Obligation de contrôle des fournisseurs (SCO)

Sécurité des informations et cybersécurité (SIC)

Domaine/intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Usage approuvé	Le fournisseur doit s'assurer que les informations et autres actifs associés sont correctement protégés, utilisés et traités. Les règles d'utilisation acceptable et les procédures de gestion des informations et des autres actifs associés doivent être identifiées, documentées et mises en œuvre. Les employés des fournisseurs, y compris les sous-traitants, qui utilisent ou ont accès aux informations de l'organisation et aux ses actifs, doivent être informés des exigences relatives à la sécurité des informations pour pouvoir protéger et manipuler les informations et les actifs de l'organisation. Ils sont responsables de l'utilisation qu'ils font des installations de traitement des informations. L'organisation doit mettre en place une politique sur l'utilisation acceptable des informations et des actifs et la communiquer à toute personne qui manipule des informations ou utilise des actifs. Le fournisseur doit prendre des mesures appropriées pour s'assurer du respect des critères d'utilisation acceptable. Les domaines suivants doivent être pris en compte : • Utilisation d'Internet. • Utilisation d'un logiciel en tant que service (SaaS, Software as a Service). • Utilisation des référentiels de code public. • Utilisation de plug-ins de navigateur et de freeware/shareware. • Utilisation des réseaux sociaux. • Utilisation de la messagerie électronique d'entreprise. • Utilisation d'une messagerie instantanée. • Utilisation du matériel informatique fourni par le fournisseur. • Utilisation du matériel informatique non fourni par le fournisseur (équipement personnel, par exemple). • Utilisation de périphériques de stockage portables/amovibles. • Responsabilités lors de la gestion, de la sauvegarde et du stockage d'actifs informationnels Barclays. • Sortie des canaux de fuite de données ; et	Les critères d'utilisation acceptables aident à soutenir l'environnement de contrôle en protégeant les actifs informationnels.

	• Le risque et les conséquences de l'usage abusif des éléments mentionnés ci-dessus et/ou les conséquences illégales, nuisibles ou choquantes d'un tel usage abusif.	
2. Frontières et sécurité du réseau	Le fournisseur doit s'assurer que l'ensemble des systèmes et applications exploités par le fournisseur et/ou son sous-traitant/ses sous-traitants ultérieurs et prenant en charge le ou les services fournis à Barclays soient protégés contre les menaces pouvant entrer dans le réseau et en sortir. Des contrôles doivent être mis en œuvre pour assurer la sécurité des informations dans les réseaux et la protection des services connectés contre les accès non autorisés. Le fournisseur doit identifier, protéger, détecter et répondre aux alertes et violations de sécurité. Les contrôles de sécurité du réseau garantissent la protection des informations dans les réseaux et leurs installations de traitement des informations connexes, et doivent inclure, sans s'y limiter, les domaines suivants : • La tenue à jour d'un inventaire de toutes les limites réseau de l'organisation (via un diagramme de l'architecture du réseau) à réviser au moins une fois par an. • Les connexions externes au réseau du fournisseur doivent être documentées, vérifiées et approuvées avant d'être établies, afin de prévenir les violations de sécurité. • Les réseaux du fournisseur doivent être protégés selon les principes de défense en profondeur (par ex. segmentation du réseau, pare-feu, etc.). • Le fournisseur doit disposer de technologies de prévention des intrusions sur le réseau afin de détecter et d'empêcher tout trafic malveillant pour l'ensemble du trafic entrant/sortant, mettre à jour les bases de données de signatures conformément aux meilleures pratiques du secteur et appliquer les mises à jour du fournisseur de solutions en temps opportun. • Le fournisseur doit s'assurer que la connectivité privée entre les clouds privés virtuels (VPC) et les réseaux sur site tiers est chiffrée et que le trafic n'est pas exposé à l'Internet public. • Tout le trafic du réseau Internet doit passer par un proxy configuré pour filtrer les connexions non autorisées. • Une séparation logique des ports/interfaces de gestion des appareils du LAN/trafic utilisateur, ainsi que des contrôles d'authentification doivent être mis en place. • Des communications sécurisées entre les appareils et la console ou les stations de gestion.	Le non-respect de ce principe peut se traduire par l'exploitation des réseaux internes ou externes par des pirates afin d'accéder au service ou aux données.

	• Assurer que la journalisation et la surveillance comprennent la détection et l'alerte d'activités suspectes (en utilisant des déclencheurs de comportement et des indicateurs de compromission), par exemple via un SIEM. • Les connexions entre les bureaux, les fournisseurs de service cloud et les centres de données doivent être chiffrées et utiliser un protocole sécurisé. Les données et/ou actifs informationnels de Barclays en transit sur le réseau local étendu du fournisseur (WAN) doivent être chiffrés. • Le fournisseur doit réviser chaque année les règles de pare-feu (pare-feu internes et externes). • Le fournisseur doit s'assurer que l'accès au réseau interne est surveillé au moyen des contrôles d'accès au réseau appropriés. • Tout accès sans fil au réseau doit être protégé par des protocoles de chiffrement fort, de segmentation, d'authentification et d'autorisation, pour prévenir les violations de la sécurité. • Pour pouvoir fournir le ou les services à Barclays, le fournisseur doit disposer d'un réseau séparé (logiquement). Le fournisseur doit s'assurer que les serveurs et les applications utilisés pour fournir des services à Barclays ne sont pas déployés sur des réseaux non fiables (réseaux situés à l'extérieur de votre périmètre de sécurité, qui échappent à votre contrôle administratif, par exemple sur Internet) sans contrôles de sécurité appropriés. Le fournisseur hébergeant les informations de Barclays (et ses sous-traitants et sous-traitants ultérieurs) dans un centre de données ou sur le cloud doit être titulaire d'une attestation de respect des meilleures pratiques du secteur en matière de gestion de la sécurité des réseaux. Réseaux T2 et T3 • Le réseau T2 doit être logiquement séparé du réseau d'entreprise du fournisseur au moyen d'un pare-feu, et tous les trafics entrants et sortants doivent être restreints et surveillés. • Le routage doit être configuré de telle sorte que les connexions soient établies uniquement avec le réseau de Barclays, et qu'elles ne soient pas routées vers d'autres réseaux du fournisseur. • Le routeur périphérique/de terminaison du dernier kilomètre du fournisseur ou la connexion aux passerelles extranet de Barclays doit être configuré de manière sécurisée, selon un concept de limitation des contrôles des ports, des protocoles et des services.	

	○ Assurer que la journalisation et la surveillance comprennent la détection et l'alerte d'activités suspectes (en utilisant des déclencheurs de comportement et des indicateurs de compromission), par exemple via un SIEM. **Le fournisseur tiers doit veiller à ce que tous les systèmes et toutes les applications fournissant des services que Barclays considère et présente comme étant à haut risque soient segmentés en réseau. Le cloisonnement d'une application métier et de ses principaux composants d'infrastructure (à l'exclusion des infrastructures critiques partagées) au sein de son propre segment de réseau, réalisé au moyen de technologies de sécurité approuvées par Barclays (pare-feu ou autres technologies équivalentes) afin de respecter les principes ci-dessous.** i. Une approche de segmentation doit être adoptée pour limiter l'exposition aux risques, empêcher les mouvements latéraux sur le réseau et réduire les risques de diffusion sur le réseau. Les applications doivent être déployées sur des segments autonomes afin de limiter les risques dans la mesure du possible. Exemple : Zone Faster Payments. Toutes les infrastructures et données liées aux applications métiers doivent être déployées dans une zone d'application sécurisée autonome, dans la mesure du possible, et séparées du réseau interne de Barclays à l'aide d'une technologie d'application approuvée par le CSO (par ex. pare-feu réseau, solution de segmentation approuvée). Remarque : certains scénarios peuvent justifier la séparation de composants tels que l'application et la base de données sur plusieurs zones, par exemple lorsque des plates-formes partagées sont exploitées. Chaque application doit être évaluée individuellement, avec l'approche la plus appropriée définie et convenue avec un consultant en sécurité CSO. ii. Les services doivent être séparés physiquement ou logiquement. La structure réseau sous-jacente (par ex. le câblage/les commutateurs) peut être partagée avec d'autres applications et services, c'est-à-dire que les segments peuvent être définis de manière logique sans qu'il soit nécessaire d'appliquer la segmentation par séparation physique du reste du réseau Barclays. iii. Les zones d'application doivent limiter les flux de trafic vers et depuis d'autres zones (y compris le réseau CIPE interne), en fonction de ceux requis pour le fonctionnement du service et de tout outil de gestion, de surveillance et de sécurité approuvé. Les configurations doivent spécifier des ports, protocoles et adresses IP spécifiques pour les chemins de communication autorisés. Toutes les autres communications doivent être limitées par défaut. Les règles contenant des plages doivent être évitées et	

	approuvées à titre exceptionnel uniquement pour garantir que seules les exigences minimales de connectivité sont activées. iv. Les conteneurs doivent être solidement séparés par des contrôles logiques forts empêchant tout mouvement latéral entre les conteneurs, imposant ainsi une isolation. La compromission d'un conteneur ne doit pas entraîner la compromission d'autres conteneurs fonctionnant sur le même hôte/cluster. v. Toutes les mises en œuvre de la segmentation doivent offrir une capacité de gestion centralisée des politiques avec une fonctionnalité (ou une intégration) permettant de vérifier et de signaler la conformité des politiques (voir le document sur la conformité des pare-feu) et de fournir un journal des modifications vérifiable. vi. Des contrôles/inspections dynamiques doivent être effectués dans la mesure du possible/de ce qui est réalisable. vii. Les capacités de segmentation doivent fonctionner de manière « sécurisée », par exemple en cas d'échec de la capacité, les ensembles de règles approuvés pour bloquer/autoriser le trafic doivent rester appliqués. viii. Tout trafic entre les systèmes de production et hors production sur les zones d'application doit être autorisé uniquement à titre exceptionnel et doit être consigné dans un journal. **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 sécurité réseau sont mis en œuvre pour protéger le service Barclays. • Le client du service cloud (CSC) doit définir ses exigences en matière de séparation des réseaux afin d'isoler les tenants dans l'environnement partagé d'un service cloud et vérifier que le fournisseur de services cloud répond à ces exigences. • La politique de contrôle d'accès du client du service cloud pour l'utilisation des services réseau doit spécifier les exigences d'accès des utilisateurs à chaque service cloud distinct utilisé. *N.B. Le terme « réseau » tel qu'employé dans le présent contrôle désigne tout réseau qui n'est pas un réseau Barclays, dont le fournisseur est responsable, y compris le réseau du sous-traitant du fournisseur.*	
3. Détection des attaques par déni de service	Le fournisseur doit être en mesure de détecter les attaques par déni de service (DoS) et par déni de service distribué (DDoS) et de s'en protéger.	En cas de non-respect de ce principe, Barclays et son fournisseur pourraient être dans l'incapacité d'empêcher

	Le fournisseur doit s'assurer que les canaux connectés à Internet ou externes sur lesquels s'appuient les services fournis à Barclays disposent d'une protection DDoS/DoS adéquate pour garantir la disponibilité. Si le fournisseur héberge des **systèmes et des applications fournissant des services** et incluant des données Barclays ou servant de base à un service offrant une résilience de catégorie 0 ou 1, il doit disposer d'une protection DoS adéquate pour assurer la disponibilité.	une attaque par déni de service d'atteindre l'objectif visé par son auteur.
4. Travail à distance (accès à distance)	Le fournisseur doit assurer la sécurité des informations lorsque les employés travaillent à distance. Des mesures de sécurité doivent être mises en œuvre pour protéger les informations accessibles et traitées en dehors des locaux de l'entreprise lors du travail à distance. Le fournisseur doit fournir des instructions aux membres du personnel concernant le travail à domicile. **Accès à distance au réseau Barclays** L'accès à distance au réseau Barclays via l'application Barclays Citrix n'est pas fourni par défaut. Pour accéder au réseau Barclays à partir d'emplacements non approuvés/hors du bureau/à domicile, et pour tout accès à distance, il est nécessaire d'obtenir l'approbation et l'autorisation préalables de Barclays (Bureau de la sécurité, équipe TPSecM - externalcyberassurance@barclayscorp.com). Le fournisseur doit s'assurer que les contrôles suivants sont en place pour l'accès à distance : • L'accès au réseau de Barclays nécessite un jeton RSA (logiciel) et une version prise en charge de l'application Citrix Workspace ; Barclays fournira des détails • Le fournisseur doit tenir un registre à jour et correct de ses employés autorisés à travailler à distance/de manière hybride avec une justification commerciale pour chaque employé approuvé, y compris les sous-traitants/sous-traitants ultérieurs. • **Le fournisseur doit procéder trimestriellement au rapprochement de tous les employés distants et à une présentation de ses résultats à Barclays (Bureau de la sécurité, équipe TPSecM - externalcyberassurance@barclayscorp.com).** • Barclays désactivera les identifiants de connexion dès qu'il lui sera signalé qu'un accès n'est plus nécessaire (par ex. fin de contrat d'un employé, réaffectation d'un projet, etc.) **dans les vingt-quatre (24) heures suivant la date de sortie/du dernier jour en fonction.** • Barclays désactivera rapidement les identifiants de connexion si ceux-ci n'ont pas été utilisés pendant un certain temps (cette période de non-utilisation ne doit pas dépasser un mois).	Les contrôles d'accès à distance permettent de s'assurer qu'aucun appareil non sécurisé et non autorisé n'est connecté à distance à l'environnement Barclays.

