BARCLAYS

Obligations de contrôle pour les fournisseurs externes

Risque lié à la technologie

Version 11.0 - Octobre 2021

Domaine du contrôle	Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Gestion de l'obsolescence	Assurer l'application continue de modalités d'assistance	Le fournisseur doit informer promptement Barclays des changements dont il a connaissance concernant sa capacité à offrir une assistance, directe ou non, en relation avec les actifs informatiques utilisés dans le cadre de la prestation de services à Barclays, y compris lorsque des produits présentent des vulnérabilités de sécurité ; il doit en outre s'assurer de la mise à niveau ou de la suppression, en temps opportun, de ces actifs informatiques.	L'existence de registres et/ou de procédures inadaptés concernant des actifs informatiques matériels et logiciels ne bénéficiant plus d'aucune assistance ou des services liés à la technologie reposant sur un matériel informatique ou des logiciels obsolètes peut se traduire par un niveau de performance inacceptable, des problèmes d'instabilité, des vulnérabilités de la sécurité, une perte d'activité et des coûts de migration excessifs.
2. Traitement des incidents	Enregistrer, classer et résoudre les incidents	Le fournisseur doit mettre en œuvre un régime de traitement des incidents liés au fonctionnement de ses systèmes informatiques et à la prestation de ses services qui garantit que ces incidents opérationnels seront dûment identifiés, enregistrés, priorisés, classés et promptement résolus au premier contact ou au moyen d'une remontée de l'information rapide et appropriée. Ceci doit comprendre un processus robuste pour la gestion rapide et efficace des incidents majeurs.	Les incidents liés à la technologie qui ne sont pas signalés dans les délais prévus ou de manière suffisamment détaillée, ou qui ne sont pas suivis des mesures correctives nécessaires, peuvent se traduire par une perturbation des systèmes/du service qui aurait pu être évitée ou par une perte ou corruption de données. Les incidents majeurs exigent une réponse améliorée et urgente du fait qu'il s'agit d'incidents qui comportent un risque significatif pour l'entreprise et peuvent avoir de graves conséquences, y compris de graves interruptions de service, une atteinte à la réputation, un impact financier et un impact sur les processus cœurs de métier.
3. Gestion des problèmes	Identifier, évaluer/analyser et résoudre les problèmes liés à la technologie	Le fournisseur doit mettre en œuvre un régime d'examen en temps opportun des problèmes sous-jacents aux incidents liés à la technologie significatifs qui assure l'identification et l'enregistrement de ces problèmes au moyen d'une analyse des causes profondes ainsi que leur résolution effective en vue de réduire le risque que l'incident se reproduise et d'en atténuer l'impact s'il venait à se reproduire. Le fournisseur doit également s'assurer qu'une	Les problèmes sous-jacents à l'origine d'incidents ayant un impact sur la prestation de services liés à la technologie, lorsqu'ils ne sont pas identifiés et résolus en temps opportun, peuvent se traduire par une perturbation des systèmes/du service qui aurait pu être évitée ou par une perte ou corruption de données.

