BARCLAYS

External Supplier Control Obligation

Sécurité des informations et cybersécurité (SIC)

Version 11.0 - Octobre 2021

Domaine/intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Cadre et gouvernance en matière de sécurité des informations/cybersécurité	Le fournisseur doit avoir mis en place un cadre standard et homogène du secteur pour assurer la gouvernance des informations et de la cybersécurité conformément aux meilleures pratiques du secteur (actuellement, les meilleurs programmes du secteur incluent NIST, ISO/IEC 27001, ITIL et COBIT) et aux exigences du secteur applicables. Cette approche permettra au fournisseur de veiller à ce que son procédé, sa technologie et son environnement physique s'accompagnent de protections ou contre-mesures. Un programme de gouvernance des informations bien structuré et en place dans toute l'entreprise doit veiller à ce que les principaux concepts de disponibilité, d'intégrité et de confidentialité soient renforcés par des contrôles adéquats prévus pour atténuer ou limiter les risques de perte, de dérangement ou de corruption pesant sur les informations ; le fournisseur doit s'assurer que les contrôles des exigences de Barclays sont en place et fonctionnent efficacement pour protéger le ou les services Barclays. Le cadre de gouvernance en matière de sécurité doit être développé, documenté, approuvé et appliqué, ce qui inclut des protections administratives, organisationnelles, techniques et physiques visant à protéger les actifs et les données contre toute perte, mauvaise utilisation, divulgation, modification et destruction, et contre tout accès. Le programme de sécurité doit inclure, mais sans s'y limiter, les éléments suivants : • Un programme énonçant des normes, une politique et des procédures et qui crée efficacement, met en œuvre et mesure en permanence l'efficacité de l'application des normes et politiques de sécurité des informations et de cybersécurité. • Un programme de sécurité exhaustif présentant une structure de direction, des mécanismes de signalement, et un contrôle exécutif clairs pour faire émerger une culture de sensibilisation et de responsabilité envers la sécurité. • Des politiques, des procédures et des procédés qui sont approuvés et communiqués à travers toute l'organisation. • Ces procédures, normes et politiques doivent être révisées régulièrement (au moins une fois par an, ou à chaque modification significative) et doivent être adaptées pour qu'elles soient conformes aux pratiques actuelles en matière de cybersécurité et à l'environnement changeant des menaces.	En cas de non-respect de ce principe, Barclays ou ses fournisseurs pourraient ne pas bénéficier d'une surveillance appropriée en matière de sécurité des informations/cybersécurité ou être dans l'incapacité d'apporter la preuve de cette surveillance. Un cadre solide pour la gouvernance de la sécurité donne le la en matière de sécurité pour toute l'organisation.

	• Le fournisseur doit s'assurer qu'une responsabilité individuelle envers les informations et les systèmes de sécurité est instaurée, en veillant à ce que la propriété appropriée des systèmes de sécurité, informations et environnements professionnels critiques soit attribuée aux individus compétents. • Le fournisseur coordonne et aligne les rôles et responsabilités du personnel en implémentant, gérant et supervisant l'efficacité du cadre et de la stratégie de sécurité avec les partenaires internes et externes. • Le fournisseur doit mettre en œuvre une infrastructure sécurisée et un cadre de contrôle pour protéger l'organisation contre toute menace (incluant la cybersécurité) • Des examens et évaluations indépendants doivent être conduits par des experts au moins une fois par an, pour s'assurer que l'organisation résout les problèmes de non-conformité des politiques, normes, procédures et obligations de conformité établies. **Le fournisseur doit veiller à ce que Barclays soit notifié (par écrit) dès qu'il est légalement tenu de le faire en cas de fusion, d'acquisition ou de tout autre changement de propriété l'affectant.**	
2. Gestion du risque de sécurité	Le fournisseur doit mettre sur pied un programme de gestion des risques qui évalue, atténue et surveille efficacement les risques liés à la sécurité et évoluant à travers son environnement contrôlé. Ce programme doit inclure, mais sans s'y limiter, les éléments suivants : • Le fournisseur doit avoir mis en place un cadre de gestion des risques approuvé par les instances dirigeantes appropriées (comité de direction ou l'un de ses sous-comités, par exemple). Ce cadre de gestion doit être intégré à la stratégie globale de l'entreprise ainsi qu'au cadre général de gestion des risques. • Alignées sur ce cadre de gestion des risques, des évaluations des risques doivent être menées au moins une fois par an, à intervalles réguliers planifiés ou lors d'événements particuliers, par exemple suite à un incident ou aux enseignements tirés associés (et conjointement à toute modification des systèmes d'informations) pour déterminer la probabilité et l'impact de tous les risques identifiés en utilisant des méthodes qualitatives et quantitatives. La probabilité et l'impact associé au risque inhérent et résiduel doivent être	Si ce contrôle n'est pas opéré, les fournisseurs risquent de ne pas être en mesure de démontrer la prise des mesures appropriées pour gérer les risques de sécurité.

	déterminés de façon indépendante, en tenant compte de toutes les catégories de risques (résultats d'audit, analyses de vulnérabilité et des menaces, et conformité réglementaire, par exemple). • Un régime approprié d'options de gestion des risques de sécurité doit être sélectionné, en tenant compte des résultats de l'évaluation des risques. • Un plan de gestion des risques de sécurité doit être élaboré, et les critères d'acceptation des risques doivent être définis par des individus responsables ayant les qualifications adéquates. Ces critères doivent inclure, de manière non limitative, la sensibilité de ces données et leur criticité commerciale. • Le fournisseur doit s'assurer que les risques identifiés sont minimisés ou éliminés de l'environnement en hiérarchisant les risques et en mettant en place des mesures de protection. • Les risques doivent être atténués jusqu'à un niveau acceptable. Des niveaux d'acceptation basés sur les critères de risques doivent être établis et documentés, conformément aux délais de résolution raisonnables et à l'approbation des parties prenantes. • Les évaluations des risques associées aux exigences de gouvernance des données doivent prendre en compte les éléments suivants : o Classification et protection des données contre toute utilisation, divulgation, perte, destruction, altération et falsification non autorisées, ou contre tout accès non autorisé. o Connaissance des emplacements où les données sensibles sont stockées et transmises à travers les applications, les bases de données, les serveurs et l'infrastructure réseau. o Respect des périodes de rétention définies et des exigences de mise au rebut en fin de vie. • Tous les ans, le fournisseur doit conduire au moins une évaluation des risques de sécurité liée à la sécurité ; selon les environnements, une fréquence supérieure peut être envisagée. **Le fournisseur doit déclarer par un enregistrement et avertir Barclays s'il est dans l'incapacité d'atténuer ou d'éliminer les risques significatifs susceptibles d'avoir une incidence sur les données de Barclays et/ou le service fourni à Barclays.**	
3. Rôles et responsabilités	Le fournisseur est tenu de veiller à ce que toutes les personnes prenant part à la fourniture du service à Barclays connaissent les exigences de contrôle formulées par Barclays dans ce document, et les respectent. Dans le cadre des exigences de contrôle	La définition claire des rôles et des responsabilités soutient la mise en œuvre des Obligations de contrôle