	• Le fournisseur doit s'assurer que le point utilisé pour se connecter à distance aux systèmes d'informations de Barclays est configuré de manière sécurisée (par ex. niveau des correctifs, état de la protection contre les logiciels malveillants, etc.). • Les services jouissant d'un accès à distance à des imprimantes via une application Citrix Barclays doivent être approuvés et autorisés par Barclays (Bureau de la sécurité, équipe TPSecM - externalcyberassurance@barclayscorp.com). Le fournisseur doit tenir un registre et effectuer un rapprochement chaque trimestre. • Les appareils personnels ou de type « Apportez vos appareils personnels » (limités aux ordinateurs portables ou de bureau) ne doivent pas être autorisés à accéder à l'environnement Barclays et/ou aux données Barclays résidant ou stockées dans l'environnement géré par le fournisseur (ce qui inclut le personnel du fournisseur, les consultants, le personnel de contingence, les entrepreneurs, les partenaires des services gérés, les sous-traitants/sous-traitants ultérieurs). Remarque : l'accès à distance au réseau et aux données Barclays n'est pas autorisé, sauf approbation et autorisation de Barclays. Accès à distance à l'environnement/au réseau du fournisseur Accès à distance à l'environnement géré par le fournisseur pour la prestation de services, ce qui inclut les données de Barclays résidant/stockées et/ou traitées dans l'environnement/le réseau du fournisseur. Le fournisseur doit s'assurer que les contrôles suivants sont en place au niveau du réseau du fournisseur pour l'accès à distance. • L'accès de connexion à distance au réseau du fournisseur doit être fortement chiffré dans le cas de données en transit et doit toujours s'accompagner d'une authentification multifacteurs. • Le fournisseur peut utiliser un bureau virtuel pour l'accès à distance • Le fournisseur doit tenir des registres des personnes qui ont travaillé à distance/de manière hybride. • Le fournisseur doit procéder à un recoupement de tous les utilisateurs à distance, conformément aux horaires communiqués par le fournisseur • Le fournisseur désactivera les identifiants de connexion dès qu'un accès n'est plus nécessaire (par ex. fin de contrat d'un employé, réaffectation d'un projet, etc.) dans les vingt-quatre (24) heures suivant la date de sortie/du dernier jour en fonction. • Les appareils personnels ou de type « Apportez vos appareils personnels » (limités aux ordinateurs portables ou de bureau) ne doivent pas être autorisés à accéder à	

<table>
<tr>
<td></td>
<td>l'environnement Barclays et/ou aux données Barclays résidant ou stockées dans l'environnement géré par le fournisseur (ce qui inclut le personnel du fournisseur, les consultants, le personnel de contingence, les entrepreneurs et les partenaires des services gérés).

Les règles du fournisseur concernant le travail à domicile, y compris les choses à faire et à ne pas faire, doivent être communiquées aux employés.

Les capacités de travail à distance (y compris à domicile) sont interdites dans le cours normal des activités lorsque des tiers sont contractuellement tenus de fournir des services à partir de l'espace dédié de la banque ou des locaux du fournisseur ou lorsque des exigences réglementaires sont applicables. Toutefois, des dispositions sont autorisées dans les plans de continuité des activités des tiers en cas de reprise après sinistre/crise/pandémie en accord avec Barclays et toute exigence de sécurité requise pour le travail à distance dans le cadre de l'accord contractuel.</td>
<td></td>
</tr>
<tr>
<td>5. Gestion des journaux de sécurité</td>
<td>Le fournisseur doit disposer d'un cadre de gestion des journaux et d'audit bien établi. Le cadre doit inclure des systèmes informatiques clés, notamment les applications, l'équipement réseau, les dispositifs de sécurité et les serveurs configurés pour consigner les événements clés. Pour enregistrer des événements, générer des preuves, garantir l'intégrité des informations de journal, les journaux doivent être inaltérables, empêcher tout accès non autorisé, identifier les événements de sécurité des informations pouvant entraîner un incident de sécurité des informations et soutenir les enquêtes. Le fournisseur doit s'assurer que les journaux sont centralisés, sécurisés de manière appropriée contre toute altération et/ou suppression et conservés par le fournisseur pendant une période minimale de 12 mois ou conformément aux exigences réglementaires, selon la période qui est la plus longue.
<table>
<tr><th>Catégorie</th><th>Service/Systèmes à faible impact</th><th>Service/Systèmes à impact moyen</th><th>Service/Systèmes à impact élevé</th></tr>
<tr><td>Conservation des journaux</td><td>3 mois</td><td>6 mois</td><td>12 mois</td></tr>
</table>
Le cadre de gestion des journaux de sécurité doit couvrir les éléments suivants :
• Le fournisseur doit définir les rôles et responsabilités des individus et équipes qui seront impliqués dans la gestion des journaux.</td>
<td>Le non-respect de ce contrôle se traduit par l'impossibilité pour le fournisseur de détecter l'utilisation inappropriée ou malveillante de ses services ou de ses données et d'y répondre dans un délai raisonnable.</td>
</tr>
</table>

	• Les journaux d'audit des événements prévus pour aider à surveiller une attaque, à la détecter, à la comprendre et/ou à assurer le rétablissement doivent être collectés, gérés et analysés.
	• Les journaux système doivent inclure des informations détaillées telles que la source de l'événement, la date, l'utilisateur, l'horodatage, les adresses source et de destination et les autres éléments utiles.
	• Les exemples de journaux d'événements peuvent inclure ce qui suit :
	  o Des Journaux des systèmes de détection des intrusions/protection contre les intrusions, des routeurs, des pare-feu, du proxy Web, des logiciels d'accès à distance (VPN), des serveurs d'authentification, des applications et de la base de données
	  o La consignation des connexions réussies et des échecs de connexion (par ex. erreur d'identifiant utilisateur ou de mot de passe), de la création, modification et suppression de comptes utilisateur
	  o Des journaux de modification de la configuration
	• Les services Barclays liés aux applications métiers et aux systèmes d'infrastructure techniques sur lesquels la consignation appropriée et relative aux meilleures pratiques du secteur doit être activée, y compris ceux qui ont été externalisés ou qui sont sur le cloud.
	• La synchronisation des horodatages des journaux d'événements avec une source commune fiable.
	• La protection des journaux d'événements de sécurité (par ex. chiffrement, MFA, contrôle des accès et sauvegarde).
	• Le déploiement d'outils d'analyse des journaux ou de gestion des événements et des informations de sécurité (Security Information and Event Management, SIEM), pour la corrélation et l'analyse des journaux.
	• Le déploiement d'outils nécessaires pour l'agrégation et la corrélation centralisée et en temps réel des activités anormales, des alertes réseau et système et des événements et informations de cybermenaces pertinents depuis plusieurs sources, y compris les sources internes et externes, pour mieux détecter et empêcher les cyberattaques multiniveaux.
	• L'analyse des journaux doit couvrir l'analyse et l'interprétation des événements relatifs à la sécurité des informations, afin de faciliter l'identification d'une activité inhabituelle ou d'un comportement anormal, qui peuvent constituer des indicateurs de compromission.
	• Les événements clés consignés dans un journal doivent comprendre les événements susceptibles d'avoir une incidence sur la confidentialité, l'intégrité et la disponibilité	

	du service fourni à Barclays, et qui peuvent faciliter l'identification ou la recherche d'incidents et/ou de violations des droits d'accès liés aux systèmes du fournisseur. • Le fait de vérifier régulièrement que le cadre continue de répondre aux exigences ci-dessus. **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 gestion des journaux de sécurité sont mis en œuvre pour protéger le service de Barclays - • Le client du service cloud doit définir et documenter ses exigences en matière de consignation des événements et vérifier que le service cloud répond à ces exigences. • Si une opération privilégiée est déléguée au client du service cloud, le fonctionnement et les performances de ces opérations doivent être consignés. Le client du service cloud doit déterminer si les fonctionnalités de journalisation fournies par le fournisseur de services cloud sont appropriées ou si le client du service cloud doit mettre en œuvre des fonctionnalités de journalisation supplémentaires. • Le client du service cloud doit demander des informations sur la synchronisation de l'horloge utilisée pour les systèmes du fournisseur de services cloud. • Le client du service cloud doit demander au fournisseur de services cloud des informations sur les capacités de surveillance de service disponibles pour chaque service cloud.	
6. Protection contre les logiciels malveillants	Conformément aux meilleures pratiques du secteur, le fournisseur doit avoir mis en place des politiques et procédures et doit avoir mis en œuvre les mesures techniques et les procédés commerciaux les accompagnant, afin de contrecarrer l'exécution d'un logiciel malveillant dans tout l'environnement informatique. Le fournisseur doit s'assurer que la protection contre les logiciels malveillants est appliquée en permanence à tous les actifs informatiques, pour prévenir toute interruption du service ou violation de sécurité. La protection contre les logiciels malveillants doit inclure, de manière non limitative, les éléments suivants : • Un logiciel de protection contre les logiciels malveillants, géré de façon centralisée, afin de surveiller et de protéger en continu l'environnement informatique de l'organisation. • Le logiciel de protection contre les logiciels malveillants de l'organisation doit mettre à jour son moteur d'analyse.	Les solutions de lutte contre les logiciels malveillants sont cruciales pour la protection des actifs informationnels de Barclays contre les codes malveillants.

	• Mise à jour régulière de la base de données de signatures • Tous les événements de détection de logiciels malveillants doivent être transmis aux outils d'administration de protection contre les logiciels malveillants de l'entreprise ainsi qu'aux serveurs de journaux d'événements pour en permettre l'analyse et déclencher les alertes adéquates. • Le fournisseur doit mettre en œuvre des contrôles appropriés pour se protéger contre les logiciels malveillants et les attaques sur les appareils mobiles utilisés pour les services de Barclays. • La passerelle de messagerie analyse toutes les communications par e-mail entrantes, sortantes et internes, y compris les pièces jointes et les URL, pour détecter des signes de contenu malveillant ou nuisible. N.B. La protection contre les logiciels malveillants doit inclure la détection du code mobile non autorisé, des virus, des logiciels espions, des enregistreurs de frappe, des réseaux zombies, des vers et des chevaux de Troie (liste non exhaustive).	
8. Sécurité des points d'extrémité	Le fournisseur doit adopter une approche en matière de gestion des points d'extrémité afin de s'assurer que ses points d'extrémité utilisés pour accéder au réseau Barclays ou pour accéder aux actifs informationnels et/ou données Barclays ou les traiter sont renforcés afin d'offrir une protection contre les attaques malveillantes. Les meilleures pratiques du secteur doivent être observées et l'architecture sécurisée des points d'extrémité doit inclure, de manière non limitative, les éléments suivants : • Le disque dur doit être complètement chiffré. • Tous les logiciels, services et ports inutiles doivent être désactivés. • Les droits d'accès d'administrateur pour l'utilisateur local doivent être désactivés. • L'employé du fournisseur ne doit pas être autorisé à modifier les réglages de base, comme le Service Pack par défaut, la partition système, les services par défaut, les anti-virus, etc. • Les ports USB doivent être désactivés pour empêcher la copie des informations/données Barclays sur des supports externes • Les signatures antivirus et les correctifs de sécurité doivent être mis à jour. • Désactivation du service de spouleur d'impression • Outil de prévention des données pour se protéger contre la violation des données de Barclays • Le fournisseur doit s'assurer de bloquer l'exfiltration des données de Barclays sur les sites de réseaux sociaux, les services de messagerie Web et les sites susceptibles de stocker des informations telles que, sans s'y limiter, Google Drive, Dropbox, iCloud.	En cas de non-mise en œuvre de ce contrôle, le réseau et les points d'extrémité de Barclays et du fournisseur pourraient être vulnérables aux cyberattaques.