		analyse proactive des incidents périodiques est réalisée afin d'identifier et de résoudre la cause des incidents courants et fréquents.	
4. Gestion des changements	Appliquer un contrôle des changements rigoureux	Le fournisseur doit s'assurer que tous les composants informatiques utilisés dans le cadre de la prestation de services à Barclays sont gérés dans le cadre d'un régime de contrôle des changements rigoureux tenant pleinement compte des objectifs suivants : 1. Aucune modification sans autorisation appropriée - une approbation doit être donnée avant la mise en œuvre Il est établi une séparation des tâches entre la personne qui initie un changement, le propriétaire, celle qui l'approuve et celle qui le met en œuvre Les changements sont planifiés et gérés en fonction du niveau de risque associé 4. Il est tenu compte de manière adaptée de l'impact éventuel des changements sur la performance et/ou la capacité des composants technologiques concernés 5. Les changements font l'objet de tests techniques et professionnels pertinents avant la mise en œuvre et les éléments de preuve issus des tests sont conservés si exigé 6. Les changements doivent être testés après la mise en œuvre pour s'assurer qu'ils ont été exécutés avec succès sans impact imprévu	L'inadéquation des processus de changement pour prévenir tout changement non autorisé, inapproprié ou géré de manière inappropriée des services liés à la technologie peut se traduire par une perturbation du service, une corruption ou une perte des données, une erreur de traitement ou des actes de fraude.
5a. Résilience technologique	Plan de rétablissement des systèmes	Le fournisseur doit avoir mis en place des plans de rétablissement des systèmes pour chaque service/système technologique requis pour assurer la fourniture des services de catégorie de résilience Barclays 0 à 3, et respecter les délais de rétablissement visés (RTO) et points de rétablissement visés (RPO) correspondants. Ces plans doivent être révisés au moins tous les 12 mois pour s'assurer de leur exactitude. **Remarque :** Pour les services/systèmes	L'absence ou l'inadéquation des plans de rétablissement des systèmes peut se traduire par une perte inacceptable concernant les services liés à la technologie fournis à l'entreprise ou aux clients à la suite d'un incident. Une tenue à jour et une mise à l'épreuve de la documentation de résilience permettent de s'assurer que les plans de rétablissement restent alignés sur les besoins commerciaux.

		technologiques de catégorie de résilience 0 ou 1 conçus selon une configuration active/passive pour les mesures de résilience, la validation des plans de rétablissement des systèmes nécessite que le système concerné reste dans l'environnement rétabli pour une durée prolongée et fonctionne normalement, pour confirmer que tous les éléments fonctionnent correctement. Il s'agit-là d'un événement de croisement de production (PCO, Production Crossover).	
5b. Résilience technologique	Plan de rétablissement de l'intégrité des données	Le fournisseur doit avoir mis en place des plans de rétablissement de l'intégrité des données pour chaque service/système technologique requis pour assurer la fourniture des services de catégorie de résilience Barclays 0 à 1. Ces plans doivent être révisés au moins tous les 12 mois pour s'assurer de leur exactitude.	La perte de données est l'une des principales menaces auxquelles nous sommes confrontés, car celle-ci peut être due à un acte malveillant ou à une défaillance système. Il est essentiel de disposer d'un plan pour un tel scénario, car cela permet d'identifier et de comprendre les sources de données et leurs dépendances.
5c. Résilience technologique	Diversité des centres de données	Le fournisseur doit s'assurer que chaque service/système technologique requis pour assurer la fourniture des services de catégorie de résilience Barclays 0 à 3 est résilient entre les centres de données, et que ces derniers sont suffisamment éloignés les uns des autres pour réduire le risque que plusieurs centres de données soient affectés simultanément par un seul et même incident.	Les centres de données doivent être équipés de sources d'alimentation, de liaisons réseau, etc. secondaires. Ils doivent également être suffisamment éloignés les uns des autres pour réduire le risque que des centres de données soient affectés simultanément par le même événement.
5d. Résilience technologique	Validation des plans de rétablissement des systèmes	Le fournisseur doit tester et valider les plans de rétablissement des systèmes pour démontrer que les services/systèmes technologiques peuvent être rétablis pour	Les systèmes technologiques fournis par le fournisseur peuvent avoir une incidence sur l'expérience des clients de Barclays. Il est essentiel de s'assurer que les fournisseurs qui prennent en charge les opérations commerciales de Barclays disposent de plans de résilience adéquats testés, ainsi que d'un mandat de réglementation pour que Barclays

