécupérables et en ayant recours, de préférence, à des techniques appropriées d'effacement des données comme une suppression sécurisée, un nettoyage, un effacement de données, une destruction des actifs, ou à une méthode logicielle d'écrasement de données, ou encore en utilisant un cadre standard pour le secteur en ce qui concerne la suppression de données (NIST). Tout le matériel (actifs informationnels) doit être mis au rebut au terme de sa durée de vie opérationnelle (défectueux, déclassés en raison de la mise hors service ou de l'absence de nécessité, utilisés dans le cadre d'un essai ou d'une validation de concept, possibilité de réutiliser les services d'effacement des données pour les équipements destinés à être réutilisés, etc.)

Les exigences en matière d'élimination s'appliquent aux sous-traitants/sous-traitants ultérieurs du fournisseur qui sont utilisés pour fournir le service à Barclays.

Les informations au format papier (incluant les coordonnées des cartes de paiement) doivent être déchiquetées en respectant au minimum la norme P4 DIN66399 et en utilisant une déchiqueteuse ou peuvent être incinérées conformément à la norme BS EN15713:2009.

Pour Barclays, les preuves de l'élimination des données doivent être conservées, dans la mesure où elles constituent une piste d'audit et des preuves, et permettent d'assurer un suivi, et doivent inclure :

- Des preuves de la destruction et/ou de l'élimination (incluant la date de l'opération et la méthode utilisée).
- Les journaux d'audit du système pour la suppression.
- Les attestations de destruction des données.
- L'identité des personnes ayant procédé à l'élimination (incluant les partenaires, les tiers ou les entrepreneurs chargés de l'élimination).
- Un rapport de destruction et de vérification doit être généré pour confirmer la réussite ou l'échec de tout processus de destruction/suppression (par exemple, un processus d'écrasement doit s'accompagner d'un rapport donnant des précisions sur les éléments qui n'ont pas pu être effacés).

Au moment de la sortie du service fourni à Barclays, le fournisseur doit veiller, après avoir reçu une notification et une autorisation de Barclays, à ce que les données de Barclays soient détruites de manière sécurisée.

Conseils pour le client du service cloud (fournisseur)

Le client du service cloud doit demander la confirmation que le fournisseur de services cloud dispose des politiques et procédures de suppression ou de réutilisation sécurisée des ressources. Le client du service cloud doit demander une description documentée du processus de résiliation du service qui couvre le retour et la suppression des actifs du client du service cloud, puis la suppression de toutes les copies de ces actifs des systèmes du prestataire de services cloud. La description doit énumérer tous les actifs et documenter le calendrier d'arrêt du service, qui doit avoir lieu en temps voulu.

MC 8.0 – Classification des informations et gestion des données

Le fournisseur doit avoir établi un plan/cadre de classification des informations et de gestion des données approprié, conforme aux bonnes pratiques du secteur et/ou aux exigences de Barclays, couvrant les points suivants :

- Classification des informations : les informations doivent être classées en termes de criticité et de sensibilité à une divulgation ou à une modification non autorisée.
- Étiquetage des informations : un ensemble approprié de procédures d'étiquetage des informations doit être développé et mis en œuvre conformément au plan de classification des informations adopté par le fournisseur.
- Gestion des actifs : des procédures de gestion des actifs doivent être élaborées et mises en œuvre conformément au plan de classification des informations adopté par le fournisseur.

Le fournisseur doit également s'assurer que tout le personnel a connaissance des exigences relatives à l'étiquetage et à la gestion du fournisseur et de Barclays, et de la manière d'appliquer la bonne classification des informations

Le fournisseur doit se reporter au schéma d'étiquetage des informations Barclays et aux exigences de gestion (annexe A, tableaux A1 et A2), ou à un autre programme convenu pour s'assurer qu'il protège et sécurise les informations de Barclays qu'il détient et/ou qu'il traite. Cette exigence s'applique à tous les actifs informationnels détenus ou traités au nom de Barclays, y compris les sous-traitants/sous-traitants ultérieurs.