	• Le partage et/ou le transfert des données Barclays au moyen de logiciels et/ou d'outils de messagerie instantanée doivent être désactivés. • La présence et/ou l'utilisation de logiciels non autorisés, y compris des logiciels malveillants, doit être détectée, arrêtée et corrigée. • Délai pour l'écran de verrouillage, limitation de la connexion TCP IP au réseau d'entreprise uniquement, agent de sécurité EPS avancé pour détecter les comportements suspects N.B. Les supports amovibles et les périphériques portables doivent être désactivés par défaut, et uniquement activés pour des raisons professionnelles légitimes. Le fournisseur doit conserver des images et modèles sécurisés de tous les systèmes d'une entreprise, conformément aux normes de configuration approuvées de l'organisation. Tout système existant ou nouvellement déployé qui a été compromis doit être configuré en utilisant des modèles ou images approuvés. Lorsque l'accès des points d'extrémité (ordinateurs portables et/ou de bureau) est accordé au réseau Barclays à l'aide de l'application Citrix Barclays utilisée par Internet, le fournisseur doit installer l'outil End Point Analysis (EPA), qui lui est fourni par Barclays pour valider la conformité du système d'exploitation et de sécurité du point d'extrémité, et seuls les appareils passant avec succès les vérifications réalisées par End Point Analysis se verront accorder un accès à distance au réseau de Barclays via l'application Citrix Barclays. Si le fournisseur n'est pas en mesure d'installer ou d'utiliser l'outil EPA, cette situation doit être signalée à votre responsable des relations Barclays/équipe d'assistance informatique de Barclays/équipe TPSecM. Appareils mobiles utilisés pour les services Barclays - • Le fournisseur doit implémenter des capacités de gestion des points d'extrémités unifiée ou des capacités de gestion des appareils mobiles pour contrôler et gérer tout au long du cycle de vie, de manière sécurisée, les appareils mobiles ayant accès à des informations Barclays classées confidentielles ou contenant de telles informations, afin de réduire le risque de compromission des données. • Le fournisseur doit veiller à mettre en place et utiliser des fonctionnalités de verrouillage et d'effacement à distance des appareils mobiles, afin de protéger les informations en cas de perte, de vol ou de compromission d'un appareil. • Les données de Barclays stockées et/ou traitées sur les données de l'appareil mobile doivent être chiffrées.	

	• Le fournisseur doit s'assurer que les appareils mobiles ne sont pas rootés et que la politique d'authentification forte est activée	

9. Prévention des fuites de données	Le fournisseur doit utiliser un cadre efficace approuvé par la direction pour protéger les données Barclays contre les fuites/exfiltration et inclure, sans s'y limiter, les canaux de fuite de données : -
	• Transfert non autorisé d'informations à l'extérieur du réseau interne et/ou du réseau du fournisseur
	  ○ E-mail
	  ○ Passerelle Web/Internet (y compris stockage en ligne et messageries électroniques sur le Web)
	  ○ DNS
	• Perte ou vol d'actifs informationnels Barclays sur des périphériques électroniques portables (y compris les informations électroniques sur des ordinateurs portables, appareils mobiles et périphériques portables)
	• Transfert non autorisé d'informations vers des appareils portables avec fil (par ex., en série, USB) et sans fil (par ex., Bluetooth, Wi-Fi).
	• Transfert non sécurisé d'informations à des tiers (sous-traitants, sous-traitants ultérieurs).
	• Impression ou copie inappropriée d'informations
	Des mesures de prévention des fuites de données doivent être appliquées aux systèmes, réseaux et autres dispositifs qui traitent, stockent ou transmettent des données/informations de Barclays.
		Des contrôles appropriés doivent être exécutés de manière efficace pour s'assurer que l'accès aux informations de Barclays est limité aux personnes autorisées (confidentialité), et que les informations sensibles sont protégées contre toute modification non autorisée (intégrité) et peuvent être récupérées et présentées si nécessaire (disponibilité).
		Le non-respect de ces exigences peut se traduire par la modification, la divulgation ou l'accès non autorisé aux informations sensibles de Barclays, ou des dommages, des pertes ou une destruction de telles informations, pouvant entraîner une sanction légale ou réglementaire, une atteinte à la réputation de Barclays, ou une perte d'affaires ou une perturbation des activités de Barclays.

10. Sécurité des données	Le fournisseur doit sécuriser les données de Barclays qu'il détient et/ou traite en combinant des techniques de chiffrement, de protection de l'intégrité et de prévention des pertes de données. L'accès aux données de Barclays doit être limité à ses employés autorisés et protégé contre la contamination, les attaques d'agrégation, les attaques d'inférence et les menaces de stockage, y compris, mais sans s'y limiter, les menaces provenant des environnements de cloud computing. Les contrôles de sécurité des données doivent couvrir, mais sans s'y limiter, les éléments suivants : 1. À tout moment, le fournisseur est dans l'obligation de se plier à l'ensemble des lois applicables en matière de protection des données. 2. Des politiques, des processus et des procédures ainsi que des processus métier et des mesures techniques s'y rapportant doivent être établis. Les flux de données	

	ayant lieu dans l'emplacement géographique du service (physique et virtuel) doivent être documentés et gérés. Cette documentation doit couvrir les détails liés aux applications et aux composants systèmes faisant partie du flux de données. 3. Un diagramme de flux des données Barclays ayant lieu dans des emplacements géographiques (y compris physiques et virtuels) dans les applications et les composants du système doit être tenu à jour. 4. Un inventaire de toutes les informations sensibles/confidentielles de Barclays stockées, traitées ou transmises par le fournisseur doit être tenu. 5. Toutes les données de Barclays doivent être classées et étiquetées conformément à la norme de classification et protection des informations approuvée par la direction. 6. Protection des données au repos. a. Les données au repos doivent être fortement chiffrées pour prévenir toute exposition des actifs informationnels de Barclays 7. Surveillance de l'activité des bases de données. a. L'accès aux bases de données et leur activité doivent être surveillés et enregistrés, afin d'identifier rapidement et efficacement toute activité malveillante. 8. Protection des données en cours d'utilisation. a. Les dispositifs de gestion des accès doivent contrôler le traitement des informations sensibles afin de les protéger contre l'exploitation des informations sensibles b. Des technologies de brouillage et de masquage des données doivent être utilisées pour protéger efficacement les données sensibles en cours d'utilisation contre toute divulgation accidentelle et/ou exploitation malveillante. 9. Protection des données en transit. a. Des capacités de chiffrement puissantes doivent être exploitées, pour protéger les données en transit. b. Le chiffrement puissant des données en transit est généralement réalisé par un chiffrement du transport ou de la charge utile (message ou champ de sélection). Les mécanismes de chiffrement du transport incluent, sans s'y limiter, les protocoles suivants : 10. Transport Layer Security (TLS) (conforme aux meilleures pratiques du secteur en matière de cryptographie moderne et incluant l'utilisation et/ou le rejet des protocoles et messages codés) 11. Toutes les données stockées dans un environnement de production et hors production doivent être protégées par chiffrement (reportez-vous au contrôle 16 Cryptographie)	

11. Sécurité des logiciels d'application	Le fournisseur doit développer des applications en utilisant des pratiques de codage sécurisées et au sein d'un environnement sécurisé. Lorsque le fournisseur développe des applications destinées à être utilisées par Barclays, ou qui sont utilisées pour appuyer le service fourni à Barclays, il doit mettre en place un cadre de développement logiciel sécurisé pour intégrer la sécurité dans le cycle de vie du développement logiciel. Le fournisseur doit tester et corriger les vulnérabilités du logiciel avant de le livrer à Barclays. La sécurité des logiciels d'application doit couvrir, sans avoir à s'y limiter, les éléments suivants :	Les contrôles protégeant le développement d'applications aident à s'assurer que les applications sont sécurisées au moment du déploiement.

	• Des normes de codage sécurisé approuvées par la direction et conformes aux bonnes pratiques du secteur doivent être mises en place et adoptées pour prévenir les vulnérabilités et les interruptions de service. • Des pratiques de codage sécurisé, appropriées pour le langage de programmation utilisé, doivent être définies. • Aucun développement ne doit être réalisé dans un environnement de production. • Les environnements des systèmes de production doivent être séparés de ceux des systèmes autres que de production. L'accès des développeurs aux environnements de production doit impérativement être surveillé. • Les tâches des environnements de production et des autres environnements doivent être séparées. • Les systèmes doivent être développés conformément aux meilleures pratiques du secteur en matière de développement sécurisé (par exemple, OWASP). • Le code doit être stocké de façon sécurisée et être soumis à un processus d'assurance qualité. • Ne pas copier d'informations sensibles dans les environnements des systèmes de développement et de test, à moins que des contrôles équivalents ne soient prévus pour les systèmes de développement et de test. • Le code doit être protégé de façon appropriée contre toute modification non autorisée une fois les essais validés et le code intégré aux systèmes de production. • Seuls des composants tiers fiables et à jour doivent être utilisés pour les logiciels développés par le fournisseur. • Des outils d'analyse dynamique et statique doivent être utilisés pour vérifier que les pratiques de codage sécurisé sont respectées. • Le fournisseur doit s'assurer que les données en ligne (y compris les informations personnelles) ne sont pas utilisées dans des environnements autres que de production. • Les applications et interfaces de programmation (API) doivent être conçues, développées, déployées et testées conformément aux meilleures pratiques du secteur (par ex. OWASP pour les applications Web). • L'utilisation des référentiels de code public doit être interdite. Le fournisseur doit protéger les applications Web en déployant des pare-feu pour applications Web (WAF) qui inspectent tout le trafic transitant vers les applications Web afin de détecter les attaques actuelles et courantes pour ce type d'application. Pour les applications qui ne sont pas basées sur le Web, des pare-feu d'application spécifiques doivent être déployés si de tels outils sont disponibles pour le type d'application considéré. Si le trafic est chiffré, l'appareil doit soit être placé en aval du chiffrement, soit être capable de déchiffrer le trafic avant de	

	procéder à l'analyse. Si aucune de ces solutions n'est réalisable, un pare-feu pour applications Web basé sur l'hôte doit être déployé. Le fournisseur doit s'assurer que toutes les solutions d'application SaaS (Logiciel en tant que service) utilisées pour les services de Barclays disposent d'un contrôle d'accès supplémentaire (contrôle d'authentification) en plus d'un contrôle d'authentification traditionnel (nom d'utilisateur/mot de passe). Le fournisseur doit inclure, mais sans s'y limiter, les éléments suivants : • Authentification multifacteurs (par exemple, jeton, SMS) • SSO (Authentification unique) • Contrôle d'accès basé sur l'adresse IP Un contrôle d'accès supplémentaire doit être mis en place pour les employés du fournisseur, les sous-traitants, les sous-traitants ultérieurs, les employés de Barclays et/ou les clients de Barclays.	
12. Gestion de l'accès logique (LAM)	L'accès aux actifs informationnels (y compris les logiciels, le matériel et les données) ne doit être accordé que sur la base du principe du « besoin d'en connaître », selon le principe du « moindre privilège ». Le propriétaire du système informatique/de l'actif informationnel est chargé de fournir une liste de tous les comptes ayant accès au système/à l'actif informationnel, et de définir le modèle de sécurité d'accès logique, y compris les profils d'accès et règles de séparation des tâches (SoD). Les applications Web hébergées par le fournisseur entrent dans le champ d'application de l'intégration Barclays LAM, et des contrôles Barclays LAM doivent être mis en œuvre pour ces applications. • Le principe du **besoin d'en connaître** signifie que les employés ont seulement accès aux informations qu'ils ont besoin de connaître afin d'exécuter leurs tâches autorisées. Par exemple, si un employé traite exclusivement avec des clients basés au Royaume-Uni, il n'a pas « besoin de connaître » des informations se rapportant aux clients basés aux États-Unis. • Le principe du **moindre privilège** signifie que les employés ne bénéficient que du niveau d'accès minimum nécessaire pour effectuer leurs tâches autorisées. Par exemple, si un employé a besoin de voir l'adresse d'un client mais n'est pas tenu de la modifier, le « moindre privilège » dont il doit bénéficier est alors un accès en lecture seule, qui doit être accordé à la place d'un accès en lecture/écriture. • La **séparation des tâches (SoD)** est une approche de la structuration des tâches, qui stipule qu'une tâche ne peut pas être effectuée par une seule personne. L'objectif	L'existence de contrôles de la gestion de l'accès logique appropriés aide à assurer la protection des actifs informationnels contre toute utilisation inappropriée. Les contrôles de la gestion de l'accès aident à s'assurer que seuls les utilisateurs approuvés peuvent accéder aux actifs informationnels.