		répondre aux exigences de la catégorie de résilience 0 à 3 stipulées par Barclays. Pour chaque service/système technologique requis pour assurer la fourniture de services de catégorie de résilience 0 ou 1 conçus selon une configuration active/passive pour les mesures de résilience, l'environnement passif doit être activé conformément aux plans de rétablissement des systèmes documentés et utilisé comme environnement de production habituel, pour une durée suffisante pour démonter la capacité et l'intégration complète (croisement de production). Les exigences relatives à la fréquence de validation doivent être fonction de la catégorie de résilience associée, c'est-à-dire : - Catégorie de résilience 0 : les plans de rétablissement des systèmes doivent être validés tous les 12 mois et le croisement de production tous les 3 mois. - Catégorie de résilience 1 : les plans de rétablissement des systèmes et le croisement de production doivent être validés tous les 12 mois. - Catégories de résilience 2 et 3 : les plans de rétablissement des systèmes doivent être validés tous les 24 mois. Si un test ne satisfait pas aux exigences de rétablissement minimales de la catégorie de résilience applicable, le fournisseur doit notifier Barclays dans les plus brefs délais et soumettre des plans correctifs détaillés (incluant les mesures à prendre et les dates d'achèvement correspondantes). Le fournisseur doit notifier Barclays avant de procéder à un croisement de production.	puisse suivre les mesures de gouvernances correctes afin de gérer ses fournisseurs. Le croisement de production est une méthode qui permet de vérifier que l'instance passive d'un système configuré en actif/passif fonctionne correctement et que sa capacité correspond à celle attendue normalement. Le croisement de production permet également de s'assurer que toute dépendance à des systèmes en amont ou en aval continue de fonctionner tel qu'attendu.

5e. Résilience technologique	Validation des plans de rétablissement de l'intégrité des données	Le fournisseur doit tester et valider les plans de rétablissement de l'intégrité des données pour chaque service/système technologique requis pour assurer la fourniture des services de catégorie de résilience Barclays 0 à 1, afin de démontrer l'intégrité des données durant le rétablissement. Cette vérification doit être effectuée tous les 12 mois. Si un plan ne satisfait pas aux exigences de rétablissement minimales de la catégorie de résilience applicable, le fournisseur doit notifier Barclays dans les plus brefs délais et soumettre des plans correctifs détaillés (incluant les mesures à prendre et les dates d'achèvement correspondantes).	Les données constituent un élément critique qui peut subir toute sorte de préjudice. Le plan documenté pour rétablir, récupérer ou recréer des données doit être testé pour confirmer son exactitude et sa viabilité.
6. Gestion des performances et des capacités	Assurer la conformité constante aux besoins de Barclays en matière de technologie	Le fournisseur doit définir des niveaux de performance et de capacité adaptés pour tous les composants informatiques clés utilisés dans le cadre de la prestation de services à Barclays, conformément aux besoins commerciaux stipulés. Il doit également s'assurer que des alertes et des seuils appropriés sont en place sur les composants clés, pour signaler tout franchissement potentiel des seuils, et que ces derniers sont examinés régulièrement afin de s'assurer que la prestation de services est alignée sur les besoins de Barclays.	L'existence de mesures inadaptées pour surveiller les niveaux de performance et/ou de capacité des ressources informatiques et la non-préservation de leur conformité aux exigences applicables à ce jour ou à l'avenir peut se traduire par une réduction et/ou interruption inacceptable des services liés à la technologie et par une perte d'activité. L'existence de définitions et/ou de documents inadaptés concernant les besoins de l'activité/des clients peut se traduire par un niveau de performance des services liés à la technologie inacceptable et par une perte d'activité.

Domaine du contrôle	Intitulé du contrôle	Description du contrôle	Raisons de l'importance
7. Développement d'applications technologiques	Appliquer une assurance de la qualité répétable	Le fournisseur doit s'assurer qu'il peut être démontré que l'ensemble des systèmes informatiques et services utilisés dans le cadre de la prestation de services auprès de Barclays ont fait l'objet de processus d'assurance de la qualité rigoureux, approfondis, et répétables, y	Des systèmes et services dont la qualité n'a pas été dûment testée et assurée peuvent entraîner une perte critique et imprévisible de la fonctionnalité des services technologiques et des processus d'entreprise.