Conseils pour le client du service cloud (fournisseur)

Le client du service cloud doit étiqueter les informations et les actifs associés gérés dans l'environnement de cloud computing conformément aux procédures d'étiquetage adoptées par le client du service cloud. Le cas échéant, les fonctionnalités fournies par le prestataire de services cloud prenant en charge l'étiquetage peuvent être adoptées.

Sauvegarde des informations/données MC 9.0

Le fournisseur doit avoir un processus de sauvegarde des données en place, pour s'assurer que l'infrastructure est régulièrement et correctement sauvegardée afin d'éviter la perte de données. Les informations stockées sous forme électronique sont sauvegardées pour garantir leur sécurité en cas de défaillance du système, de sinistre ou d'incident. Les plans de sauvegarde doivent être développés, testés et mis en œuvre pour répondre à la politique spécifique en matière de sauvegarde.

Plan de sauvegarde, les éléments suivants doivent être pris en compte :

- Définition des exigences en matière de sauvegarde : les exigences en matière de sauvegarde des données sont clairement définies, enregistrées et convenues avec l'entreprise
- Production d'enregistrements précis et complets des copies de sauvegarde et des procédures de restauration documentées ;
- Fréquence de sauvegarde (par exemple, sauvegarde complète ou différentielle)
- Stockage sécurisé des sauvegardes
    - stockage des sauvegardes dans un emplacement distant sûr et sécurisé, à une distance suffisante pour éviter tout dommage causé par un sinistre sur le site principal ;
- Test régulier des supports de sauvegarde pour s'assurer qu'ils peuvent être utilisés en cas d'urgence si nécessaire. Test de la capacité à restaurer les données sauvegardées sur un système de test, et sans écraser le support de stockage d'origine en cas d'échec du processus de sauvegarde ou de restauration et entraîner des dommages ou des pertes de données irréparables ;
- Assurance que la perte de données accidentelle est détectée avant de procéder à la sauvegarde.

- Vérification que la sauvegarde est adaptée

Les sauvegardes doivent être correctement protégées par des dispositifs de sécurité physique et/ou des technologies de chiffrement lorsqu'elles sont stockées ou déplacées à travers le réseau/sites. Cela inclut les sauvegardes à distance et les services cloud.

Toutes les données de Barclays doivent être sauvegardées régulièrement, conformément aux exigences du service.

Lorsque le fournisseur de services cloud fournit une fonction de sauvegarde dans le cadre du service cloud, le client du service cloud doit demander les spécifications de la fonction de sauvegarde au fournisseur de services cloud. Le client du service cloud doit également vérifier qu'il répond à ses besoins en matière de sauvegarde. Le client du service cloud est responsable de la mise en œuvre des fonctions de sauvegarde lorsque le fournisseur de services cloud ne les fournit pas.

Le fournisseur doit s'assurer que des processus de sauvegarde et de restauration appropriés ont été mis en place pour tous les services et systèmes informatiques utilisés dans le cadre de la prestation de services fournie à Barclays, qu'ils sont appliqués en conformité avec les besoins de Barclays et que leur efficacité est périodiquement démontrée.

Le fournisseur doit s'assurer que tous les supports de sauvegarde associés à la prestation de services fournie à Barclays, ainsi que les modalités de traitement et de stockage de ces supports, sont à tout moment sûrs et fiables.

MC 10.0 - Gestion de la configuration

Le fournisseur doit définir et mettre en œuvre des processus et des outils pour appliquer les configurations définies (y compris les configurations de sécurité) pour le matériel, les logiciels, les services (y compris les services cloud) et les réseaux, pour les systèmes nouvellement installés ainsi que pour les systèmes opérationnels pendant toute leur durée de vie.

Gestion des configurations : le fournisseur doit disposer d'un ensemble de configurations approuvées et testées pour le matériel, les logiciels et les réseaux. Elles doivent être enregistrées et un journal de toutes les modifications apportées aux configurations doit être tenu à jour. Ces documents doivent être conservés en lieu sûr. Cela peut être réalisé de différentes manières, par exemple sous la forme de bases de données de configuration ou de modèles de configuration.