	principal est d'atténuer le risque de fraude. Par exemple, un employé qui demande la création d'un compte ne doit pas être celui qui approuve la demande. Les processus de gestion des accès doivent être définis, documentés et appliqués conformément aux meilleures pratiques du secteur. Conformément à la politique du groupe Barclays en matière de sécurité des informations et de cybersécurité et à la norme de gestion des identités et des accès (IAM), cela nécessite les éléments suivants : • Intégration Barclays LAM : Le fournisseur doit s'assurer que les processus de gestion des accès exploitent l'ensemble d'outils central de Barclays IAM pour faciliter les contrôles LAM. Les listes de contrôle d'accès aux systèmes informatiques (ACL) doivent être soumises à l'équipe IAM dans le cadre du processus d'intégration du système informatique à l'ensemble d'outils IAM. Afin d'optimiser l'efficacité des contrôles LAM en aval, le fournisseur doit s'assurer que l'alimentation est automatique et quotidienne. Pour les systèmes accessibles aux utilisateurs principaux (par ex. : accès à distance/domaine, transferts), l'ACL doit être quotidienne. • Contrôles des nouveaux membres : tous les accès doivent être appropriés et approuvés avant la mise en service. • Contrôles des transferts : tous les accès doivent être examinés avant le jour du transfert pour confirmer l'accès qui doit être conservé, révoqué ou activé. L'accès confirmé pour révocation doit être supprimé avant le jour du transfert. • Contrôles des départs : tous les accès utilisés pour accéder aux ressources d'information de Barclays et/ou fournir des services à Barclays doivent être supprimés à la date de fin du contrat de l'employé avec le fournisseur. • Propriété du compte : Un compte unique doit être associé à un seul employé, qui sera responsable de toute activité conduite en utilisant ce compte. Les informations de compte et les mots de passe ne doivent pas être partagés avec d'autres employés. • Comptes inactifs : les comptes qui sont non utilisés depuis 60 jours consécutifs ou plus doivent être suspendus et/ou désactivés (et, au besoin, des archives doivent être conservées). • Re-certification de l'accès : tous les accès doivent être examinés tous les 12 mois (pour les accès non privilégiés) et tous les 6 mois (pour les accès privilégiés), afin de s'assurer que l'accès reste approprié. • Vérification de l'identité (ID&V) : des contrôles doivent être en place pour s'assurer que les processus de gestion de l'accès incluent des mécanismes appropriés pour la vérification de l'identité.	

	• Authentification : tous les comptes doivent être authentifiés avant que l'accès logique ne soit accordé. Les applications et les mécanismes d'authentification ne doivent pas afficher les mots de passe ou les codes PIN. Une longueur et une complexité appropriées des mots de passe, un historique des mots de passe, une fréquence des changements de mots de passe, une authentification multifacteurs et une gestion sécurisée des informations d'identification doivent être en place. • Sécurisation des identifiants de connexion non personnels : les identifiants de connexion non personnels (mots de passe et secrets) doivent être intégrés à un outil de gestion des informations d'identification approprié (p. ex. CyberArk). Lorsque cela n'est pas possible, les identifiants de connexion doivent être sécurisés afin qu'aucun humain ne puisse les utiliser. Lorsqu'une utilisation humaine du compte est requise, l'accès doit être temporaire et limité dans le temps, et les identifiants doivent être réinitialisés par la suite. • Gestion des identifiants de connexion : Les mots de passe des comptes personnels doivent être modifiés au moins tous les 90 jours. Les mots de passe des comptes privilégiés et interactifs doivent être modifiés tous les 120 jours ou après chaque utilisation humaine afin qu'aucun humain n'ait connaissance du mot de passe ou, si le mot de passe comporte 30 caractères ou plus, tous les 365 jours ou après chaque utilisation humaine afin qu'aucun humain n'ait connaissance du mot de passe. Les mots de passe des comptes interactifs doivent être différents des 12 mots de passe précédents. • Accès limité dans le temps : L'accès personnel privilégié à l'infrastructure de production et de reprise après sinistre utilisée par le personnel de Barclays ou le personnel non permanent de Barclays doit être limité dans le temps et avoir obtenu les autorisations appropriées. • Surveillance des activités privilégiées : La surveillance des activités privilégiées doit être effectuée. 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 des contrôles appropriés de la gestion de l'accès logique sont mis en œuvre pour protéger le service Barclays - • Le client du service cloud doit utiliser des techniques d'authentification suffisantes (par exemple, l'authentification multifacteurs) pour authentifier les administrateurs du service cloud du client du service cloud sur les capacités administratives d'un service cloud en fonction des risques identifiés. • Le client du service cloud doit s'assurer que l'accès aux informations du service cloud peut être limité conformément à sa politique de contrôle d'accès et que de telles	

	restrictions sont appliquées. Cela inclut la restriction de l'accès aux services cloud, aux fonctions des services cloud et aux données clients des services cloud gérées dans le service. • Lorsque l'utilisation de programmes utilitaires est autorisée, le client du service cloud doit identifier les programmes utilitaires à utiliser dans son environnement de cloud computing et s'assurer qu'ils n'interfèrent pas avec les contrôles du service cloud.	
13. Gestion des vulnérabilités	Le fournisseur doit exploiter un programme de gestion des vulnérabilités au moyen de politiques et procédures établies, de mesures techniques, de procédés et/ou de mesures organisationnelles s'y rapportant, visant à surveiller efficacement, détecter en temps opportun et résoudre les vulnérabilités affectant les applications détenues ou gérées par le fournisseur ou l'application développée/le code, le réseau de l'infrastructure et les composants système, pour assurer l'efficacité des contrôles de sécurité mis en place. La gestion des vulnérabilités doit couvrir, mais sans s'y limiter, les éléments suivants : • Des rôles et des responsabilités définies par rapport aux mesures de surveillance, de déclaration, de signalement et de résolution. • Des outils et une infrastructure appropriés pour la détection des vulnérabilités doivent être en place. • Le fournisseur de service conduira régulièrement des analyses des vulnérabilités à l'aide de signatures de vulnérabilité mises à jour (selon une périodicité imposée par les meilleures pratiques du secteur) afin d'identifier efficacement les vulnérabilités, connues ou non, sur toutes les classes d'actifs de l'environnement. • Un processus d'évaluation des risques doit être appliqué pour déterminer l'ordre dans lequel les vulnérabilités découvertes doivent être corrigées. • Les vulnérabilités doivent être gérées efficacement, par des activités de correction performantes et la gestion des correctifs, pour réduire le risque qu'elles soient exploitées (une résolution intervient en temps utile et dans le respect des meilleures pratiques du secteur et/ou d'un programme de gestion des correctifs). • Un processus de validation de la correction des vulnérabilités doit être mis en place pour vérifier rapidement et efficacement la correction des vulnérabilités sur toutes les classes d'actifs de l'environnement. • Les résultats d'analyses consécutives des vulnérabilités doivent être comparés régulièrement afin de s'assurer que les vulnérabilités ont été corrigées en temps opportun.	Si ce contrôle n'est pas mis en œuvre, des pirates informatiques pourraient exploiter ces vulnérabilités des systèmes pour mener des cyber-attaques qui pourraient se traduire par un dommage relevant de la réglementation et une atteinte à la réputation.

<table>
<tr>
<td></td>
<td>Pour les services du fournisseur liés aux applications/à l'infrastructure d'hébergement au nom de Barclays (y compris les tiers à haut risque communiqués)

• Si des vulnérabilités critiques et/ou graves sont identifiées, le fournisseur doit en informer Barclays sur-le-champ.
• Le fournisseur doit résoudre les vulnérabilités conformément au tableau figurant ci-dessous ou en accord avec Barclays (Bureau de la sécurité, équipe TPSecM).
<table>
<tr><th>Priorité</th><th>Notation</th><th>Jours de fermeture (maximum)</th></tr>
<tr><td>P1</td><td>Critique</td><td>15 (30 jours max.)</td></tr>
<tr><td>P2</td><td>Élevée</td><td>60</td></tr>
<tr><td>P3</td><td>Moyenne</td><td>180</td></tr>
<tr><td>P4</td><td>Faible</td><td>Pas de SLA</td></tr>
</table>
L'ensemble des problèmes de sécurité et vulnérabilités susceptibles d'avoir un impact substantiel sur l'infrastructure d'hébergement ou sur les applications de Barclays fournies par le fournisseur et pour lesquelles le fournisseur a décidé d'accepter le risque doivent être communiqués et/ou notifiés à Barclays dans les plus brefs délais et convenus par écrit avec Barclays (Bureau de la sécurité, équipe TPSecM - externalcyberassurance@barclayscorp.com).

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 gestion des vulnérabilités sont mis en œuvre pour protéger le service Barclays -

• Le client du service cloud doit demander des informations au fournisseur de services cloud sur la gestion des vulnérabilités techniques susceptibles d'affecter les services cloud fournis. Le client du service cloud doit identifier les vulnérabilités techniques qu'il sera chargé de gérer et définir clairement un processus pour les gérer.</td>
<td></td>
</tr>
<tr>
<td>14. Gestion des correctifs</td>
<td>Le fournisseur doit disposer d'un programme de gestion des correctifs soutenu par des politiques et procédures, des mesures techniques, des procédés commerciaux et/ou mesures organisationnelles, visant à surveiller et/ou à assurer le suivi du besoin de correction et à</td>
<td>Si ce contrôle n'a pas été effectué, cela peut se traduire par la fragilisation des services</td>
</tr>
</table>

	utiliser des correctifs de sécurité pour gérer tout le patrimoine et/ou l'environnement du fournisseur. Le fournisseur doit s'assurer que les serveurs, les périphériques réseau, les applications et les périphériques de point d'extrémité sont tenus à jour avec les derniers correctifs de sécurité, conformément aux meilleures pratiques du secteur, et en s'assurant des points suivants : • Le fournisseur doit évaluer et tester tous les correctifs sur des systèmes qui représentent avec précision la configuration des systèmes de production cible avant de les déployer sur les systèmes de production. Il doit également s'assurer du bon fonctionnement du service corrigé après l'application d'un correctif. Si un correctif ne peut pas être appliqué à un système, des contre-mesures appropriées doivent être prises. • Avant leur mise en œuvre, toutes les modifications informatiques clés doivent être consignées, testées et approuvées via un processus de gestion des modifications solide approuvé, afin de répondre aux besoins futurs en matière d'audit, d'enquête, de dépannage et d'analyse. • Le fournisseur doit vérifier que les correctifs sont appliqués dans les environnements de production et de reprise après incident (DR).	face aux problèmes de sécurité, entraînant ainsi un risque de compromission des données des consommateurs, de perte de service ou d'autres activités malveillantes.
15. Tests de pénétration/évaluation de la sécurité informatique	Le fournisseur doit faire appel à un prestataire de services de sécurité qualifié et indépendant pour réaliser une évaluation de la sécurité informatique/un test de pénétration portant sur l'infrastructure informatique, y compris le site de reprise après incident et les applications Web liées au(x) service(s) que le fournisseur fournit à Barclays. Cet essai ou cette évaluation doit avoir lieu au moins une fois par an afin d'identifier les vulnérabilités exploitables susceptibles de violer la confidentialité des données de Barclays par le biais de cyberattaques. Toutes les vulnérabilités doivent être hiérarchisées et suivies jusqu'à leur résolution. Le test doit être réalisé conformément aux meilleures pratiques du secteur. Pour les services du fournisseur liés aux applications/à l'infrastructure d'hébergement effectués au nom de Barclays (y compris les tiers à haut risque communiqués) • Le fournisseur doit informer et convenir avec TPSecM de la portée de l'évaluation de la sécurité et s'accorder avec Barclays sur cette portée, en particulier sur les dates de début et de fin de l'évaluation, afin de prévenir toute perturbation des activités clés de Barclays. • Tous les problèmes représentant un risque accepté doivent être communiqués à et approuvés par Barclays (Bureau de la sécurité, équipe TPSecM).	Si ce contrôle n'est pas effectué, le fournisseur pourrait être dans l'incapacité d'évaluer les cybermenaces auxquelles il est confronté et la pertinence et la solidité de ses moyens de défense. Les informations de Barclays pourraient être divulguées et/ou une perte de service pourrait se produire, ce qui peut entraîner un dommage relevant de la réglementation ou une atteinte à la réputation

<table>
<tr>
<td></td>
<td>

Une fois par an, le fournisseur doit partager avec Barclays (Bureau de la sécurité, équipe TPSecM - externalcyberassurance@barclayscorp.com) le dernier rapport d'évaluation de la sécurité.
Si des vulnérabilités critiques et/ou graves sont identifiées, le fournisseur doit en informer Barclays sur le champ.
Le fournisseur doit résoudre les vulnérabilités conformément au tableau figurant ci-dessous ou en accord avec Barclays (Bureau de la sécurité, équipe TPSecM).