	de Barclays, le fournisseur doit s'assurer qu'une équipe appropriée de spécialistes et/ou que des personnes ayant les compétences requises ainsi que des rôles et des responsabilités définies pour la gestion des exigences de contrôle de Barclays soient en place et interviennent efficacement pour assurer la protection du ou des services de Barclays. Le fournisseur doit définir et communiquer les rôles et les responsabilités concernant tous les domaines de sécurité couverts par l'exigence en matière de contrôle. Ceux-ci doivent être révisés régulièrement (et dans tous les cas au moins une fois tous les 12 mois) et après chaque changement matériel apporté à l'activité ou au modèle d'exploitation du fournisseur. Parmi les rôles clés doit figurer un cadre supérieur, qui sera responsable de la sécurité des informations et de la cybersécurité. Il appartient au fournisseur de s'assurer que ses salariés et/ou son personnel connaissent les exigences de contrôle énoncées par cette politique standard ainsi que par les politiques et normes connexes, et les respectent. Le fournisseur doit nommer un contact responsable de tout signalement et chargé de communiquer avec Barclays.	pour les fournisseurs par rapport aux informations et à la cybersécurité.
4. Usage approuvé	Le fournisseur doit définir et publier des critères d'utilisation acceptables pour informer tout son personnel (incluant les entrepreneurs et les utilisateurs tiers des systèmes de l'organisation) sur ses responsabilités. 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 acceptable 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. Le fournisseur doit prendre les mesures appropriées pour s'assurer du respect des critères d'utilisation acceptable.	
5. Formation et sensibilisation	Le fournisseur doit avoir établi un programme de formation, d'éducation et de sensibilisation à la sécurité pour tous les employés, sous-traitants et utilisateurs tiers des systèmes de l'organisation. Ce programme doit être obligatoire le cas échéant. Toutes les personnes ayant accès aux informations ou données de Barclays doivent suivre un programme de formation et d'éducation offrant une sensibilisation appropriée et être tenues au courant régulièrement des mises à jour des procédures, processus et politiques techniques et de l'organisation liées à leur fonction au sein de celle-ci. Les niveaux d'éducation, de formation et de sensibilisation doivent être fonction des rôles et consignés dans une plate-forme adaptée de gestion des formations. Le fournisseur doit s'assurer que tout le personnel sous son contrôle suit une formation obligatoire portant sur la sécurité des informations (continuellement mise à jour pour tenir compte de l'évolution des menaces et des risques spécifiques au secteur) et qui inclut les meilleures pratiques du secteur et la protection des données Barclays. Cette formation doit être dispensée dans les trente jours qui suivent la date à laquelle l'employée a rejoint l'organisation, et une remise à niveau doit avoir lieu au moins une fois par an par la suite. Les éléments ci-dessous doivent être inclus, le cas échéant : Les groupes à haut risque, par exemple les personnes disposant d'un accès privilégié ou à des postes sensibles pour l'entreprise (y compris les utilisateurs privilégiés, les cadres supérieurs, le personnel en charge de la sécurité des informations et de la cybersécurité, et les parties prenantes tierces), doivent suivre une formation approfondie de sensibilisation situationnelle sur la sécurité des informations et la cybersécurité adaptée à leurs rôles et responsabilités. Au cas où et quand cela semblerait appropriée, cette formation doit être assurée par des experts tiers externes.	La formation et la sensibilisation viennent à l'appui de tous les autres contrôles présentés dans cette annexe. En cas de non-respect de ce principe, les employés pertinents ne seront pas informés des cyber-risques et des vecteurs utilisés pour mettre en œuvre des attaques et seront dans l'incapacité de détecter ou de prévenir des attaques.
6. Gestion des incidents de sécurité	Le fournisseur doit établir un cadre de gestion des incidents de sécurité pour confirmer efficacement, signaler efficacement, limiter et résoudre un incident de sécurité survenant dans son environnement.	L'existence d'un processus de gestion et de réponse en cas d'incident aide à assurer la maîtrise

	Le fournisseur doit rédiger des plans adaptés de réponse aux incidents par rapport à chaque catégorie de risques et/ou d'incidents connus de sécurité et définissant les rôles du personnel, les mécanismes de signalement et les phases de la gestion et du traitement des incidents : • Confirmation des incidents : établissement d'un processus de confirmation des incidents, reposant sur diverses sources de données et intégré à travers toute l'entreprise, afin de confirmer efficacement un incident de sécurité (cette approche peut être adoptée lorsque le fournisseur a mis en place, dans l'environnement informatique, des mécanismes de détection et de surveillance à la fois efficaces et appropriés). • Classification des incidents : établissement d'un processus de classification des incidents, pour classer rapidement et efficacement les incidents confirmés selon différents types d'événements. • Signalement d'un incident : établissement de mécanismes appropriés visant à signaler l'incident (en fonction de la classification) aux parties prenantes appropriées, aux personnes responsables et, le cas échéant, à des spécialistes externes afin de réagir rapidement en cas d'incident. • Endiguement des incidents : utilisation du personnel, des processus et des technologies disponibles pour identifier rapidement et efficacement l'élément constitutif d'une attaque et contenir l'incident de sécurité dans l'environnement. • Résolution : utilisation du personnel, des processus et des technologies disponibles pour résoudre efficacement et rapidement une menace de sécurité et/ou ses composants se trouvant dans l'environnement. Une résolution efficace permettra, à l'avenir, de prévenir les attaques d'une nature similaire. Le fournisseur doit chercher à améliorer les réponses aux incidents lorsque cela est possible en intégrant les leçons tirées des mesures de détection/réponses actuelles et antérieures. Le fournisseur doit s'assurer que les équipes de réponse en cas d'incident et les processus pertinents en cas d'incident sont contrôlés au moins une fois par an, pour s'assurer de sa capacité à répondre aux incidents de cybersécurité identifiés. • Les simulations et les tests doivent démontrer que Barclays sera informé d'un incident de sécurité et de son impact à son encontre ; cette situation serait	rapide et à éviter l'aggravation des incidents.

	prouvée lorsque le fournisseur démontre l'aptitude à contacter les personnes compétentes en cas d'incident de cette nature. • Communication : le fournisseur doit nommer un contact pour les incidents de sécurité, lequel communiquera avec Barclays en cas d'incident. Le fournisseur doit communiquer à Barclays les coordonnées de ce contact, ainsi que tout changement le concernant, y compris son numéro de téléphone et les heures auxquelles il est joignable. Les informations suivantes doivent être incluses : Nom, responsabilités au sein de l'organisation, rôle, adresse e-mail et numéro de téléphone Le fournisseur informera Barclays (et devra, le cas échéant, veiller à ce que l'un de ses sous-traitants informe également Barclays) de tout incident qu'il découvre et qui affecte ou qui, d'après ses soupçons, pourrait affecter le service fourni à Barclays ou les informations/données de Barclays dans un délai raisonnable et, dans tous les cas, au plus tard deux (2) heures après le moment où le fournisseur découvre l'incident de sécurité. En présence d'une violation de données suspectée ou connue (incluant une atteinte à la sécurité se traduisant par une destruction, une perte ou une altération accidentelle ou illicite de données personnelles, par leur divulgation non autorisée ou par un accès non autorisé à ces dernières), le fournisseur doit informer Barclays de ces incidents dans un délai raisonnable courant dès leur découverte et, en tout état de cause, au plus tard dans les deux (2) heures suivant le moment où le fournisseur découvre l'incident en cause. En plus de la notification indiquée ci-dessus, le fournisseur transmettra à Barclays un rapport pour tout incident affectant le service fourni à Barclays ou les informations/données de Barclays, dans les vingt-quatre (24) heures suivant le moment où il le découvre,. Ce rapport doit inclure les informations suivantes : • La date et l'heure où le fournisseur a découvert l'incident de sécurité • Les territoires suspectés d'être touchés • Le type d'incident de sécurité et un bref résumé le décrivant • L'impact sur les services fournis à Barclays et/ou sur les informations et/ou données de Barclays (et, le cas échéant, les personnes concernées qui sont touchées), ainsi que les conséquences probables à leur égard • Le statut de l'incident de sécurité (par exemple, le recours à des experts scientifiques, la notification des autorités compétentes, la connaissance du	

	vecteur utilisé pour mener une attaque, la mise en place d'une surveillance approfondie, la prise de mesures d'endiguement) • La mesure prise ou envisagée pour résoudre l'incident de sécurité • Les précisions sur les données compromises Ces incidents, ainsi que toutes les mises à jours en cours relatives aux efforts de résolution et aux notifications à l'attention des personnes concernées, doivent être signalés au responsable des fournisseurs de Barclays ainsi qu'au centre d'opérations conjointes de Barclays (Joint Operations Centre, JOC) au sein du **bureau de la sécurité de Barclays (Chief Security Office, CSO) à l'adresse** gcsojoc@barclays.com. Veillez à ce que le sujet de l'e-mail soit le suivant « [Indiquez le nom du fournisseur] – Incidents de sécurité – A traiter en urgence » Si l'incident est très urgent et doit être signalé sur-le-champ, le JOC peut être joint grâce à sa ligne d'assistance, qui est ouverte 24 heures sur 24 et tous les jours de la semaine : • Royaume-Uni : +44 330 041 5586 • États-Unis : +1 201 499 1900 • Inde : +91 (788)22 310 781 9890	
7. Classification et protection des informations	Le fournisseur doit avoir établi un plan ou cadre de classification, de gestion et de stockage des informations approprié, conforme aux meilleures pratiques du secteur et/ou aux exigences de Barclays, et couvrant, de manière non limitative, les points suivants : • Examen continu des informations et/ou données de Barclays actuelles et nouvelles • Assignation du schéma correct d'étiquetage des informations aux informations/données de Barclays. • Gestion et stockage sécurisés des informations et/ou données de Barclays et, le cas échéant, conformément à la classification assignée. • Assurance que tout le personnel a connaissance des exigences relatives à l'étiquetage, au stockage et à la gestion du fournisseur et de Barclays, et de la manière d'appliquer la bonne classification des informations. Le fournisseur doit se reporter au schéma d'étiquetage des informations Barclays et aux exigences de gestion (annexe B, tableaux B1 et B2), ou à un autre programme convenu pour s'assurer qu'il protège et sécurise les informations de Barclays qu'il	Le non-respect de ces exigences peut se traduire par la modification, la divulgation ou l'accès non autorisé(e) aux données de Barclays, ou par des dommages, des pertes ou une destruction de telles données, pouvant entraîner un dommage relevant de la réglementation et une atteinte à la réputation.