Surveillance des configurations : les configurations doivent être surveillées à l'aide d'un ensemble complet d'outils de gestion du système (par exemple, services de maintenance, support à distance, outils de gestion d'entreprise, logiciels de sauvegarde et de restauration) et doivent être examinées régulièrement pour vérifier les paramètres de configuration, évaluer la force des mots de passe et évaluer les activités réalisées. Les configurations réelles peuvent être comparées aux modèles cibles définis. Tout écart doit être corrigé, soit par application automatique de la configuration cible définie, soit par une analyse manuelle de l'écart suivie d'actions correctives.

Enregistrement et gestion des éléments de configuration : le fournisseur doit tenir des registres complets et exacts pour l'ensemble des Éléments de configuration relevant du champ d'application utilisés dans la fourniture de la prestation de services fournie à Barclays (y compris la propriété et les dépendances/mappages en amont/aval). Le fournisseur doit avoir mis en place des contrôles garantissant le maintien permanent de l'exactitude et de l'exhaustivité des données.

Isolation de l'environnement de production : le fournisseur doit s'assurer que les services de production fournis à Barclays ne dépendent d'aucun composant hors production afin de garantir une prestation de services sécurisée et fiable.

Configuration sécurisée : le fournisseur doit établir un cadre visant à s'assurer que tous les équipements réseau et/ou systèmes configurables sont configurés de manière sécurisée et conformément aux meilleures pratiques du secteur (par ex. NIST, SANS et CSSI).

- L'élaboration des politiques, des procédures et/ou des mesures organisationnelles, et des outils permettant de mettre en œuvre les normes de configuration de la sécurité relevant des meilleures pratiques du secteur pour tous les appareils réseau, les systèmes d'exploitation, les applications et les serveurs autorisés.
- Des vérifications régulières (tous les ans au minimum) de leur mise en œuvre, pour s'assurer que tout non-respect des normes de sécurité de base est rapidement corrigé. Des vérifications et une surveillance appropriées mises en place pour s'assurer de l'intégrité des infrastructures et des appareils.
- Les systèmes et appareils réseau doivent être configurés de manière à fonctionner conformément aux principes de sécurité (par ex. concept de limitation des contrôles des ports, des protocoles et des services, interdiction des logiciels non autorisés, suppression et désactivation des comptes utilisateurs inutiles, changement des mots de passe par défaut des comptes, suppression des logiciels inutiles, etc.).
- Un audit de configuration périodique doit être réalisé au moins une fois par an pour assurer que l'environnement de production réel ne dispose pas d'une configuration non autorisée.
- La gestion de la configuration doit régir les normes de configuration sécurisée pour toutes les classes d'actifs et détecter, alerter et répondre efficacement aux modifications ou aux écarts de la configuration.

Conseils pour le client du service cloud (fournisseur) utilisé pour fournir un ou plusieurs services à Barclays

Le client du service cloud (CSC) doit s'assurer que les contrôles appropriés de configuration sécurisée sont mis en œuvre pour protéger le service Barclays -

- Lors de la configuration de machines virtuelles, les clients du service cloud doivent s'assurer que les aspects appropriés sont renforcés (par ex. uniquement les ports, protocoles et services nécessaires) et que les mesures techniques appropriées sont en place (par ex. protection contre les logiciels malveillants, journalisation) pour chaque machine virtuelle utilisée.

Droit d'inspection

À réception d'une notification écrite de Barclays adressée au moins dix (10) jours ouvrables à l'avance, le fournisseur doit autoriser Barclays à procéder à un examen de la sécurité de tout site ou toute technologie utilisé(e) par le fournisseur ou ses sous-traitants/sous-traitants ultérieurs pour développer, tester, améliorer, entretenir ou exploiter les systèmes du fournisseur utilisés dans le cadre des services, afin de s'assurer que le fournisseur respecte ses obligations envers Barclays. Le fournisseur devra également autoriser Barclays à procéder à une inspection au moins une fois par an ou juste après un incident de sécurité.

Si, au cours d'une inspection, Barclays identifie un défaut de conformité concernant les contrôles, Barclays procède à une évaluation des risques et doit préciser un délai de correction. Le fournisseur devra alors prendre toutes les mesures correctives requises avant l'expiration de ce délai.