<table>
<tr><th>Priorité</th><th>Notation</th><th>Jours de fermeture (maximum)</th></tr>
<tr><td>P1</td><td>Critique</td><td>15 (30 jours max.)</td></tr>
<tr><td>P2</td><td>Élevée</td><td>60</td></tr>
<tr><td>P3</td><td>Moyenne</td><td>180</td></tr>
<tr><td>P4</td><td>Faible</td><td>Pas de SLA</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>16. Cryptographie</td>
<td>
Le fournisseur doit s'assurer de l'utilisation appropriée et efficace de la cryptographie pour protéger la confidentialité, l'authenticité ou l'intégrité des données/informations de Barclays, conformément aux exigences commerciales et de sécurité des informations, en tenant compte des exigences légales, réglementaires et contractuelles liées à la cryptographie.

Lors de l'utilisation de la cryptographie, les éléments suivants doivent être pris en compte :

la politique spécifique sur la cryptographie définie par l'organisation, y compris les principes généraux de protection des informations. Une politique spécifique sur l'utilisation de la cryptographie est nécessaire pour maximiser les avantages et minimiser les risques liés à l'utilisation de techniques cryptographiques et pour éviter une utilisation inappropriée ou incorrecte.
identification du niveau de protection requis et de la classification des informations, et définition du type, de la force et de la qualité des algorithmes cryptographiques requis.
l'utilisation de la cryptographie pour la protection des informations stockées sur des supports de stockage et transmises sur des réseaux à ces périphériques ou supports de stockage.
l'approche de la gestion des clés, y compris les méthodes permettant de gérer la génération et la protection des clés cryptographiques et la récupération des

</td>
<td>Une protection par chiffrement et des algorithmes à jour et adaptés assurent la protection ininterrompue des actifs informationnels de Barclays.</td>
</tr>
</table>

	informations chiffrées en cas de perte, de compromission ou d'endommagement des clés. • Raisons de la cryptographie : le fournisseur doit documenter les raisons pour lesquelles il a recours à une technologie cryptographique et réviser celles-ci régulièrement pour s'assurer qu'elles sont toujours adaptées aux fins poursuivies. • Procédures du cycle de vie de la cryptographie : le fournisseur doit tenir à jour et gérer un jeu de procédures documentées concernant la gestion du cycle de vie de la cryptographie, détaillant les processus de bout en bout de la gestion clé, de la création à la destruction, en passant par le chargement et la distribution. Le fournisseur doit retirer ses clés après la fin de la période de service ou mettre en place un programme de rotation des clés obligatoire. • Certificats numériques : le fournisseur doit s'assurer que tous les certificats sont obtenus depuis un groupe d'autorités de certification approuvées et validées disposant de services de révocation et de politiques de gestion des certificats. Il doit également s'assurer que les certificats autosignés sont utilisés uniquement lorsqu'il est techniquement impossible de prendre en charge une solution basée sur des autorités de certification. De plus, des contrôles manuels doivent être mis en place pour garantir l'intégrité, l'authenticité des clés et la révocation et le renouvellement en temps opportun. • Approbation des opérations manuelles : le fournisseur doit s'assurer que tous les événements gérés par des individus concernant les clés et les certificats numériques, y compris l'enregistrement et la création de nouvelles clés et de nouveaux certificats, sont approuvés à un niveau approprié et qu'une trace de ces approbations est conservée. • Création des clés et cryptopériode : le fournisseur doit s'assurer que toutes les clés sont générées aléatoirement par du matériel certifié ou par logiciel, au moyen d'un générateur de nombres pseudo-aléatoire cryptographiquement sécurisé. o Le fournisseur doit s'assurer qu'une cryptopériode limitée et définie, à l'issue de laquelle les clés sont remplacées ou désactivées, peut s'appliquer à toutes les clés. Les meilleures pratiques du secteur et du National Institute of Standards and Technology (NIST, Institut national des normes et de la technologie) en la matière doivent être respectées. • Protection du stockage des clés : le fournisseur doit s'assurer que les clés de chiffrement secrètes/privées n'existent que sous les formes suivantes : o Dans les limites cryptographiques d'un module/appareil de sécurité dont le matériel est certifié. o Dans une forme chiffrée sous une autre clé établie ou dérivée d'un mot de passe.	

	○ Dans des composants séparés répartis entre des groupes de dépositaires distincts. ○ Suppression des clés de la mémoire hôte pour la période de chiffrement, sauf si requises par la protection des modules de sécurité matérielle. • Le fournisseur doit s'assurer que les clés à haut risque sont générées et conservées dans les limites de la mémoire des modules de sécurité matérielle. Cela inclut : ○ Les clés pour les services réglementés pour lesquels des modules de sécurité matérielle sont obligatoires. ○ Les certificats représentant Barclays auprès d'autorités de certification. ○ Les certificats racine, de délivrance, OCSP et d'autorités d'enregistrement utilisés pour délivrer des certificats protégeant les services Barclays. ○ Les clés protégeant les référentiels de clés agrégés stockés, les informations d'authentification ou les données personnelles. • Sauvegarde et stockage des clés : le fournisseur doit conserver une sauvegarde de toutes les clés, pour prévenir toute interruption du service en cas de corruption ou de restauration des clés. L'accès aux sauvegardes est limité à des emplacements sécurisés, soumis à une séparation des connaissances et à un double contrôle. La protection cryptographique des sauvegardes des clés doit être au moins aussi efficace que celle des clés utilisées. • Inventaire : le fournisseur doit tenir à jour un inventaire complet de l'utilisation du chiffrement dans les services qu'il fournit à Barclays. Cet inventaire doit détailler toutes les clés de chiffrement, tous les certificats numériques, et tous les logiciels et équipements de chiffrement qu'il gère, pour éviter tout dommage en cas d'incident. L'inventaire doit être signé et révisé au moins une fois par trimestre, et transmis à Barclays. L'inventaire doit inclure les éléments suivants, le cas échéant : ○ Équipe d'assistance informatique ○ Actifs associés ○ Algorithmes, longueur et hiérarchie des clés, environnement, autorité de certification, empreinte digitale, protection du stockage des clés, et objectif technique et opérationnel. • Objectif fonctionnel et opérationnel : les clés ne doivent avoir qu'un seul objectif fonctionnel et opérationnel. Elles ne doivent pas non plus être partagées entre plusieurs services ou en dehors des services Barclays. • Pistes d'audit : le fournisseur doit réaliser chaque trimestre un examen auditable des registres et conserver une preuve de cet examen au moins pour tous les événements de gestion du cycle de vie des clés et des certificats ayant une chaîne complète de responsabilités pour toutes les clés, depuis la génération jusqu'à la destruction, en	

	passant par le chargement et la distribution, afin de détecter toute utilisation non autorisée. • Équipement : le fournisseur stocke les équipements dans des zones sécurisées et conserve une piste d'audit pour toute la durée du cycle de vie des clés, afin de s'assurer que la chaîne de responsabilités des dispositifs de chiffrement n'est pas compromise. Cette piste est vérifiée tous les trimestres. • Le fournisseur doit s'assurer que l'équipement de chiffrement est certifié niveau 2 FIPS140-2, et niveau 3 pour la gestion des clés cryptographiques et de la sécurité physique, ou pour les modules de sécurité matérielle PCI. Le fournisseur peut décider d'autoriser les cartes à puce ou les jetons électroniques certifiés FIPS comme dispositifs acceptables hors site pour le stockage des clés représentant et détenues par des individus ou des clients. • Compromission des clés : le fournisseur gère et surveille un plan relatif à la compromission des clés, pour s'assurer que des clés de remplacement soient générées indépendamment des clés compromises et ainsi éviter que la clé compromise ne fournisse des informations sur la clé de remplacement. En cas de compromission, le Centre d'opérations conjointes (JOC) du Bureau de la sécurité de Barclays (CSO) doit être averti (gcsojoc@barclays.com). • Solidité des algorithmes et des clés : le fournisseur doit veiller au retrait des algorithmes peu performants et s'assurer que les algorithmes et la longueur des clés utilisés sont conformes aux meilleures pratiques applicables du secteur et du National Institute of Standards and Technology (NIST). • Le fournisseur doit évaluer l'utilisation d'algorithmes vulnérables aux attaques quantiques et les plans de migration à mettre en place.	
17. Cloud Computing	Le fournisseur (client du service cloud - CSC) doit veiller à ce que le service cloud utilisé pour le ou les services fournis à Barclays s'accompagne d'un cadre bien défini de contrôles de sécurité visant à atteindre les objectifs de confidentialité, d'intégrité, et de disponibilité, et à s'assurer que des contrôles de sécurité soient en place et fonctionnent efficacement pour protéger le ou les services Barclays. Le fournisseur doit être certifié ISO/IEC 27017 ou 27001, ou SOC 1 ou 2 ou avoir mis en place un cadre de sécurité sur le cloud similaire ou les meilleures pratiques du secteur et avoir pris des mesures de sécurité pour veiller à ce que toute la technologie cloud soit sécurisée. Il convient de s'assurer que le prestataire de services cloud est titulaire d'une certification portant sur les meilleures pratiques du secteur, incluant les contrôles appropriés et équivalents à Cloud Controls Matrix (CCM), la dernière version de Cloud Security Alliance.	Le non-respect de ce contrôle cloud risque de compromettre les données de Barclays, ce qui peut se traduire par un dommage relevant de la réglementation ou une atteinte à la réputation.

	Le fournisseur est tenu de s'assurer de la réalisation des contrôles de sécurité des données concernant les actifs informationnels et/ou les données de Barclays, qui incluent les informations personnelles stockées sur le cloud, tandis que le prestataire de services cloud (CPS) est responsable de la sécurité de l'environnement du cloud computing. Le fournisseur demeure responsable de la configuration et de la surveillance des mesures de mise en œuvre des contrôles de sécurité afin d'assurer une protection contre les incidents de sécurité, incluant les violations de données. Le fournisseur doit prendre des mesures de sécurité en ce qui concerne tous les aspects du service fourni, y compris le modèle cloud de responsabilité partagée, afin d'en garantir la confidentialité, l'intégrité, la disponibilité et l'accessibilité, en réduisant les possibilités d'accès, par des personnes non autorisées, aux informations de Barclays et aux services utilisés par Barclays. Les contrôles de sécurité du cloud doivent couvrir, sans pour autant devoir s'y limiter, les domaines énoncés ci-après pour les modèles de déploiement (IaaS/PaaS/SaaS) : • Gouvernance & mécanismes de responsabilité • Gestion de l'identité et de l'accès • Sécurité du réseau (incluant la connectivité) • Sécurité des données (en transit, au repos, stockées) • Suppression/purge sécurisée des données • Cryptographie, chiffrement et gestion des clés - CEK • Consignation et surveillance • Virtualisation • Séparation des services Les actifs informationnels et/ou les données de Barclays, y compris les informations personnelles stockées dans le cloud dans le cadre du service fourni à Barclays, doivent être approuvés par Barclays (Bureau de la sécurité, équipe TPSecM). Le fournisseur doit indiquer à Barclays les emplacements des zones de données et les zones de données de basculement où les données de Barclays seront stockées ou conservées.	