	détient et/ou qu'il traite. Cette exigence s'applique à tous les actifs informationnels détenus ou traités au nom de Barclays.	
8. Gestion des actifs informatiques (matériels et logiciels)	Le fournisseur doit s'assurer qu'un programme de gestion des actifs efficace est en place pour toute la durée de vie des actifs. La gestion des actifs doit régir le cycle de vie des actifs, depuis leur acquisition jusqu'à leur mise au rebut, et fournir visibilité et sécurité pour toutes les classes d'actifs dans l'environnement. Le fournisseur doit tenir un inventaire précis et complet de tous les actifs critiques présents sur tous les sites et/ou pour tous les sites géographiques utilisés pour fournir des services à Barclays, y compris l'équipement Barclays hébergé sur les sites du fournisseur et/ou par un sous-traitant et fourni par Barclays. Le fournisseur doit vérifier cet inventaire des actifs au moins une fois par an pour s'assurer qu'il est à jour, complet et exact. Le processus de gestion des actifs doit au moins couvrir les éléments suivants : • Tous les actifs informationnels et de l'infrastructure sont schématisés et/ou mis à jour en permanence. • L'infrastructure et les actifs informationnels sont ensuite protégés conformément à leur classification, à leur criticité et à leur valeur pour l'entreprise. • Le fournisseur doit avoir mis en place des contrôles qui veillent à l'enregistrement et à la maintenance continue des données des actifs matériels pendant tout le cycle de vie des actifs. • Le fournisseur doit assurer la mise à jour de l'inventaire des actifs • **Les fournisseurs de niveaux 1, 2 et 3 doivent conserver des inventaires à jour, complets et précis des actifs (y compris l'ensemble des points d'extrémité, l'équipement réseau, les jetons RSA et/ou tout autre actif fourni par Barclays).** • **Le fournisseur doit effectuer le rapprochement de tous les actifs de Barclays (matériels & logiciels) chaque année et fournir une attestation à Barclays (Bureau de la sécurité, équipe ECAM).** • Les actifs non autorisés doivent être retirés du réseau ou mis en quarantaine, et l'inventaire doit être mis à jour en temps opportun. • Tenue à jour d'une liste de tous les logiciels autorisés requis pour fournir le service à Barclays. • Seuls les systèmes d'exploitation et applications logicielles actuellement pris en charge et mis à jour par le fournisseur doivent être ajoutés à l'inventaire des	L'existence d'un inventaire des actifs informationnels complet et précis est fondamentale pour assurer la mise en œuvre des contrôles appropriés. En cas de non-respect de ce principe, les actifs de Barclays ou les actifs utilisés par les fournisseurs pour fournir des services à Barclays pourraient être compromis, ce qui pourrait se traduire par des pertes financières, des pertes de données, une atteinte à la réputation et des sanctions réglementaires.

	logiciels autorisés de l'organisation. Les logiciels non pris en charge doivent être identifiés comme tels dans l'inventaire. Les logiciels arrivant en fin de vie doivent être également identifiés comme tels dans l'inventaire. Le fournisseur doit s'assurer que des procédures efficaces sont mises en place pour atténuer, en temps utile, les problèmes liés aux technologies non prises en charge, et à la fin de vie, au retrait et à la destruction d'actifs et de données, pour éliminer le risque de compromission des données.	
9. Suppression/Destruction des actifs physiques et rémanence des données venant des informations électroniques	La destruction ou l'effacement des actifs informationnels de Barclays, qui sont sauvegardés dans un format physique ou électronique, doit être opéré par des moyens sécurisés et adaptés au risque les accompagnant, en veillant à ce que les données de Barclays ne soient pas récupérables. Le fournisseur doit avoir mis en place des politiques et procédures efficaces pour évaluer continuellement les actifs informationnels de Barclays sauvegardés dans un format physique ou électronique, et déterminer le moment où leur destruction ou effacement est approprié et s'impose, que ce soit en vertu d'un contrat ou aux fins légales ou réglementaires de la sécurité des informations. Barclays peut également former une demande écrite pour solliciter la destruction des actifs informationnels de Barclays. Le fournisseur doit élaborer des procédures, et mettre en place les processus métier et mesures techniques s'y rapportant et qui sont engagés pour mettre au rebut de manière sécurisée et garantir la suppression et/ou l'effacement des données de Barclays (incluant ses copies de sauvegarde) de tous les supports de stockage, en s'assurant que les données ne peuvent pas être récupérées par des méthodes d'informatique légale. Les données de Barclays sauvegardées sur un support doivent être supprimées dans une mesure suffisante pour qu'elles ne puissent pas être récupérées et en ayant recours, de préférence, à des techniques appropriées d'effacement des données comme une suppression sécurisée, un nettoyage, un effacement de données, une destruction de données, ou à une méthode logicielle d'écrasement de données, ou encore en utilisant un cadre standard du secteur sur la suppression de données (NIST). Tout le matériel peut être éliminé au terme de sa durée de vie opérationnelle (matériel défaillant, mis hors service suite à une révision, retiré ou n'étant plus utile, utilisé pour un essai ou pour démontrer un concept, etc.). Des services de suppression de données peuvent être utilisés pour un équipement devant être réutilisé.	La destruction sécurisée des actifs informationnels aide à s'assurer que les actifs informationnels Barclays ne peuvent pas être récupérés pour toute violation de données ou perte ou activité malveillante.

	Les exigences d'élimination sont applicables à la quatrième partie et/ou aux agences en sous-traitance du fournisseur qui sont utilisées pour fournir le service à Barclays. Les informations en format papier (incluant les coordonnées des cartes de paiement) doivent être déchiquetées en respectant au moins la norme P4 DIN66399 et en utilisant une déchiqueteuse ou peuvent être incinérées conformément à la norme BS EN15713:2009. Pour Barclays, les preuves de l'élimination des données doivent être conservées, dans la mesure où elles constituent une piste d'audit et des preuves, et permettent d'assurer un suivi, et doivent inclure : • Des preuves de la destruction et/ou de l'élimination (incluant la date de l'opération et la méthode utilisée). • Les journaux d'audit du système à supprimer. • Les attestations de destruction des données. • L'identité des personnes ayant réalisé l'élimination (incluant les partenaires, les tiers ou les entrepreneurs chargé de l'élimination). • Un rapport de destruction et de vérification doit être généré pour confirmer la réussite ou l'échec d'un processus de destruction et/ou de suppression (par exemple, un processus d'écrasement doit s'accompagner d'un rapport donnant des précisions sur les éléments qui n'ont pas pu être supprimés). Au moment de la sortie, le fournisseur doit veiller, après avoir reçu une notification et une autorisation de Barclays, à ce que les données de Barclays soient détruites de manière sécurisée.	
10. Frontières et sécurité du réseau	**Le fournisseur doit s'assurer que l'ensemble des systèmes informatiques exploités par lui-même ou son sous-traitant et prenant en charge le ou les services fournis à Barclays soient protégés contre les menaces pesant sur le réseau du fournisseur (et celui des sous-traitants en cause) et pouvant entrer dans le réseau et en sortir.** Le fournisseur doit surveiller, détecter, prévenir et, si nécessaire, résoudre le flux d'informations transitant à travers des réseaux de différents niveaux de fiabilité, en se concentrant sur les atteintes à la sécurité. Les mécanismes d'intégrité du réseau doivent inclure, mais sans s'y limiter, les éléments suivants :	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.