Le fournisseur devra apporter toute aide raisonnablement demandée par Barclays en lien avec l'inspection et fournir la documentation soumise durant l'inspection. La documentation devra être remplie et renvoyée à Barclays dans les plus brefs délais. Le fournisseur devra également aider Barclays en remplissant le questionnaire d'évaluation ainsi qu'en fournissant les preuves demandées lors de tout examen d'assurance.

Annexe A : schéma d'étiquetage des informations Barclays et exigences de gestion des données

Tableau A1 : Schéma d'étiquetage des informations Barclays

Étiquette	Définition	Exemples
Secrètes	Les informations doivent être classées « **secrètes** » si leur divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de la structure de gestion des risques d'entreprise (ERMF) comme étant « critique » (financier ou non financier). Ces informations sont réservées à un public spécifique et ne doivent pas être diffusées ultérieurement sans l'autorisation de l'auteur. Le public peut comprendre des destinataires externes avec l'autorisation explicite du propriétaire des informations.	• Informations sur les fusions ou acquisitions potentielles • Informations sur la planification stratégique – commerciale et organisationnelle • Certaines informations relatives à la configuration de la sécurité des informations • Certains rapports et résultats d'audit • Comptes rendus du comité exécutif • Coordonnées d'authentification ou d'identification et de vérification (ID&V) – client et collaborateur • Grandes quantités d'informations sur les titulaires de cartes • Prévisions de bénéfices ou résultats financiers annuels (avant publication officielle) • Tout élément couvert en vertu d'un accord de non-divulgation (AND) formel
Diffusion restreinte - Interne	Les informations doivent être classées comme étant à« **Diffusion restreinte - Interne** » si les destinataires prévus sont uniquement des employés authentifiés de Barclays et des prestataires de services gérés (PSG) de Barclays avec un contrat actif en place, et si ces informations sont réservées à un public spécifique. Une divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de l'ERMF comme étant « majeur » ou « limité » (financier ou non financier). Ces informations ne sont pas destinées à une diffusion générale mais peuvent être transmises ou partagées par des destinataires selon le principe du besoin de connaître.	• Stratégies et budgets • Évaluations des performances • Rémunération du personnel et données personnelles • Évaluations de la vulnérabilité
Diffusion restreinte – Externe	Les informations doivent être classées comme étant à « **Diffusion restreinte - Externe** » si les destinataires prévus sont des employés authentifiés de Barclays et des PSG de Barclays avec un contrat actif en place et si ces informations sont réservées à un public spécifique ou à des parties externes qui sont autorisées par le propriétaire des informations. Une divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de l'ERMF comme étant « majeur » ou « limité »	• Nouveaux plans de produits • Contrats de clients • Contrats juridiques • Informations clients individuelles/de petit volume destinées à être envoyées en externe • Communications avec les clients.

	(financier ou non financier). Ces informations ne sont pas destinées à une diffusion générale mais peuvent être transmises ou partagées par des destinataires selon le principe du besoin de connaître.	• Documentation d'offre de nouvelles émissions (par ex. prospectus, notice d'offre) • Documents de recherche finaux • Informations importantes n'ayant pas été rendues publiques (IIPP) et n'appartenant pas à Barclays • Tous les rapports de recherche. • Certains documents marketing • Analyses du marché • Rapports et résultats d'audit
Aucune restriction	Les informations doivent être classées dans la catégorie « Aucune restriction » si elles sont destinées à une diffusion générale, ou si elles ne sont pas susceptibles d'avoir un impact négatif sur l'entreprise si elles étaient diffusées.	• Documents marketing • Publications • Annonces publiques • Offres d'emploi • Informations sans impact sur Barclays

Tableau A2 : schéma d'étiquetage des informations Barclays – exigences de gestion des données

*** Les informations relatives à la configuration de la sécurité des systèmes, les résultats d'audit, et les dossiers personnels peuvent être classés comme des informations à diffusion restreinte – interne ou secrètes, en fonction de l'impact qu'une divulgation non autorisée aurait sur l'entreprise.