Espace bancaire dédié

Pour les services fournis nécessitant un espace bancaire dédié officiel, les exigences techniques et physiques d'un tel espace doivent être définies. (Si un espace bancaire dédié est requis pour le service, les exigences de contrôle s'appliqueront.)

Les différents types d'espace bancaire dédié sont les suivants :

Niveau 1 (première classe) : l'intégralité de l'infrastructure informatique est gérée par **Barclays** via la fourniture d'un réseau local, d'un réseau local étendu et d'ordinateurs de bureau gérés par **Barclays** à un site du fournisseur, avec un espace Barclays dédié.

Niveau 2 (classe affaire) : l'intégralité de l'infrastructure informatique est gérée par le **fournisseur** et connectée aux passerelles Extranet de **Barclays**. Le réseau local, le réseau local étendu et les ordinateurs de bureau sont détenus et gérés par le fournisseur.

Niveau 3 (classe économie) : l'intégralité de l'infrastructure informatique est gérée par le **fournisseur** et connectée aux passerelles Internet de **Barclays**. Le réseau local, le réseau local étendu et les ordinateurs de bureau sont détenus et gérés par le fournisseur.

18.1 Espace bancaire dédié – Séparation physique	La zone physique occupée doit être dédiée à Barclays et ne doit pas être partagée avec d'autres entreprises/fournisseurs. Elle doit est séparée physiquement et logiquement.
18.2 Espace bancaire dédié – Contrôle de l'accès physique	• Le fournisseur doit avoir mis en place un processus d'accès physique couvrant les méthodes et autorisations d'accès à l'espace bancaire dédié où les services sont fournis. • L'entrée dans les zones de l'espace bancaire dédié et la sortie de ces zones doivent être limitées et surveillées par le biais de mécanismes de contrôle de l'accès physique, pour s'assurer que seul le personnel autorisé peut y accéder (en fonction de son rôle) et qu'il est approuvé (par le propriétaire du service bancaire). • Une carte d'accès électronique autorisée pour accéder aux zones de l'espace bancaire dédié sur le site doit être utilisée. • Le fournisseur doit mener des vérifications de base chaque trimestre pour s'assurer que seules les personnes autorisées accèdent à l'espace bancaire dédié. Les exceptions sont étudiées minutieusement, jusqu'à résolution. • Les droits d'accès sont retirés dans les 24 heures pour tous les employés mutés, quittant ou abandonnant l'entreprise (et des archives appropriées doivent être conservées). • Des gardiens doivent patrouiller régulièrement à l'intérieur de l'espace bancaire dédié pour identifier efficacement tout accès non autorisé ou toute activité potentiellement malveillante. • Des contrôles automatiques sécurisés doivent être mis en place pour accéder à l'espace bancaire dédié, y compris : Pour les employés autorisés : o Badge avec photo, visible en permanence o Pose de lecteurs de carte de proximité o Activation et surveillance d'un mécanisme anti-retour • Le fournisseur doit mettre en place des processus et des procédures pour le contrôle et la surveillance des personnes extérieures à l'entreprise, y compris les sous-traitants, et sous-traitants ultérieurs qui accèdent à l'espace bancaire dédié pour des activités de maintenance ou d'entretien ménager.
18.3 Espace bancaire dédié – Vidéosurveillance	• Un système de vidéosurveillance doit être mis en place dans l'espace bancaire dédié pour enregistrer et signaler efficacement tout accès non autorisé et/ou toute activité malveillante, et faciliter les enquêtes en cas d'incident. • Tous les points d'entrée et de sortie de l'espace bancaire dédié doivent être sous vidéosurveillance.

	• Test de fonctionnement et de qualité des caméras et les caméras de sécurité doivent être placées judicieusement et fournir en permanence des images nettes permettant une identification si nécessaire, afin de capturer toute activité malveillante et de faciliter les enquêtes le cas échéant. Le fournisseur doit stocker les images capturées par le système de vidéosurveillance pendant 30 jours, et tous les enregistrements et dispositifs d'enregistrement doivent être placés dans un lieu sécurisé, pour éviter toute modification, toute suppression ou tout visionnage « fortuit » des écrans associés au système de vidéosurveillance. L'accès aux enregistrements doit être contrôlé et limité aux personnes autorisées.
18.4 Espace bancaire dédié – Accès au réseau Barclays et jeton d'authentification Barclays	• Tout utilisateur doit uniquement s'authentifier sur le réseau Barclays depuis l'espace bancaire dédié en utilisant un jeton d'authentification multifacteurs fourni par Barclays. • Le fournisseur doit tenir un registre des individus auxquels des jetons d'authentification Barclays (jetons RSA) ont été fournis et doit effectuer un rapprochement chaque trimestre. • Barclays désactivera les informations d'authentification dès qu'un accès n'est plus nécessaire (par exemple, licenciement d'un employé, réaffectation d'un projet, etc.) à la **date de départ/dernier jour ouvrable/date du dernier jour en fonction reçue** avec le fournisseur. • Barclays désactivera rapidement les identifiants de connexion si ceux-ci n'ont pas été utilisés pendant un certain temps (cette période de non-utilisation ne doit pas dépasser un mois). • Les services jouissant d'un accès à distance à des imprimantes via une application Citrix Barclays doivent être approuvés et autorisés par Barclays (Bureau de la sécurité, équipe TPSecM). Le fournisseur doit tenir un registre et effectuer un rapprochement chaque trimestre. Voir le contrôle - 4 Travail à distance (accès à distance)
18.5 Espace bancaire dédié - Assistance en cas d'absence	L'accès à distance à l'environnement de l'espace bancaire dédié n'est pas assuré par défaut en cas d'absence du bureau, en dehors des heures de travail ou en cas de télétravail. Tout accès à distance doit être approuvé par les équipes Barclays concernées (y compris le Bureau de la sécurité, équipe TPSecM). Les capacités de travail à distance (y compris à domicile) sont interdites dans le cours normal des activités lorsque des tiers sont contractuellement tenus de fournir des services à partir de l'espace dédié de la banque ou des locaux du fournisseur ou lorsque des exigences réglementaires sont applicables. Toutefois, des dispositions sont autorisées dans les plans de continuité des activités des tiers en cas de reprise après sinistre/crise/pandémie en accord avec Barclays et toute exigence de sécurité requise pour le travail à distance dans le cadre de l'accord contractuel.
18.6 Espace bancaire dédié - Sécurité du réseau	• Tenue à jour d'un inventaire de toutes les frontières réseau de l'organisation (via un diagramme de l'architecture du réseau). • La conception et l'implémentation du réseau doivent être révisées au moins une fois par an. • Le réseau de l'espace bancaire dédié doit être logiquement séparé du réseau d'entreprise du fournisseur au moyen d'un pare-feu. Tous les trafics entrants et sortants doivent être restreints et surveillés.

	• Le routage doit être configuré de telle sorte que les connexions soient établies uniquement avec le réseau de Barclays, et qu'elles ne soient pas routées vers d'autres réseaux du fournisseur. • Le routeur périphérique du fournisseur connecté aux passerelles extranet de Barclays doit être configuré de manière sécurisée, selon un concept de limitation des contrôles des ports, des protocoles et des services. o La connexion et la surveillance doivent être activées. • Le réseau de l'espace bancaire dédié doit être surveillé et seuls les appareils autorisés doivent être acceptés au moyen des contrôles d'accès au réseau appropriés. Voir le contrôle - 2 Frontières et sécurité du réseau
18.7 Espace bancaire dédié – Réseau sans fil	Le réseau sans fil du réseau de l'espace bancaire dédié doit être désactivé pour fournir les services Barclays.
18.8 Espace bancaire dédié – Sécurité du point d'extrémité	Les architectures de postes de travail sécurisées (y compris les ordinateurs portables) doivent être configurées conformément aux meilleures pratiques du secteur pour les ordinateurs du réseau de l'espace bancaire dédié. Les meilleures pratiques du secteur doivent être mises en place et l'architecture de la sécurité des appareils utilisés aux points d'extrémité de l'espace bancaire dédié doit inclure, de manière non limitative, les éléments suivants : • Chiffrement complet du disque dur. • Tous les logiciels, services et ports inutiles doivent être désactivés. • Les droits d'accès d'administrateur pour l'utilisateur local doivent être désactivés. • L'employé du fournisseur ne doit pas être autorisé à modifier les réglages de base, comme le Service Pack par défaut, les services par défaut, etc. • Les ports USB doivent être désactivés pour empêcher la copie des informations/données Barclays sur des supports externes • Les signatures anti-logiciels malveillants et les correctifs de sécurité doivent être mis à jour. • Désactivation du service de spouleur d'impression • Le partage et le transfert des données de Barclays au moyen de logiciels ou d'outils de messagerie instantanée doivent être désactivés. • La présence et/ou l'utilisation de logiciels non autorisés, y compris des logiciels malveillants, doit être détectée, arrêtée et corrigée. • Délai pour l'écran de verrouillage, limitation de la connexion TCP IP au réseau d'entreprise uniquement, agent de sécurité EPS avancé pour détecter les comportements suspects. Voir le contrôle - 8 Sécurité des points d'extrémité

18.9 Espace bancaire dédié – E-mails et Internet	• La connexion au réseau doit être sécurisée et restreindre les activités liées aux e-mails et à Internet sur le réseau de l'espace bancaire dédié.
	• Le fournisseur doit limiter la possibilité d'accéder aux sites de réseaux sociaux, aux services de messagerie électronique sur le Web et aux sites permettant de stocker des informations sur Internet (par exemple Google Drive, Dropbox, iCloud, etc.).
	• Le transfert non autorisé de données Barclays en dehors du réseau de l'espace bancaire dédié doit être protégé contre les fuites de données :
	  • E-mail
	  • Passerelle Web/Internet (y compris stockage en ligne et messageries électroniques sur le Web)
	• Application de filtres d'URL basés sur le réseau, qui limitent la capacité du système à se connecter aux sites Internet ou aux sites internes du fournisseur.
	• Blocage de toutes les pièces jointes et/ou du téléchargement de fonctionnalités vers des sites Web.
	• Autorisation uniquement des clients de messagerie électronique et des navigateurs Web parfaitement compatibles.

18.10 Espace bancaire dédié – « Apportez vos appareils personnels »/Appareils personnels	Les appareils personnels/de type « Apportez vos appareils personnels » ne doivent pas être autorisés à accéder à l'environnement Barclays et/ou aux données Barclays.

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. Chaque partie supportera ses propres frais en ce qui concerne tout examen/audit/évaluation.

Annexe A : Glossaire

Définitions	
Compte	Informations d'identification (par exemple, un identifiant utilisateur et un mot de passe) par le biais desquelles l'accès à un système informatique est géré via des contrôles d'accès logique.
Sauvegarde	Une sauvegarde ou le processus de sauvegarde désigne la réalisation de copies de données afin que ces copies supplémentaires puissent être utilisées pour restaurer les données d'origine après une perte de données.
Espace bancaire dédié	Espace bancaire dédié désigne tous locaux détenus ou contrôlés par un membre du groupe du fournisseur ou des sous-traitants ou sous-traitants ultérieurs, qui sont exclusivement dédiés à Barclays et depuis lesquels les services sont exécutés ou fournis.
Meilleures pratiques du secteur	Le recours aux meilleures et aux plus récentes procédures, pratiques, normes et certifications de référence sur leur marché et le respect d'un niveau de diligence et d'attention qui serait raisonnablement attendu d'une organisation professionnelle très compétente, expérimentée et de premier plan, qui fournit des services similaires ou identiques aux services fournis à Barclays.
BYOD	Bring your own devices (Apportez vos appareils personnels)
Cryptographie	L'application d'une théorie mathématique pour développer des techniques et algorithmes pouvant être appliqués aux données pour garantir des objectifs comme la confidentialité, l'intégrité des données et/ou l'authentification.
Cybersécurité	Le recours à des technologies, procédés, contrôles et mesures organisationnelles pour protéger les systèmes informatiques, les réseaux, les programmes, les appareils et les données contre les attaques numériques qui peuvent inclure (sans limitation) la divulgation, la destruction ou l'altération non autorisée d'un matériel, d'un logiciel ou de données, leur perte, leur vol ou leur endommagement.
Données	Enregistrement de faits, de concepts ou d'instructions sur un support de stockage à des fins de communication, de récupération et de traitement par des moyens automatiques, et présentation sous la forme d'informations compréhensibles par des humains.
Déni de service (attaque par)	Une tentative de rendre une ressource informatique indisponible pour ses utilisateurs prévus.
Destruction / suppression	L'action d'écraser, d'effacer ou de détruire physiquement des informations afin qu'elles ne puissent pas être récupérées.
TPSecM	L'équipe chargée de la gestion de la sécurité des tiers (TPSecM) est responsable de la gestion des positions des fournisseurs en matière de sécurité.
Chiffrement	La transformation d'un message (données, audio ou vidéo) sous une forme dénuée de sens qui ne peut pas être comprise par les lecteurs non autorisés. Cette transformation change le format texte clair en un format texte chiffré.
MSM	Module de sécurité matérielle. Appareil dédié qui assure la génération, le stockage et l'utilisation sécurisés des clés de chiffrement, ainsi que l'accélération des processus de chiffrement.