	• 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, ainsi que les vulnérabilités potentielles et le besoin de retrait et de renouvellement de l'infrastructure du réseau, doivent être révisées au moins une fois par an ou si des exigences, motivées par un événement donné, entraînent des modifications. • Les connexions externes au réseau du fournisseur doivent être documentées, routées via un pare-feu, 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 exemple, segmentation du réseau, pare-feu, contrôle de l'accès physique à l'équipement réseau, etc.). • Le fournisseur doit utiliser des technologies de prévention des intrusions sur le réseau afin de détecter et d'empêcher tout trafic malveillant d'entrer sur le réseau. • Utilisation de pare-feu réseau puissants pour fournir une couche de protection en périphérie contre les attaques réseau malveillantes. • Tout le trafic du réseau Internet doit passer par un proxy configuré pour filtrer les connexions non autorisées. • La connexion et la surveillance doivent être activées. • La sécurité des périphériques réseau doit être renforcée pour empêcher toute attaque malveillante. • Une séparation logique des ports/interfaces de gestion des appareils du trafic utilisateur, ainsi que des contrôles d'authentification doivent être en place. • Toutes les règles de configuration qui autorisent un trafic à transiter par les périphériques réseau doivent être documentées dans un système de gestion de la configuration, accompagnées de la raison d'être précise de chaque règle. • La communication sur des ports TCP ou UDP non autorisés, ou le trafic d'applications non autorisées doivent être refusés, pour s'assurer que seuls les protocoles autorisés peuvent franchir les frontières du réseau de l'organisation. • Analyse régulière depuis l'extérieur de chaque frontière fiable du réseau, pour détecter toute connexion non autorisée accessible à travers la frontière. • Communications sécurisées entre les appareils et la console ou les stations de gestion. • Configuration des systèmes de surveillance pour enregistrer les paquets réseau traversant la frontière à chaque frontière réseau de l'organisation.	

	• 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). • Tout accès sans fil au réseau doit être protégé par des protocoles de chiffrement, de segmentation, d'authentification et d'autorisation, pour prévenir les violations de la sécurité. • Le fournisseur doit s'assurer que l'accès au réseau interne est surveillé et que seuls les appareils autorisés sont acceptés au moyen des contrôles d'accès au réseau appropriés. • L'accès de connexion à distance au réseau du fournisseur doit utiliser une authentification multifacteur. • Pour pouvoir fournir le ou les services à Barclays, le fournisseur doit disposer d'un réseau séparé. Le fournisseur doit s'assurer qu'aucun serveur utilisé pour fournir le service à Barclays n'est déployé sur des réseaux qui ne sont pas fiables (réseau en dehors du périmètre de sécurité ou hors du contrôle administratif du fournisseur, par exemple connecté à Internet) sans contrôles de sécurité appropriés. Le fournisseur hébergeant les informations de Barclays (et ses sous-traitants) 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. 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 sont établies uniquement avec le réseau de Barclays, et qu'elles ne sont 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.	

	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.	
11. Détection des dénis 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. 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 DoS adéquate pour garantir la disponibilité. Si le fournisseur héberge une application connectée à Internet et incluant des données restreintes ou servant de base à un service offrant une résistance de catégorie 0 ou 1, elle doit être soumise à une protection allant jusqu'à la couche 7 à l'aide de technologies appropriées qui doivent être approuvées par Barclays.	En cas de non-respect de ce principe, Barclays et ses fournisseurs pourraient être dans l'incapacité d'empêcher une attaque par déni de service d'atteindre l'objectif visé par son auteur.
12. Travail à distance (accès à distance)	Pour ce qui concerne l'accès à distance accordé au réseau de Barclays et opéré par des applications Citrix de Barclays et/ou des données de Barclays sauvegardées et/ou stockées dans des environnements et/ou sur des réseaux gérés par le fournisseur, si le fournisseur ou l'un de ses sous-traitants accèdent aux données de Barclays ou aux données personnelles ou informations sensibles de Barclays, qui sont fournies au fournisseur, dans un format physique ou virtuel, lorsqu'il a besoin d'en avoir connaissance et devant être accédées, partagées ou traitées à distance, notamment lorsque son personnel est susceptible de travailler à domicile, le fournisseur doit solliciter l'approbation de Barclays (Bureau de la sécurité, équipe ECAM) avant de prendre de tels arrangements. Par rapport à l'accès à distance, le fournisseur doit au moins s'assurer que les éléments suivants sont en place : • L'accès de connexion à distance au réseau du fournisseur doit être chiffré dans une mesure concernant les données en transit et toujours s'accompagner d'une authentification multifacteur. • L'accès au réseau Barclays doit se faire via l'application Citrix Barclays, avec jeton RSA (matériel et logiciel) fourni par Barclays. • Le fournisseur doit tenir un inventaire de tous les jetons RSA (matériels et logiciels) fournis par Barclays et mettre en place un processus de gestion incluant la vérification et la surveillance de l'allocation, de l'utilisation et du retour des jetons (jetons matériels).	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 tenir un registre des individus auxquels il a été demandé de travailler à distance, et les raisons de cette demande. • **Le fournisseur doit effectuer le rapprochement de tous les utilisateurs distants chaque trimestre et fournir une attestation à Barclays (Bureau de la sécurité, équipe ECAM).** • 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). • Le fournisseur doit s'assurer que le point d'extrémité utilisé pour se connecter à distance aux systèmes d'informations de Barclays est configuré de manière sécurisée et conformément aux meilleures pratiques du secteur (par exemple, niveau des correctifs, état de la protection contre les logiciels malveillants, solution Endpoint Detection & Response (EDR), connexion, 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 ECAM). Le fournisseur doit tenir un registre et effectuer un rapprochement chaque trimestre. • **Les appareils personnels et/ou de type « Apportez vos appareils personnels » ne doivent pas être autorisés à accéder à l'environnement Barclays et/ou aux données Barclays résidant et/ou stockées dans l'environnement géré par le fournisseur (ce qui inclut, de manière non limitative, le personnel du fournisseur, les consultants, le personnel de contingence, les entrepreneurs et les partenaires des services (MSP) gérés).** Lorsque l'accès des points d'extrémité (ordinateurs portables et/ou de bureau) est accordé au réseau Barclays à l'aide des applications Citrix Barclays utilisées 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 les vérifications réalisées par End Point Analysis se verront accorder un accès à distance au réseau de Barclays par 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 fournisseurs de Barclays. Remarque : Barclays désactivera les identifiants de connexion dès qu'il lui sera signalé qu'un accès n'est plus nécessaire (par exemple, fin de contrat d'un employé, réaffectation d'un projet, etc.) dans les **vingt-quatre (24) heures.**	

<table>
<tr>
<td>13. Gestion des journaux de sécurité</td>
<td>Le fournisseur doit s'assurer qu'il a été mis en place un cadre de gestion des journaux et d'audit confirmant que les systèmes et procédés informatiques clés, qui incluent les applications, l'équipement réseau, les banques de données, les points d'extrémité, les dispositifs de sécurité, l'infrastructure et les serveurs, créent les journaux s'imposant conformément aux consignes et aux meilleures pratiques du secteur. Ces journaux doivent être sécurisés de manière appropriée, détenus au niveau central, et conservés par le fournisseur pendant une durée minimale de 12 mois ou selon une base prévue par les catégories figurant ci-dessous et convenablement justifiée.
<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 processus de gestion des journaux de sécurité doit au moins couvrir les éléments suivants :

Le fournisseur doit établir des politiques et procédures pour la gestion des journaux.
Le fournisseur doit créer et gérer une infrastructure de gestion des journaux.
Le fournisseur doit définir les rôles et responsabilités des individus et équipes qui seront impliqués dans la gestion des journaux.
Les journaux d'audit des événements prévus pour aider à surveiller une attaque, à la détecter, à la comprendre et 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 autres éléments utiles.
Les exemples de journaux d'événements pourraient inclure ce qui suit :

Journaux des systèmes de détection des intrusions/protection contre les intrusions, des routeurs, pare-feu, proxy Web, logiciels d'accès à distance (VPN), serveurs d'authentification, applications, et base de données
Connexions réussies et échecs de connexion (par exemple, erreur d'identifiant utilisateur ou de mot de passe), création, modification et suppression de comptes utilisateur

</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>

	○ 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. • Analyse des journaux d'événements de sécurité (y compris la normalisation, l'agrégation et la corrélation). • Synchronisation des horodatages des journaux d'événements avec une source commune fiable. • Protection des journaux d'événements de sécurité (par exemple, chiffrement, MFA, contrôle d'accès et sauvegarde). • Application des mesures requises pour résoudre les problèmes identifiés et répondre aux incidents de cybersécurité rapidement et efficacement. • 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. • Déploiement d'outils tel que nécessaire 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. 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 matériels et/ou de violations des droits d'accès liés aux systèmes du fournisseur.	
14. 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.	Les solutions de lutte contre les logiciels malveillants sont cruciales pour la protection des actifs informationnels Barclays contre les codes malveillants.