Étape du cycle de vie	Secrètes	Diffusion restreinte - interne	Diffusion restreinte - externe
Création et introduction	• Un propriétaire des informations doit être affecté aux actifs.	• Un propriétaire des informations doit être affecté aux actifs.	• Un propriétaire des informations doit être affecté aux actifs.
Stockage	• Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. • Les actifs électroniques stockés doivent être protégés par chiffrement ou par des contrôles compensatoires appropriés s'il existe un risque significatif que des individus non autorisés puissent accéder à de tels actifs.	• Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones publiques (y compris les zones publiques au sein des locaux auxquelles les visiteurs peuvent accéder sans supervision). • Les informations ne doivent pas être conservées dans des zones publiques dans les locaux auxquelles les visiteurs peuvent accéder sans supervision.	• Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. • Les actifs électroniques stockés doivent être protégés par chiffrement ou par des contrôles compensatoires appropriés s'il existe un risque significatif que des individus non autorisés puissent accéder à de tels actifs.

	• Toutes les clés utilisées pour protéger les données, l'identité et/ou la réputation de Barclays doivent être protégées par des modules de sécurité matérielle certifiés FIPS 140-2 niveau 3 ou plus.		
Accès et utilisation	• Les actifs (physiques ou électroniques) ne doivent pas être manipulés ou laissés sans surveillance dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. Les actifs peuvent être manipulés si des contrôles adaptés sont en place (par exemple, écrans de confidentialité). • Les actifs imprimés doivent l'être au moyen d'outils d'impression sécurisés. • Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique.	• Les actifs (physiques ou électroniques) ne doivent pas être laissés dans des zones publiques en dehors des locaux. • Les actifs (physiques ou électroniques) ne doivent pas être conservés dans des zones publiques dans les locaux auxquelles les visiteurs peuvent accéder sans supervision. • Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique si nécessaire.	• Les actifs (physiques ou électroniques) ne doivent pas être manipulés ou laissés sans surveillance dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. Les actifs peuvent être manipulés si des contrôles adaptés sont en place (par exemple, écrans de confidentialité). • Les actifs imprimés doivent être récupérés immédiatement dans l'imprimante. Si cela n'est pas possible, des outils d'impression sécurisés doivent être utilisés. • Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique.
Partage	• Une étiquette d'information visible doit être apposée sur chaque page des actifs physiques. • Les enveloppes contenant des actifs physiques doivent porter à l'avant une étiquette d'information visible et être scellées avec un sceau inviolable. Elles doivent être placées à l'intérieur d'une deuxième enveloppe non étiquetée avant distribution. • Les actifs électroniques doivent porter un étiquetage d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page une étiquette d'information visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation.	• Une étiquette d'information visible doit être apposée sur les actifs physiques. L'étiquette doit figurer au minimum sur la page de titre. • Les actifs électroniques doivent porter un étiquetage d'information clairement visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation. • Les actifs doivent uniquement être distribués aux individus employés par l'organisation, ou dans le cadre d'une obligation contractuelle appropriée vis-à-vis de celle-ci ou encore dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat.	• Une étiquette d'information visible doit être apposée sur les actifs physiques. L'étiquette doit figurer au minimum sur la page de titre. • Les enveloppes contenant des actifs physiques doivent porter à l'avant une étiquette d'information visible. • Les actifs électroniques doivent porter un étiquetage d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page une étiquette d'information visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation.

	• Les actifs doivent uniquement être distribués aux individus employés par l'organisation, ou dans le cadre d'une obligation contractuelle appropriée vis-à-vis de celle-ci ou encore dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. • Les actifs doivent être distribués uniquement aux individus spécialement autorisés à les recevoir par le propriétaire des informations. • Les actifs ne doivent pas être télécopiés. • Les actifs électroniques doivent être chiffrés au moyen d'un mécanisme de protection cryptographique approuvé lorsqu'ils transitent en dehors du réseau interne. • Pour les actifs électroniques, une chaîne de responsabilité doit être observée.		• Les actifs doivent uniquement être distribués aux individus employés par l'organisation, ou dans le cadre d'une obligation contractuelle appropriée vis-à-vis de celle-ci ou encore dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. • Les actifs doivent être distribués uniquement aux individus qui ont besoin de les recevoir. • Les actifs ne doivent pas être télécopiés, à moins que l'expéditeur ne se soit assuré que les destinataires soient prêts à les récupérer. • Les actifs électroniques doivent être chiffrés au moyen d'un mécanisme de protection cryptographique approuvé lorsqu'ils transitent en dehors du réseau interne.
Archivage et destruction	• Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. • Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou des autres emplacements similaires en temps opportun. • Les supports sur lesquels des actifs électroniques secrets ont été stockés doivent être nettoyés de façon appropriée avant ou pendant la destruction.	• Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. • Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou des autres emplacements similaires en temps opportun.	• Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. • Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou des autres emplacements similaires en temps opportun.