Actif informationnel	Toute information caractérisée par une certaine valeur en termes de confidentialité, d'intégrité et de disponibilité. Ou Une information ou un groupe d'informations présentant une valeur pour l'organisation.
Propriétaire de l'actif informationnel	La personne physique, au sein de l'entreprise, chargée de classer un actif et de s'assurer de sa gestion correcte.
Moindre privilège	Le niveau d'accès/de permission minimal permettant à un utilisateur ou à un compte d'accomplir les fonctions professionnelles relevant de son rôle.
Périphérique réseau/équipement réseau	Tout appareil informatique connecté à un réseau et utilisé pour gérer, prendre en charge ou contrôler un réseau. Cela inclut, sans s'y limiter, les routeurs, les commutateurs, les pare-feu et les équilibreurs de charge.
Code malveillant	Un logiciel écrit dans l'intention de contourner la politique de sécurité d'un système informatique, d'un appareil ou d'une application. Les virus informatiques, les chevaux de Troie et les vers informatiques en sont des exemples.
Authentification multifacteurs (MFA)	Une authentification exigeant deux techniques d'authentification différentes ou plus. Parmi les exemples figure l'utilisation d'un jeton de sécurité, où une authentification fructueuse dépend de quelque chose que la personne détient (à savoir, le jeton de sécurité) et de quelque chose que l'utilisateur connaît (à savoir, le code confidentiel du jeton de sécurité).
Informations personnelles	Les informations relatives à une personne physique identifiée ou identifiable (« personne concernée ») ; une personne physique identifiable est une personne 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 à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.
Accès privilégié	Désignation retenue pour l'accès spécial (supérieur à un niveau standard), les permissions ou les aptitudes dont bénéficie un utilisateur, un procédé ou un ordinateur.
Compte privilégié	Un compte qui dispose d'un niveau élevé de contrôle sur un système informatique donné. Un tel compte est généralement utilisé pour la maintenance des systèmes, la gestion de la sécurité ou les modifications de configuration d'un système informatique. Exemples : comptes « Administrateur », « racine », Unix avec uid=0, comptes de support, comptes de gestion de la sécurité, comptes d'administration des systèmes et comptes administrateur locaux
Accès à distance	Technologie et techniques utilisées pour accorder, à partir d'un site externe et à des utilisateurs autorisés, un accès aux réseaux et systèmes d'une organisation.
Système	Dans le cadre du présent document, un système se compose de personnes physiques, de procédures, d'équipements informatiques et de logiciels. Les éléments de cette entité complexe sont utilisés en combinaison dans l'environnement opérationnel ou d'assistance visé pour exécuter une tâche donnée ou atteindre un objectif spécifique, fournir une assistance ou satisfaire les exigences d'une mission.
Doit	Signifie que les implications devront être parfaitement comprises et soigneusement évaluées.

Incidents de sécurité	Les incidents de sécurité sont des événements qui incluent, de manière non limitative : • Tentatives (fructueuses ou infructueuses) d'obtenir l'accès non autorisé à un système ou à ses données. • Perturbation indésirable ou déni de service. • Utilisation non autorisée d'un système pour le traitement ou le stockage de données. • Modifications des caractéristiques de l'équipement, du microprogramme ou des logiciels sans connaissance, instruction ou consentement du propriétaire. • Vulnérabilité d'une application qui aboutit à l'accès non autorisé aux données.
Machine virtuelle :	environnement complet prenant en charge l'exécution du logiciel invité. REMARQUE : une machine virtuelle est une encapsulation complète du matériel virtuel, des disques virtuels et des métadonnées qui lui sont associées. Les machines virtuelles permettent le multiplexage de la machine physique sous-jacente via une couche logicielle appelée hyperviseur.

Secret bancaire

Contrôles supplémentaires uniquement pour les juridictions autorisant le secret bancaire (Suisse/Monaco)

Version finale 14.0 – Octobre 2024

Domaine/intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Rôles et responsabilités	Le fournisseur doit définir et communiquer les rôles et responsabilités relatifs à la gestion des données d'identification des clients (ci-après DIC). Le fournisseur doit examiner les documents décrivant les rôles et responsabilités relatifs aux DIC après chaque changement substantiel apporté au modèle d'exploitation (ou à l'activité) du fournisseur ou au moins une fois par an et les distribuer conformément au secret bancaire approprié. Les rôles clés doivent inclure un cadre supérieur, responsable de la protection et de la surveillance de l'ensemble des activités relatives aux DIC (voir l'annexe A pour la définition de cet acronyme). Le nombre de personnes accédant aux DIC doit être limité au strict minimum, selon le principe du besoin de connaître.	La définition claire des rôles et des responsabilités soutient la mise en œuvre de l'annexe Obligations de contrôle pour les fournisseurs externes.
2. Signalement de violation de DIC	Des contrôles, processus et procédures documentés doivent être mis en place pour assurer le signalement et la gestion de toute violation ayant un impact sur des DIC. Toute violation des exigences de gestion (tel que défini au tableau B2) doit faire l'objet d'une réponse du fournisseur et être signalée immédiatement à l'entité Barclays correspondante soumise au secret bancaire (au plus tard dans les 24 heures). Un processus de réponse en cas d'incident destiné à gérer en temps opportun et à signaler régulièrement les événements impliquant des DIC doit être défini et testé régulièrement. Le fournisseur doit s'assurer que les mesures correctives identifiées à la suite d'un incident soient traitées selon un plan correctif (action, propriété, date de livraison), et partagées et approuvées par la juridiction autorisant le secret bancaire correspondante. Une mesure corrective doit être prise par le fournisseur en temps utile. Si le fournisseur externe fournit des services de conseils et qu'un de ses employés est à l'origine d'un incident de prévention de perte de données, la banque signalera l'incident au fournisseur. Le cas échéant, la banque a le droit de demander le remplacement de l'employé.	L'existence d'un processus de réponse en cas d'incident aide à assurer la maîtrise rapide et à éviter l'aggravation des incidents. Toute violation ayant un impact sur des DIC peut porter gravement atteinte à la réputation de Barclays et entraîner des amendes et une perte de l'agrément bancaire en Suisse ou à Monaco.

3. Formation et sensibilisation	Les employés du fournisseur qui ont accès à des DIC et/ou les gèrent doivent suivre une formation* qui englobe les exigences relatives au secret bancaire des DIC après toute modification des réglementations ou au moins une fois par an. Le fournisseur doit s'assurer que tous ses nouveaux employés (qui ont accès à des DIC et/ou les gèrent), suivent, dans un délai raisonnable (d'environ 3 mois), une formation pour s'assurer qu'ils comprennent leurs responsabilités eu égard aux DIC. Le fournisseur doit assurer un suivi des employés qui ont suivi la formation. * les juridictions autorisant le secret bancaire fourniront des orientations sur le contenu attendu de la formation.	La formation et la sensibilisation viennent à l'appui de tous les autres contrôles présentés dans cette annexe.
4. Schéma d'étiquetage des informations	***Le cas échéant****, le fournisseur doit appliquer le schéma d'étiquetage des informations Barclays (tableau E1 de l'annexe E), ou un autre programme convenu avec la juridiction autorisant le secret bancaire, à l'ensemble des actifs informationnels détenus ou traités pour le compte de la juridiction autorisant le secret bancaire. Les exigences de gestion des données DIC sont stipulées au tableau E2 de l'annexe E. * « ***le cas échéant*** » *fait référence à l'avantage qu'apporte l'étiquetage par rapport au risque associé. Par exemple, l'étiquetage d'un document n'est pas approprié si cela conduit à la violation des exigences anti-violation réglementaires.*	L'existence d'un inventaire des actifs informationnels complet et précis est fondamentale pour assurer la mise en œuvre des contrôles appropriés.
5. Cloud Computing/stockage externe	Toute utilisation du cloud computing et/ou d'un stockage externe des DIC (sur des serveurs en dehors de la juridiction autorisant le secret bancaire ou en dehors de l'infrastructure du fournisseur) dans le cadre du service offert à ladite juridiction doit être approuvée par les équipes locales concernées correspondantes (y compris le bureau de la sécurité, et les services Conformité et Juridique). De plus, des contrôles doivent être mis en œuvre conformément aux lois et réglementations applicables dans la juridiction autorisant le secret bancaire correspondante pour protéger les informations DIC eu égard au profil de risque élevé qu'elles présentent.	Le non-respect de ce principe risque de compromettre les données clients (DIC) incorrectement protégées, ce qui peut se traduire par une sanction légale ou réglementaire, ou une atteinte à la réputation.

Annexe B : Glossaire

** Les données d'identification des clients sont des données particulières en raison des lois relatives au secret bancaire en vigueur en Suisse et à Monaco. À ce titre, les contrôles énumérés ici viennent compléter ceux énumérés ci-dessus.

Terme	Définition
DIC	Données d'identification des clients
CSSI	Cybersécurité et sécurité des informations
Employé du fournisseur	Toute personne directement affectée au fournisseur en tant qu'employé permanent, ou toute personne fournissant des services au fournisseur pendant une période limitée (comme un consultant)
Actif	Une information ou un groupe d'informations présentant une valeur pour l'organisation.
Système	Dans le cadre du présent document, un système se compose de personnes physiques, de procédures, d'équipements informatiques et de logiciels. Les éléments de cette entité complexe sont utilisés en combinaison dans l'environnement opérationnel ou d'assistance visé pour exécuter une tâche donnée ou atteindre un objectif spécifique, fournir une assistance ou satisfaire les exigences d'une mission.
Utilisateur	Un compte attribué à un employé, consultant, sous-traitant ou travailleur intérimaire du fournisseur qui dispose d'un accès autorisé à un système appartenant à Barclays sans privilèges étendus.

Annexe C : DÉFINITION DE DONNÉES D'IDENTIFICATION DES CLIENTS

Les **DIC directes (DICD)** peuvent être définies comme des identifiants uniques (détenus par le client) qui permettent, en tant que tels et d'eux-mêmes, d'identifier un client sans accéder aux données figurant dans les applications bancaires de Barclays. Elles ne doivent pas être ambiguës, ni sujettes à interprétation, et peuvent comprendre des informations comme le prénom, le nom, le nom de la société, la signature, l'ID de réseaux sociaux, etc. Les DIC directes désignent des données clients qui ne sont pas détenues ni créées par la banque.

Les **DIC indirectes (DICI)** sont réparties en 3 niveaux

- Les **DICI N1** peuvent être définies comme des identifiants uniques (détenus par la banque) qui permettent d'identifier individuellement un client si un accès aux applications bancaires ou à d'autres **applications tierces** est fourni. L'identificateur ne doit pas être ambigu, ni sujet à interprétation, et peut comprendre des identifiants comme le numéro de compte, le code IBAN, le numéro de carte de crédit, etc.
- Les **DICI N2** peuvent être définies comme des informations (détenues par le client) qui, associées à d'autres, permettraient de déduire l'identité d'un client. Alors que ces informations ne peuvent pas être utilisées seules pour identifier un client, elles peuvent être utilisées avec d'autres informations pour identifier un client. Les DICI N2 doivent être protégées et gérées avec la même rigueur que les DICD.
- Les **DICI N3** peuvent être définies comme des identifiants uniques mais anonymisés (détenus par la banque) qui permettent d'identifier un client si un accès aux applications bancaires est fourni. La différence avec les DICI N1 est que les informations sont classées « Restreintes - externes » au lieu de secret bancaire, à savoir qu'elles ne sont pas soumises aux mêmes contrôles.