	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 régulièrement son moteur d'analyse et sa base de données de signatures dans le respect des meilleures pratiques du secteur. • 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 place les contrôles appropriés afin de se protéger contre les logiciels malveillants pour mobile et les attaques perpétrées à l'encontre des appareils mobiles se connectant aux réseaux de Barclays ou du fournisseur et accédant aux données Barclays. • Les procédés doivent être en place pour que des réunions et/ou forums tenus régulièrement (selon une périodicité mensuelle) puissent discuter des vulnérabilités potentielles et/ou des mises à jour s'imposant. Les mesures de résolution doivent être priorisées et prises en temps utile. Les comptes-rendus des signalements, des forums et des mesures de résolution doivent être conservés. 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).	
15. Normes relatives à la configuration sécurisée	Le fournisseur doit établir un cadre visant à s'assurer que tous les équipements réseau et systèmes configurables sont configurés de manière sécurisée et conformément aux meilleures pratiques du secteur (par exemple, NIST, SANS et CIS). Le processus standard de configuration doit couvrir, mais sans s'y limiter, les éléments suivants : • Élaboration des politiques, des procédures et/ou mesures organisationnelles, et des outils permettant de mettre en œuvre les normes de configuration de la sécurité relevant des meilleures pratiques du secteur pour tous les appareils réseau, les systèmes d'exploitation, les applications et les serveurs autorisés.	Les contrôles relatifs aux normes applicables aux infrastructures aident à protéger les actifs informationnels contre tout accès non autorisé. Le respect des normes applicables aux infrastructures et les contrôles permettant de s'assurer que les changements sont autorisés aident

	• Vérifications régulières (tous les ans) de leur mise en œuvre, pour s'assurer que tout non-respect des normes de sécurité de base est rapidement corrigé. Vérifications et surveillance appropriées en place pour s'assurer que l'intégrité des infrastructures et des appareils est préservée. • Les systèmes et appareils réseau doivent être configurés de manière à fonctionner conformément aux principes de sécurité (par exemple, concept de limitation des contrôles des ports, des protocoles et des services, interdiction des logiciels non autorisés, enlèvement et désactivation des comptes utilisateurs inutiles, changement des mots de passe par défaut des comptes, suppression des logiciels inutiles, etc.). La gestion de la configuration doit régir les normes de configuration sécurisée pour toutes les classes d'actifs, et détecter, alerter et répondre efficacement aux modifications ou déviations de la configuration.	à protéger les actifs informationnels de Barclays.
16. Sécurité des points d'extrémité	Le fournisseur doit s'assurer que les 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 de la sécurité des points d'extrémité doit inclure, de manière non limitative, les éléments suivants : • Les disques doivent être chiffrés. • Tous les logiciels, services et ports inutiles doivent être désactivés. • Les droits d'accès d'administrateur pour l'utilisateur local doivent être désactivés. • Le personnel 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, etc. • Le port USB doit être désactivé, pour empêcher la copie des données Barclays sur des supports externes. • Les signatures antivirus et les correctifs de sécurité doivent être mis à jour. • La protection contre les pertes de données doit être limitée à l'interdiction du copier/couper/coller et des impressions d'écran des données Barclays. • Par défaut, l'accès à des imprimantes doit être désactivé. • 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	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.

	stocker des informations sur Internet (par exemple, Google Drive, Dropbox, iCloud, etc.). • Le partage et/ou le transfert des actifs informationnels et/ou données Barclays au moyen de logiciels et/ou d'outils de messagerie instantanée doivent être désactivés. • La capacité et les processus de détection de logiciels non autorisés identifiés comme malveillants, et la prévention de l'installation de logiciels non autorisés, doivent être assurés. 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 de l'entreprise, conformément aux normes de configuration approuvées de l'organisation. Tout système existant ou nouvellement déployé venant à être compromis doit être réinstallé en utilisant l'un des modèles ou l'une des images. 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 les vérifications réalisées par End Point Analysis se verront accorder un accès à distance au réseau de Barclays par 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 fournisseurs de Barclays. Appareils mobiles utilisés pour les services Barclays - 1. Le fournisseur doit implémenter 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 classifiées ou contenant de telles informations, afin de réduire le risque de compromission des données. 2. Le fournisseur doit veiller à mettre en place 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 des appareils. 3. Les données (Barclays) contenues dans les appareils mobiles doivent être chiffrées.	

17. Prévention des fuites de données	Le fournisseur doit mettre en place un cadre pour se protéger contre toute fuite de données inappropriée y compris, mais sans s'y limiter, via les canaux suivants :
	• Transfert non autorisé d'informations à l'extérieur du réseau interne et/ou du réseau du fournisseur
	  o E-mail
	  o Passerelle Web/Internet (y compris le stockage en ligne et les messageries électroniques sur le Web)
	  o 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 périphériques portables
	• Échange d'informations non sécurisé avec des tiers (4ème parties ou sous-traitants)
	• Impression ou copie inappropriée d'informations
		Des contrôles appropriés efficaces doivent être exécutés 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(e) 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

18. Sécurité des données	Le fournisseur doit s'assurer que les actifs informationnels et/ou données Barclays résidant sur le réseau du fournisseur ou dont ce dernier a la garde bénéficient d'une sécurité appropriée des données en combinant des techniques de chiffrement, des moyens sécurisés d'accès aux données, ainsi que des techniques de protection de l'intégrité et de prévention des pertes de données. Il est important de veiller à limiter convenablement l'accès aux actifs informationnels et/ou données Barclays, incluant les données personnelles, et à sécuriser ces accès. Les contrôles de sécurité des données doivent couvrir, mais sans s'y limiter, les éléments suivants : 1. A tout moment, le fournisseur est dans l'obligation de se plier à l'une et l'ensemble des lois applicables en matière de protection des données. 2. Des politiques et procédures doivent être établies, et les mesures techniques et processus métier et/ou mesures organisationnelles s'y rapportant mis en place, afin d'inventorier, de documenter et de gérer les flux de données résidant de manière permanente ou provisoire sur les applications (physiques et virtuelles) distribuées géographiquement, sur l'infrastructure et sur les composants systèmes du service, et/ou partagés avec des tiers.	

	3. Un inventaire de toutes les informations sensibles/confidentielles (actifs informationnels et/ou données Barclays) stockées, traitées ou transmises par le fournisseur doit être tenu. 4. Une norme de classification des données doit être élaborée pour que les informations sensibles (actifs informationnels et/ou données Barclays) puissent être classées et protégées correctement. 5. Toutes les données de Barclays doivent être classées et étiquetées conformément à la norme de classification et protection des informations. 6. Protection des données au repos ; a. Les données au repos doivent être au moins chiffrées, pour prévenir toute exploitation des informations sensibles via un accès non autorisé. 7. Surveillance de l'activité des bases de données ; a. L'accès aux bases de données et l'activité de celles-ci doivent être surveillés et enregistrés, afin d'identifier rapidement et efficacement toute activité malveillante. 8. Protection des données en cours d'utilisation ; a. La consultation et l'utilisation des informations sensibles doivent être contrôlées au moyen de dispositifs de gestion d'accès, pour prévenir l'exploitation des informations sensibles. b. Des technologies d'obscurcissement 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 des données en transit est généralement réalisé par 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 : • 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) • Tunnels sécurisés (IPsec) • Secure Shell (SSH)	