Annexe B : Définitions

Informations confidentielles de Barclays désigne toute information obtenue par le responsable fournisseur, le fournisseur ou tout membre du Personnel du fournisseur (ou à laquelle l'un d'entre eux a accès) dans le cadre des présentes Conditions générales et/ou de tout contrat relatif (i) à des activités commerciales, produits et/ou développements de toute entité Barclays et/ou (ii) à des employés, clients, contreparties, tiers/fournisseurs et/ou sous-traitants de toute entité Barclays (autres que les Entités du fournisseur), y compris toute propriété intellectuelle détenue par une entité Barclays (y compris

en vertu d'un contrat) ou tout fournisseur/entrepreneur tiers, des Données personnelles protégées, les présentes Conditions générales, chaque module et chaque contrat, ainsi que les registres conservés dans le cadre de tout contrat et toute information relative aux plans, prix, méthodologies, processus, données financières de l'entité ou de la personne concernée, droits de propriété intellectuelle, recherche, systèmes, programmes et/ou technologies de l'information, passés, présents ou futurs ;

Données de Barclays désigne l'ensemble des données, informations, textes, dessins et autres documents intégrés dans tout support, y compris tous les supports électroniques, optiques, magnétiques ou matériels qui (i) sont accessibles par le fournisseur dans le cadre d'un contrat, (ii) sont fournis au fournisseur par toute entité Barclays, ou (iii) que le fournisseur génère, collecte, traite, stocke ou transmet en rapport avec tout contrat, à l'exclusion des matériels du fournisseur.

Systèmes de Barclays désigne les systèmes d'information électroniques comprenant un ou plusieurs matériels, équipements, logiciels, périphériques et réseaux de communication détenus, contrôlés, exploités et/ou utilisés par une entité Barclays.

Cyber-incident désigne tout événement, qu'il ait été confirmé qu'un tel événement s'est réellement produit ou que le fournisseur ou Barclays ait des motifs raisonnables de croire qu'il s'est produit (sur la base d'une menace crédible, de renseignements ou autre), ayant entraîné ou ayant le potentiel de compromettre (i) la confidentialité, l'intégrité ou la disponibilité totale des Données de Barclays, ou (ii) la confidentialité, l'intégrité ou la disponibilité totale et le fonctionnement normal d'un Système du fournisseur ou d'un Système de Barclays.

Incident technologique désigne une interruption non planifiée d'un service informatique ou une réduction de la qualité d'un service informatique, y compris, sans s'y limiter, la défaillance d'un élément de configuration qui n'a pas encore eu d'impact sur un service. Incident majeur désigne un incident qui présente un risque/un impact important pour Barclays et qui peut entraîner de graves conséquences, notamment une perte importante de productivité, des dommages à la réputation/réglementation et un impact sur les principaux processus d'entreprise, les contrôles ou les systèmes clés.