Veuillez vous référer au Schéma 1 Arbre décisionnel DIC pour obtenir une vue d'ensemble de la méthode de classification.

Les DIC directes et indirectes N1 ne doivent pas être partagées avec des personnes extérieures à la Banque et doivent respecter à tout moment le principe du besoin de connaître. Les DICI N2 peuvent être partagées selon le principe du besoin de connaître, mais ne doivent pas être partagées conjointement avec toute autre DIC. En partageant plusieurs DIC, il est possible de créer une « association toxique » qui peut potentiellement révéler l'identité d'un client. Nous définissons une association toxique comme un ensemble comprenant au minimum deux DICI N2. Les DICI N3 peuvent être partagées car elles ne sont pas classées comme des informations de niveau secret bancaire, à moins qu'un usage récurrent du même identifiant ne puisse se traduire par la collecte de données DICI N2 suffisantes pour révéler l'identité du client.

Classification des informations	Secret bancaire			Diffusion restreinte - Interne
Classification	DIC directes (DICD)	DIC indirectes (DICI)		
		Indirectes (N1)	Potentiellement indirectes (N2)	Identifiant impersonnel (N3)
Type d'informations	Nom du client/prospect	Numéro du conteneur/ID du conteneur	Lieu de naissance	Tout identifiant strictement interne de l'application de traitement/hébergement des DIC
	Nom de la société	Numéro MACC (compte monétaire avec ID conteneur Avaloq)	Date de naissance	Identifiant dynamique
	Relevé de compte	ID services de données partagés	Nationalité	ID rôle partie CRM
	Signature	Code IBAN	Intitulé	ID conteneur externe
	ID réseau social	Coordonnées de connexion banque électronique	Situation de famille	
	Numéro de passeport	Numéro de coffre	Code postal	
	Numéro de téléphone	Coordonnées de carte de crédit	Situation patrimoniale	
	Adresse e-mail	Message SWIFT	Solde/montant d'opération important	
	Intitulé du poste ou intitulé PPE	ID interne partenaire professionnel	Dernière visite du client	
	Pseudonyme		Langue	
	Adresse IP		Sexe	
	Numéro de télécopie		Date d'expiration CC	
			Contact principal	
			Lieu de naissance	
			Date d'ouverture du compte	

Exemple : Si vous envoyez un courriel ou partagez un document avec des personnes externes (y compris des tiers en Suisse ou à Monaco) ou des collaborateurs internes au sein d'une autre société affiliée/filiale située en Suisse, à Monaco ou dans d'autres pays (par exemple au Royaume-Uni).

1. Nom du client

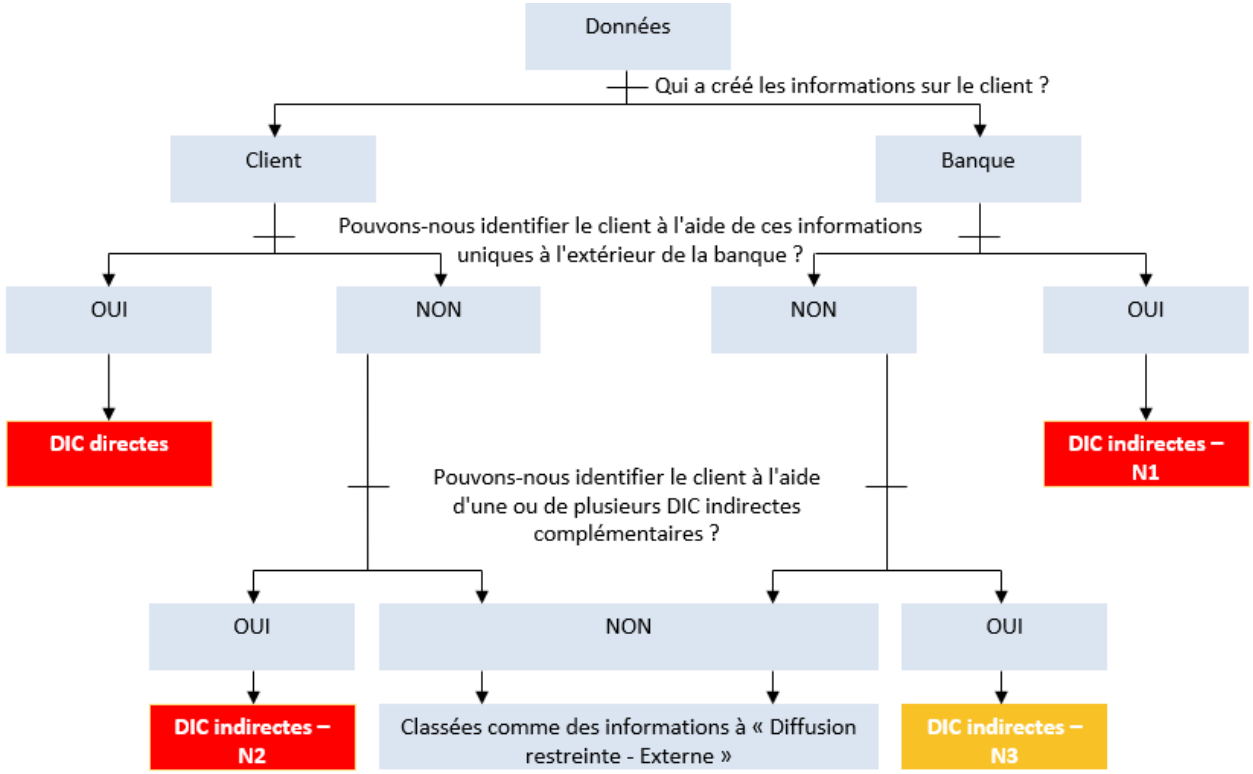
   (DICD) = violation du secret bancaire

2. ID conteneur

   (DICI N1) = violation du secret bancaire

3. Situation patrimoniale + nationalité

   (DICI N2) + (DICI N2) = violation du secret bancaire



Annexe D : Schéma d'étiquetage des informations Barclays

Tableau D1 : Schéma d'étiquetage des informations Barclays

** L'étiquette Secret bancaire est propre aux juridictions autorisant le secret bancaire.

Étiquette	Définition	Exemples
Secret bancaire	Informations apparentées à toute donnée d'identification des clients (DIC) directe ou indirecte, suisse. La classification « secret bancaire » s'applique aux informations apparentées à toute donnée d'identification des clients directe ou indirecte. Par conséquent, un accès par tous les employés, même ceux situés au sein de la juridiction propriétaire, n'est pas approprié. L'accès à ces informations est requis uniquement par les individus qui ont besoin de les connaître pour remplir leurs tâches officielles ou leurs responsabilités contractuelles. Une divulgation, un accès ou un partage non autorisé(e), aussi bien au niveau interne qu'externe de l'entité, desdites informations peut avoir un impact critique, entraîner des poursuites pénales, et avoir des conséquences civiles et administratives comme des amendes et une perte de l'agrément bancaire, si elles sont divulguées à des membres du personnel non autorisés aussi bien au niveau interne qu'externe.	• Nom du client • Adresse du client • Signature • Adresse IP du client (plus d'exemples à l'annexe D)

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 (NDA) 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 ; 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 informations personnelles. • Évaluations de la vulnérabilité. • Rapports et résultats d'audit.

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 ; 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 » (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.	• Plans de nouveaux produits. • Contrats de clients. • Contrats juridiques. • Informations clients individuelles/de petit volume destinées à être envoyées au niveau externe. • Communications avec les clients. • 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) n'appartenant pas à Barclays. • Tous les rapports de recherche. • Certains documents de marketing. • Analyses du marché.
Aucune restriction	Des informations destinées à une diffusion générale, ou qui ne sont pas susceptibles d'avoir un impact sur l'entreprise si elles étaient diffusées.	• Documents de marketing. • Publications. • Annonces publiques. • Offres d'emploi. • Informations sans impact sur Barclays.

Tableau D2 : Schéma d'étiquetage des informations – exigences de gestion

** Exigences de gestion spécifiques des données DIC pour garantir leur confidentialité conformément aux exigences réglementaires

Étape du cycle de vie	Exigences relatives au secret bancaire
Création et étiquetage	Comme pour « Diffusion restreinte - externe » et : • Un propriétaire des DIC doit être affecté aux actifs.
Stockage	Comme pour « Diffusion restreinte - externe » et : • Les actifs doivent être stockés sur des supports amovibles uniquement pendant la durée explicitement requise par un besoin commercial spécifique, les organismes de réglementation ou des auditeurs externes. • Les volumes importants d'actifs informationnels relevant du secret bancaire ne doivent pas être stockés sur des appareils/supports portables. Pour obtenir de plus amples informations, veuillez contacter l'équipe cybersécurité et sécurité des informations locale (ci-après CSSI). • 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, selon le principe du besoin de connaître ou du besoin d'avoir. • Des pratiques de sécurisation du lieu de travail, comme un bureau bien rangé et un verrouillage de l'ordinateur de bureau, doivent être observées pour protéger les actifs (physiques ou électroniques). • Les actifs informationnels sur des supports amovibles doivent uniquement être utilisés pour le stockage pendant la durée explicitement requise et doivent être conservés sous clé lorsqu'ils ne sont pas utilisés. • Les transferts de données ponctuels vers des appareils/supports portables exigent l'autorisation du propriétaire des données, du service conformité et de l'équipe CSSI.
Accès et utilisation	Comme pour « Diffusion restreinte - externe » et : • Les actifs ne doivent pas être emportés/visualisés en dehors du site (locaux de Barclays) sans l'autorisation formelle du propriétaire des DIC (ou son adjoint). • Les actifs ne doivent pas être emportés ni visualisés en dehors du territoire de tenue des registres du client sans l'autorisation formelle du propriétaire des DIC (ou son adjoint) et du client (décharge/pouvoir limité). • Des pratiques de sécurisation du télétravail, en s'assurant qu'aucun espionnage par-dessus l'épaule n'est possible, doivent être observées lorsque des actifs physiques sont emportés en dehors du site.
	• S'assurer que les personnes non autorisées ne peuvent pas observer ou accéder aux actifs électroniques contenant des DIC en utilisant un accès restreint aux applications d'entreprise.
Partage	Comme pour « Diffusion restreinte - externe » et : • Les actifs doivent être distribués uniquement en se conformant au « principe du besoin de connaître » ET au sein des systèmes d'information et du personnel de la juridiction d'origine autorisant le secret bancaire. • Les actifs transférés ponctuellement au moyen de supports amovibles exigent l'autorisation du propriétaire des actifs informationnels et de l'équipe CSSI.

	• Les communications électroniques doivent être chiffrées pendant leur transit. • Les actifs (copie papier) envoyés par courrier doivent être expédiés au moyen d'un service exigeant un accusé de réception. • Les actifs doivent être distribués uniquement en se conformant au « principe du besoin de connaître ».
Archivage et destruction	Comme pour « Diffusion restreinte - externe »

*** 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 restreintes – internes ou secrètes–, en fonction de l'impact qu'une divulgation non autorisée aurait sur l'entreprise.

Étape du cycle de vie	Diffusion restreinte - interne	Diffusion restreinte - externe	Secrètes
Création et introduction	• Un propriétaire des actifs informationnels doit être affecté aux actifs.	• Un propriétaire des actifs informationnels doit être affecté aux actifs.	• Un propriétaire des actifs informationnels doit être affecté aux actifs.
Stockage	• 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.	• 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 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.	• 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.
Partage	• 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.	• 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.	• Une étiquette d'information visible doit être apposée sur chaque page des actifs physiques.

	• 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 électroniques doivent porter un étiquetage d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page un étiquetage 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 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.	• 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 un étiquetage 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 uniquement être distribués aux individus spécialement autorisés à les recevoir par le propriétaire des actifs informationnels.

			• 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.
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 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. • Les supports sur lesquels des actifs électroniques secrets ont été stockés doivent être nettoyés de façon appropriée avant ou pendant la destruction.