	c. Les protocoles de sécurité du transport doivent être configurés de manière à empêcher la négociation des algorithmes moins performants et/ou des clés plus courtes, lorsque les deux points d'extrémité prennent en charge l'option la plus performante. 10. Sauvegarde des données a. Des dispositions doivent être prises pour s'assurer que les informations sont dûment sauvegardées et récupérables (et pour qu'elles ne puissent pas être récupérées dans un délai raisonnable) conformément aux exigences convenues avec Barclays. b. Les sauvegardes doivent être correctement protégées par des dispositifs de sécurité physique ou des technologies de chiffrement lorsqu'elles sont stockées ou déplacées à travers le réseau. Cela inclut les sauvegardes à distance et les services cloud. c. Toutes les données Barclays doivent être sauvegardées régulièrement et automatiquement.	
19. 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 à l'appui du service fourni à Barclays, il doit mettre en place un cadre de développement sécurisé pour prévenir les violations de sécurité, et pour identifier et corriger les vulnérabilités que pourrait comporter le code lors du développement. La sécurité des logiciels d'application doit couvrir, d'une manière ne devant pas nécessairement être limitative, 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 conformes aux bonnes pratiques du secteur doivent être en place et adoptées, pour prévenir les vulnérabilités de sécurité et les interruptions de service, ce qui offre en même temps une protection contre les éventuelles vulnérabilités connues. • 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. • 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 données personnelles) ne seront 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 exemple, OWASP pour les applications Web). 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-feux 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 ne convient, un pare-feu pour applications Web basé sur l'hôte doit être déployé.	
20. Gestion de l'accès logique (LAM)	L'accès aux informations doit être soumis à restrictions, et en prenant dûment en considération les principes du besoin de connaître, du moindre privilège et de séparation des tâches. Le propriétaire des actifs informationnels est chargé de décider des personnes qui doivent accéder et de leur niveau d'accès. • Le principe du besoin de connaître veut que les personnes aient seulement accès aux informations qu'elles 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 veut que les personnes bénéficient seulement du niveau minimum de privilège nécessaire pour exécuter leurs tâches autorisées. Par exemple, si un employé a besoin de voir l'adresse d'un client mais ne sera 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 lecture/écriture. • Le principe de séparation des tâches veut qu'au moins deux personnes soient responsables de parties séparées de toute tâche afin de prévenir toute erreur et toute fraude. Par exemple, un employé qui demande la création d'un compte ne doit pas être celui qui approuve la demande. Le fournisseur doit s'assurer que l'accès aux informations personnelles est géré de façon appropriée et limité aux personnes qui en ont besoin pour fournir le service. La définition des processus de gestion de l'accès doit être conforme aux meilleures pratiques du secteur et inclure les éléments suivants : • Le fournisseur doit s'assurer que les processus et décisions de gestion de l'accès sont documentés et s'appliquent à tous les systèmes informatiques (qui stockent ou traitent des actifs informationnels Barclays), et, une fois mis en œuvre, ces processus doivent fournir des contrôles appropriés pour : Les nouveaux employés, les employés mutés, les employés quittant l'entreprise et l'accès à distance.	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.

	• Des contrôles doivent être en place à des fins d'autorisation, pour s'assurer que le processus d'octroi, de modification et de révocation d'un accès inclut un niveau d'autorisation proportionnel aux privilèges octroyés. • 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. • Chaque compte doit être associé à une seule personne, qui sera responsable de toute activité conduite en utilisant ce compte. • Recertification de l'accès : des contrôles doivent être en place pour s'assurer que les autorisations d'accès sont révisées au moins tous les 12 mois, afin de veiller à ce qu'elles soient adaptées aux buts visés. • Toutes les autorisations d'accès privilégié doivent être révisées au moins tous les six (6) mois, et des contrôles adéquats doivent être mis en œuvre pour les critères d'accès privilégié.	

	• Contrôles des employés mutés : accès modifié dans les 24 heures suivant la date de la mutation (des archives appropriées doivent être conservées) ; • Contrôles des employés quittant l'entreprise : l'intégralité de l'accès logique utilisé pour fournir des services à Barclays doit être supprimée dans les 24 heures suivant la date du départ (des archives appropriées doivent être conservées), • Accès à distance - des contrôles de l'accès à distance doivent être autorisés uniquement par le biais de mécanismes acceptés par Barclays (Bureau de la sécurité, équipe ECAM), et l'accès à distance doit utiliser une authentification multifacteur. • Authentification : les meilleures pratiques du secteur en matière de longueur et de complexité des mots de passe, de fréquence de changement des mots de passe, d'authentification multifacteur, de gestion sécurisée des identifiants de connexion et autres contrôles doivent être suivies. • Comptes inactifs - les comptes non utilisés depuis 60 jours consécutifs ou plus doivent être suspendus et/ou désactivés (et, le cas échéant, des archives doivent être conservées). • Les mots de passe des comptes interactifs doivent être modifiés au moins tous les 90 jours, et doivent être différents des douze (12) mots de passe utilisés précédemment. • Les comptes privilégiés doivent être modifiés après chaque utilisation, et au moins tous les 90 jours. • Les comptes interactifs doivent être désactivés après un maximum de cinq (5) tentatives d'accès infructueuses consécutives ou un nombre maximum inférieur, si les meilleures pratiques du secteur l'exigent.	
21. Gestion des vulnérabilités	Le fournisseur doit avoir établi des politiques et procédures, et mis en place les mesures techniques, les procédés et/ou les 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, 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.	En cas de non-mise en œuvre de ce contrôle, 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.

- Des outils et une infrastructure appropriés pour la détection des vulnérabilités doivent être en place.
- Des analyses des vulnérabilités doivent être conduites régulièrement (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.
- Un processus de validation de la correction des vulnérabilités doit être en place, pour vérifier rapidement et efficacement la correction des vulnérabilités sur toutes les classes d'actifs de l'environnement.
- 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 industrielles).
- Les résultats d'analyses consécutives des vulnérabilités doivent être comparés régulièrement afin de s'assurer que les vulnérabilités ont été corrigées en temps opportun.

Pour les services du fournisseur liés **aux applications et/ou à l'infrastructure d'hébergement** au nom de Barclays,

- 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 ECAM).

Priorité	Notation	Jours de fermeture (maximum)
P1	Critique	15
P2	Élevé	30
P3	Moyen	60

	<table><tr><td>P4</td><td>Faible</td><td>180</td></tr><tr><td>P5</td><td>Informationnelle</td><td>360</td></tr></table> Tous les problèmes de sécurité et vulnérabilités susceptibles d'avoir un impact substantiel sur l'infrastructure d'hébergement ou sur les applications Web 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 ECAM).	
22. Gestion des correctifs	Le fournisseur doit avoir établi des politiques et procédures, et mis en place les mesures techniques, les procédés commerciaux et/ou les mesures organisationnelles s'y rapportant, visant à surveiller et/ou assurer le suivi du besoin de correction et à utiliser des corrections sécuritaires pour gérer tout le patrimoine et/ou l'environnement du fournisseur. Le fournisseur doit veiller à ce que les correctifs de sécurité les plus récents soient appliqués aux systèmes, aux actifs, aux réseaux et aux applications en temps opportun, conformément aux meilleures pratiques du secteur, et en s'assurant des points suivants : • Le fournisseur doit tester tous les correctifs sur les 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 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 changements solide approuvé, afin de prévenir toute interruption de service ou violation de la sécurité. • Le fournisseur doit s'assurer que les correctifs sont appliqués dans les environnements de production et de reprise après incident (DR).	La non-mise en œuvre de ce contrôle peut se traduire par la fragilisation des services face aux problèmes de sécurité, entraînant ainsi un risque de compromission des données des consommateurs, de perte de service ou d'autres activités malveillantes.
23. Simulation de menaces / tests de pénétration /	Le fournisseur doit faire appel à un prestataire de services de sécurité qualifié indépendant pour réaliser une évaluation de la sécurité informatique/simulation de	En cas de non-mise en œuvre de ce contrôle, les fournisseurs pourraient être dans l'incapacité

<table>
<tr>
<td>évaluation de la sécurité informatique</td>
<td>menaces portant sur l'infrastructure informatique, y compris le site de reprise après incident et les applications Web liées aux services 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 susceptibles d'être exploitées pour 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 à l'application/infrastructure d'hébergement au nom de Barclays,

• Le fournisseur doit informer Barclays de la portée de l'évaluation de 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 Barclays et approuvés par celui-ci (Bureau de la sécurité, équipe ECAM).
• Une fois par an, le fournisseur doit partager avec Barclays (Bureau de la sécurité, équipe ECAM) le dernier rapport d'évaluation sur 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 ECAM).