Évaluation de l'impact sur la protection des données désigne une évaluation de l'impact des opérations de Traitement envisagées sur la protection des données personnelles, tel que requis par la Législation sur la protection des données ;

Législation sur la protection des données désigne, dans la mesure applicable à l'exécution de l'une des obligations des fournisseurs en vertu d'un contrat : (i) la Directive européenne concernant la protection de la vie privée et les communications électroniques 2002/58/CE (qui peut être modifiée ou remplacée de temps à autre), (ii) le Règlement général sur la protection des données de l'UE 2016/679 (le RGPD), les décisions et directives de la Commission européenne et toutes les lois nationales d'application, (iii) le RGPD du Royaume-Uni, (iv) les dispositions de la loi américaine *Gramm–Leach–Bliley Act* relative aux informations personnelles non publiques, (v) la loi américaine *Health Insurance Portability and Accountability Act* de 1996, et (vi) toutes les autres lois, réglementations et directives réglementaires applicables relatives à la protection des données et de la vie privée dans (a) toute juridiction dans laquelle l'entité Barclays concernée est située, les obligations des fournisseurs sont exécutées, la Personne concernée est située, ou toute

donnée personnelle protégée est en cours de Traitement, de stockage ou d'utilisation et (b) toute juridiction à partir de laquelle le fournisseur remplit l'une de ses obligations en vertu d'un Contrat ;

Obligations de contrôle de la confidentialité des **données** désigne tout calendrier de confidentialité des données faisant partie de l'Annexe 7 (Obligations de contrôle pour les fournisseurs externes).

Personne concernée a le sens qui lui est donné par la Législation sur la protection des données. Lorsque ce terme n'est pas défini par la Législation sur la protection des données, il désigne une personne physique identifiée ou une personne physique identifiable qui peut être identifiée, directement ou indirectement, et notamment par une référence à un identifiant comme un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

Bonne pratique du secteur désigne, en ce qui concerne toute action et toute circonstance, l'exercice du plus haut degré de compétence, de diligence, de prudence et de prévoyance que l'on pourrait raisonnablement attendre d'une personne hautement qualifiée et expérimentée engagée dans le même type d'entreprise dans des circonstances identiques ou similaires.

Données personnelles a le sens qui lui est donné dans la Législation sur la protection des données. Lorsque ce terme n'est pas défini par la Législation sur la protection des données, il désigne toute information relative à une Personne concernée, ou identifiant directement ou indirectement une Personne concernée.

Violation de données personnelles a le sens qui lui est donné dans la Législation sur la protection des données. Lorsque ce terme n'est pas défini par la Législation sur la protection des données, il désigne toute violation de sécurité entraînant la destruction accidentelle ou illicite, la perte, l'altération, la divulgation non autorisée ou l'accès aux Données personnelles transmises, stockées ou Traitées de toute autre manière.

Traitement a le sens qui lui est donné dans la Législation sur la protection des données. Lorsque ce terme n'est pas défini par la Législation sur la protection des données, il désigne toute opération ou un ensemble d'opérations effectuées sur des Données personnelles, que ce soit ou non par des moyens automatiques, tels que (sans s'y limiter) la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou la mise à disposition, l'alignement ou la combinaison, le blocage, l'effacement ou la destruction et les termes **Traiter** et **Traité(e)(s)** ont la signification correspondante ;

Sous-traitant désigne tout Tiers fournissant de temps à autre des biens et/ou des services dans le cadre de : (a) la fourniture de produits, services et/ou livrables ; et/ou (b) le Traitement ou toute autre utilisation de toute Donnée personnelle protégée dans la mesure permise par un contrat.

Personnel du fournisseur/tiers désigne toutes les personnes et/ou entités qui exécutent une partie des services ou fournissent un ou plusieurs produits en vertu d'un contrat, y compris les employés, Sous-traitants et/ou agents du fournisseur ou de l'un de ses Sous-traitants.

Systèmes du fournisseur/tiers désigne des systèmes d'information électroniques (qui peuvent inclure un ou plusieurs matériels, équipements, logiciels, périphériques et réseaux de communication) qui sont utilisés (ou dont une partie est utilisée) : (i) pour fournir des produits ou services à une société affiliée de Barclays dans le cadre d'un contrat, ou (ii) sont gérés, administrés, surveillés ou sous le contrôle du fournisseur ou d'un Sous-traitant dans le cadre d'un contrat.

Système désigne tout système d'information électronique (qui peut inclure un ou plusieurs matériels, équipements, logiciels, périphériques et réseaux de communication) qui est utilisé ou dont une partie est utilisée pour fournir des biens ou des services à une société affiliée de Barclays dans le cadre d'un contrat.