<table>
<tr><th>Priorité</th><th>Notation</th><th>Jours de fermeture (maximum)</th></tr>
<tr><td>P1</td><td>Critique</td><td>15</td></tr>
<tr><td>P2</td><td>Élevé</td><td>30</td></tr>
<tr><td>P3</td><td>Moyen</td><td>60</td></tr>
<tr><td>P4</td><td>Faible</td><td>180</td></tr>
<tr><td>P5</td><td>Informationnelle</td><td>360</td></tr>
</table>
</td>
<td>d'évaluer les cybermenaces auxquelles il sont confrontés et la pertinence et la solidité de leurs moyens de défense.

Les informations de Barclays pourraient être divulguées et/ou une perte de service se produire, ce qui peut entraîner un dommage relevant de la réglementation ou une atteinte à la réputation</td>
</tr>
</table>

24. Cryptographie	• Raisons de la cryptographie : le fournisseur doit documenter les raisons pour lesquels 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. • 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. • 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 en place pour garantir l'intégrité, l'authenticité des clés, et la révocation et le renouvellement en temps opportun. • 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 frontières 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. o Dans des composants séparés, dans des groupes de dépositaires distincts.	L'existence d'une protection par chiffrement et d'algorithmes à jour et adaptés assure la protection ininterrompue des actifs informationnels de Barclays.

	○ Suppression des clés de la mémoire hôte pour la période de chiffrement, sauf si requis 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 division 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 un examen auditable des registres et conserver une preuve de cet examen pour tous les événements de gestion du cycle de vie des clés et des certificats, afin de démontrer la chaîne complète de responsabilités de 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. o 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 sont générées de façon indépendante 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 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).	
25. Informatique Cloud	Le fournisseur 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 sécuritaires visant à protéger les principaux concepts de confidentialité, d'intégrité, et de disponibilité, et à s'assurer que des contrôles sécuritaires sont 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 en cloud similaire ou des 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 par rapport aux meilleures pratiques du secteur, incluant les contrôles appropriés et équivalents à Cloud Controls Matrix (CCM), la dernière version de Cloud Security Alliance. Le fournisseur est tenu de s'assurer des contrôles de la sécurité des données concernant les actifs informationnels et/ou les données de Barclays, qui incluent les	Le non-respect de ce contrôle cloud risque de compromettre les données Barclays, ce qui peut se traduire par un dommage relevant de la réglementation ou une atteinte à la réputation.

	données personnelles du cloud, tandis que le prestataire de services cloud (CPS) est responsable de la sécurité du service cloud. 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 par rapport à tous les aspects du service fourni et incluant le modèle cloud de responsabilité partagée, afin d'en garantir la confidentialité, l'intégrité, la disponibilité et l'accessibilité, en réduisant les chances 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) • Cryptographie, chiffrement et gestion des clés - CEK • Consignation et surveillance • Virtualisation • Séparation des services Les actifs informationnels et/ou les données Barclays incluant les données personnelles et stockés dans le cloud dans le cadre du service fourni à Barclays doivent être approuvés par Barclays (Bureau de la sécurité, équipe ECAM). Lorsque des données sensibles (personnelles et restreintes) sont gardées par un prestataire de services cloud, le fournisseur doit indiquer à Barclays les emplacements, les zones de données et les zones de données de basculement où la garde de ces données sera assurée.	
26. 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 :	La non-mise en œuvre de ce contrôle peut se traduire par l'absence de contrôles physiques et techniques appropriés, et donc par des retards ou des interruptions des services, ou par des violations

	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.	de la cybersécurité et/ou des incidents de sécurité.
26.1 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.	
26.2 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. • 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 ou quittant 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 en place pour accéder à l'espace bancaire dédié, y compris : Pour le personnel autorisé : o Badge avec photo, visible en permanence o Pose de lecteurs de carte de proximité o Activation 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 tiers qui accèdent à l'espace bancaire dédié pour des activités de maintenance ou d'entretien ménager.	

26.3 Espace bancaire dédié – Vidéosurveillance	• Un système de vidéosurveillance doit être en place dans l'espace bancaire dédié pour détecter efficacement tout accès non autorisé 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. • 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.
26.4 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 multifacteur fourni par Barclays. • Le fournisseur doit tenir un registre des individus auxquels des jetons d'authentification Barclays ont été fournis et doit effectuer un rapprochement chaque trimestre. • Barclays désactivera les identifiants de connexion dès qu'il lui sera signalé qu'un accès n'est plus nécessaire (par exemple, fin de contrat d'un employé, ré-affectation d'un projet, etc.) dans les vingt-quatre (24) heures. • 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 ECAM). Le fournisseur doit tenir un registre et effectuer un rapprochement chaque trimestre. Voir le contrôle - 12 Travail à distance (accès à distance)
26.5 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 ECAM).
26.6 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 sont établies uniquement avec le réseau de Barclays, et qu'elles ne sont 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 - 10 Frontières et sécurité du réseau
26.7 Espace bancaire dédié – Réseau sans fil	Les réseaux sans fil doivent être désactivés pour le segment réseau Barclays pour fournir les services.
26.8 Espace bancaire dédié – Sécurité du point d'extrémité	Les architectures de postes de travail sécurisées 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 : • Les disques doivent être chiffrés. • Tous les logiciels, services et ports inutiles doivent être désactivés. • Les droits d'accès administrateur pour l'utilisateur local doivent être désactivés. • Le personnel du fournisseur ne doit pas être autorisé à modifier les réglages de base, comme le Service Pack par défaut, les services par défaut, etc. ; • Le port USB doit être désactivé, pour empêcher la copie des données Barclays sur des supports externes. • Les signatures antivirus et les correctifs de sécurité doivent être mis à jour. • La protection contre les pertes de données doit être limitée à l'interdiction du copier/couper/coller et aux outils d'impression d'écran et de capture d'impression des données Barclays ; • Par défaut, l'accès à des imprimantes doit être désactivé ; • Le partage et le transfert des données Barclays au moyen de logiciels ou d'outils de messagerie instantanée doivent être désactivés ; • La capacité et les processus de détection de logiciels non autorisés identifiés comme malveillants, et la prévention de l'installation de logiciels non autorisés, doivent être assurés. Voir le contrôle - 16 Sécurité des points d'extrémité
26.9 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 le stockage en ligne et les 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.	

26.10 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	Le fournisseur, à réception d'une notification écrite de Barclays adressée au moins dix (10) jours ouvrables à l'avance, 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 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. Le fournisseur doit 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 effectue une évaluation des risques et précise un délai de correction. Le fournisseur prend alors toutes les mesures correctives requises avant l'expiration de ce délai. Le fournisseur doit apporter toute aide raisonnablement demandée par Barclays en lien avec l'inspection, et la documentation soumise durant l'inspection doit être remplie et renvoyée à Barclays.	Si cela n'est pas convenu, les fournisseurs seront dans l'incapacité de présenter toutes les garanties de respect de ces obligations de sécurité.

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 qu'un membre du groupe du fournisseur ou que tout sous-traitant détient ou contrôle, 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.
ECAM	External Cyber Assurance and Monitoring (Surveillance et cyber-assurance externe) ; équipe qui évalue la position du fournisseur 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 sécurisée 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 qui présente 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 multifacteur (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).
Données 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 d'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.

Annexe B : Schéma d'étiquetage des informations Barclays

Tableau B1 : Schéma d'étiquetage des informations Barclays

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

	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.	• Documentation d'offre de nouvelle émission (par exemple, prospectus, notice d'offre) • Documents de recherche finaux • Informations importantes n'ayant pas été rendues publiques (IIPP) et n'appartenant pas à Barclays • Tous les rapports de recherche • Certains documents marketing • Analyses du marché • Rapports et résultats d'audit
Aucune restriction	Les informations doivent être classées « Aucune restriction » si elles sont destinées à une diffusion générale, ou si elles ne sont pas susceptibles d'avoir un impact négatif sur l'entreprise si elles étaient diffusées.	• Documents marketing • Publications • Annonces publiques • Offres d'emploi • Informations sans impact sur Barclays

Tableau B2 : Schéma d'étiquetage des informations Barclays – exigences de gestion

*** 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	Secrètes	Restreintes - internes	Restreintes - externes
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 où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. • Les actifs électroniques stockés doivent être protégés par chiffrement ou par des contrôles compensatoires appropriés s'il existe un risque significatif que des individus non autorisés puissent accéder à de tels actifs.	• Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones publiques (y compris les zones publiques au sein des locaux auxquelles les visiteurs peuvent accéder sans supervision). • Les informations ne doivent pas être conservées dans des zones publiques dans les locaux auxquelles les visiteurs peuvent accéder sans supervision.	• Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. • Les actifs électroniques stockés doivent être protégés par chiffrement ou par des contrôles compensatoires appropriés s'il existe un risque significatif que des individus non autorisés puissent accéder à de tels actifs.

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

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

Secret bancaire

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

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 d'en 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 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 sont traitées selon un plan correctif (action, propriété, date de livraison), et partagées et approuvées par la juridiction autorisant le secret bancaire correspondante. Une mesure de résolution 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 (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 C : 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 qui présente 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 D : 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 Barclays. Ceci ne doit pas être ambigu, ni sujet à interprétation, et peut comprendre des informations comme le prénom, le nom, le nom de la société, la signature, l'ID au sein du réseau social, 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 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			Confidentiel - Interne
Classification	DIC directes (DICD)	DIC indirectes (DICI)		
		Indirectes (N1)	Potentiellement indirectes (N2)	Identifiant impersonnel (N3)
Type d'informations	Nom du client	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	Fonctions	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 PEP	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, Royaume-Uni).

1. Nom du client

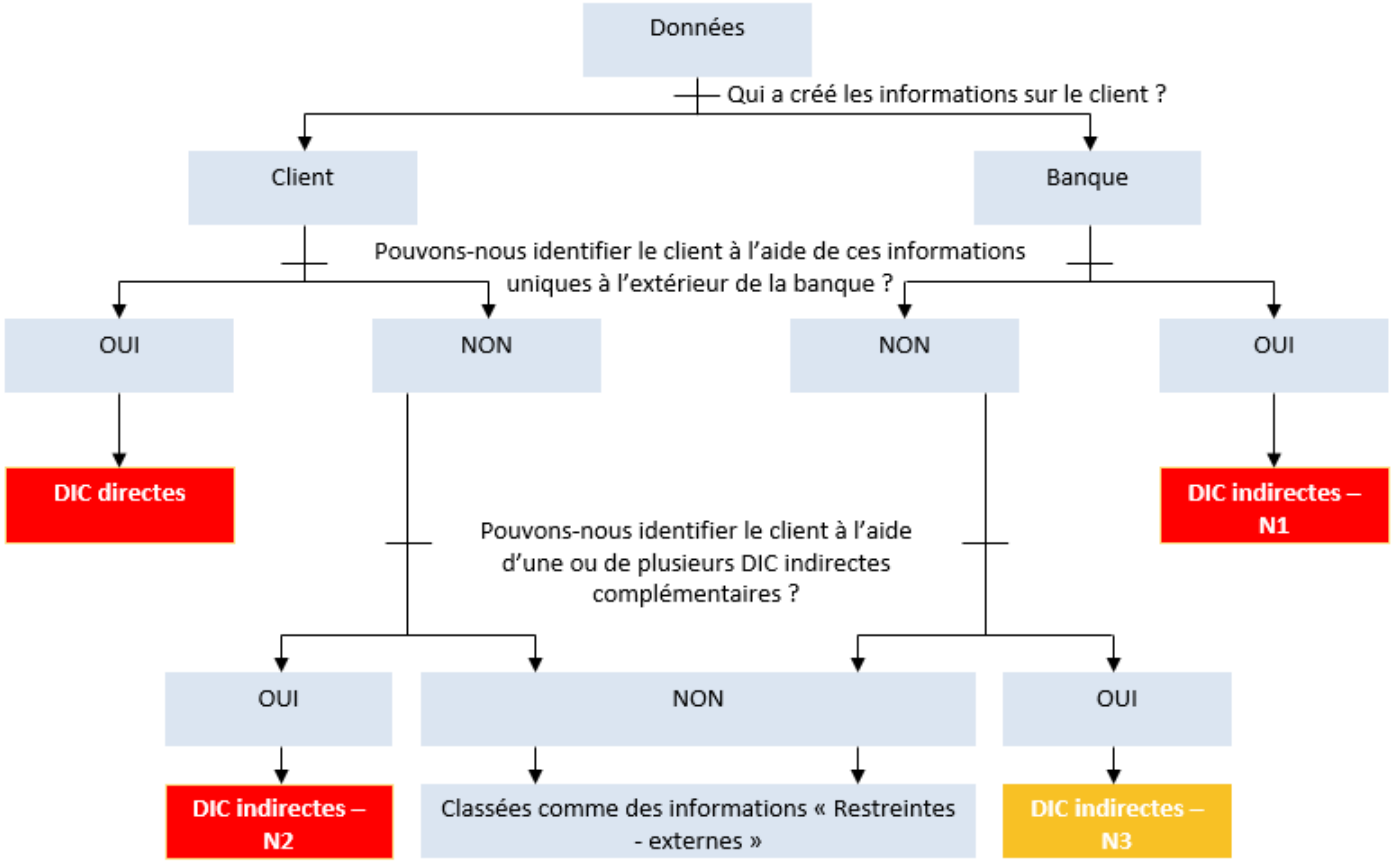
   (DICD) = violation du secret bancaire

2. ID conteneur

   (DICI N1) = violation du secret bancaire

3. Situation patrimoniale + nationalité

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


Données
Qui a créé les informations sur le client ?
Client
Banque
Pouvons-nous identifier le client à l'aide de ces informations uniques à l'extérieur de la banque ?
OUI
NON
NON
OUI
DIC directes
DIC indirectes – N1
Pouvons-nous identifier le client à l'aide d'une ou de plusieurs DIC indirectes complémentaires ?
OUI
NON
OUI
DIC indirectes – N2
Classées comme des informations « Restreintes - externes »
DIC indirectes – N3

Annexe E : Schéma d'étiquetage des informations Barclays

Tableau E1 : 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	• Informations sur les fusions ou acquisitions potentielles. • Informations sur la planification stratégique – commerciale et organisationnelle.

	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.	• Certaines informations relatives à la configuration de la sécurité des informations. • Certains rapports et résultats d'audit. • Comptes rendus du comité exécutif. • Coordonnées d'authentification ou d'identification et de vérification (ID&V) – client et collaborateur. • Grandes quantités d'informations sur les titulaires de cartes. • Prévisions de bénéfices ou résultats financiers annuels (avant publication officielle). • Tout élément couvert en vertu d'un accord de non-divulgation (AND) formel.
Restreintes - internes	Les informations doivent être classées « restreintes - internes » si les destinataires prévus sont uniquement des employés authentifiés Barclays et des prestataires de services gérés (PSG) Barclays avec un contrat actif en place et ces informations sont réservées à un public spécifique. Une divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de l'ERMF comme étant « majeur » ou « limité » (financier ou non-financier). Ces informations ne sont pas destinées à une diffusion générale mais peuvent être transmises ou partagées par des destinataires selon le principe du besoin de connaître.	• Stratégies et budgets. • Évaluations des performances. • Rémunération du personnel et données personnelles. • Évaluations de la vulnérabilité. • Rapports et résultats d'audit.
Restreintes - externes	Les informations doivent être classées « restreintes - externes » si les destinataires prévus sont des employés authentifiés Barclays et des PSG Barclays avec un contrat actif en place et ces informations sont réservées à un public spécifique ou à des parties externes qui sont autorisées par le propriétaire des informations.	• 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.

	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.	• Documentation d'offre de nouvelle émission (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 E2 : Schéma d'étiquetage des informations – exigences de gestion

** Les 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 « Restreintes - externes » et : • Un propriétaire des DIC doit être affecté aux actifs.

Stockage	Comme pour « Restreintes - externes » 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 être utilisés pour stockage uniquement 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 « Restreintes - externes » et : • Les actifs ne doivent pas être emportés / visualisés en dehors du site (locaux Barclays) sans l'autorisation formelle du propriétaire des DIC (ou son adjoint). • Les actifs ne doivent pas être emportés ni visualisés en dehors de la juridiction 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 « Restreintes - externes » 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 « Restreintes - externes »

*** 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	Restreintes - internes	Restreintes - externes	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 de 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 une étiquette 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 être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou 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 une étiquette d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page une étiquette d'information visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation. • Les actifs doivent être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou 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 se soit assuré que les destinataires sont 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 une étiquette d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page une étiquette d'information visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation. • Les actifs doivent être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. • Les actifs doivent être distribués uniquement aux individus spécialement autorisés par le propriétaire des actifs informationnels à les recevoir.

			• 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 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 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 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.