		compris mais sans y être limité, des tests fonctionnels et non-fonctionnels, des tests de la sécurité statique des applications, et une assurance de la qualité des codes au moyen d'un examen par les pairs ou d'outils automatisés.	
	Acceptation des résultats opérationnels	Le fournisseur doit convenir sur une base ponctuelle ou continue de définitions mutuellement acceptables des résultats opérationnels selon lesquelles de nouvelles versions ou des versions à jour de systèmes informatiques et services sont fournies à et acceptées par Barclays. La formulation de ces définitions doit comprendre des aspects fonctionnels et non-fonctionnels suffisants des systèmes et services, et peut se présenter sous toute forme appropriée mutuellement convenue comme des manuels des systèmes existants, une documentation détaillée des exigences mutuellement convenues, des témoignages d'utilisateurs, des cas d'utilisation ou toute autre forme appropriée. Le fournisseur doit collaborer avec Barclays pour s'assurer que les résultats opérationnels en totalité ou en partie mutuellement convenue sont acceptés sur une base ponctuelle ou continue d'après l'acceptation de l'entreprise Barclays de ces définitions préalablement convenues.	Un accord inadéquat quant au comportement fonctionnel et non-fonctionnel des systèmes peut entraîner une différence par rapport au comportement des systèmes attendu par Barclays, générant un risque pour les processus d'entreprise et opérationnels.
8. Modalités concernant la sauvegarde des systèmes et des données	Mettre en œuvre des processus de sauvegarde et restauration appropriés et efficaces	Le fournisseur doit s'assurer que des processus de sauvegarde et restauration appropriés de tous les services et systèmes informatiques utilisés dans le cadre de la prestation de services à Barclays, appliqués en conformité avec les besoins de Barclays et dont l'efficacité est périodiquement démontrée, ont été mis en place.	L'absence de sauvegarde des données de l'entreprise, ou l'existence de sauvegardes insuffisamment contrôlées, peut se traduire par une perturbation des systèmes/du service, une perte de données ou la divulgation inappropriée de données.

	Assurer l'utilisation de supports de sauvegarde sûrs et fiables	Le fournisseur doit s'assurer que tous les supports de sauvegarde associés à la prestation de services à Barclays, ainsi que les modalités de traitement et de stockage de ces supports, conservent à tout moment un caractère sûr et fiable.	L'absence de sauvegarde des données de l'entreprise, ou l'existence de sauvegardes insuffisamment contrôlées, peut se traduire par une perturbation des systèmes/du service, une perte de données ou la divulgation inappropriée de données.
9. Gestion de la configuration	Isoler l'environnement de production	Le fournisseur doit s'assurer que les services de production fournis à Barclays ne dépendent d'aucun composant hors production afin de garantir une prestation de services sécurisée et fiable.	L'existence d'entrées de registre inappropriées concernant des composants technologiques (matériel informatique et logiciels), y compris la propriété et le recours à des composants de tiers, peut se traduire par un défaut de sécurité ou de fiabilité de services et de données. L'utilisation de composants hors production dans le cadre de la prestation de services de production génère un risque au sens où ils peuvent ne pas être conformes à ou gérés par des normes de production.
	Consignation et administration des informations de configuration	Le fournisseur doit tenir des registres complets et exacts pour définir l'ensemble des éléments de configuration relevant du champ d'application utilisés dans le cadre de la prestation de services auprès de Barclays (y compris propriété et dépendances/mappages en amont/aval). Le fournisseur doit mettre en place des contrôles permettant de s'assurer que l'exactitude et l'exhaustivité des données sont préservées.	Des entrées de registre inappropriées ou incomplètes (ainsi que les dépendances/mappages apparenté(e)s à d'autres éléments de configuration) peuvent se traduire par des services et des données non sécurisés ou instables en raison d'une évaluation inefficace de l'impact d'incidents et de changements.
10. Gestion des actifs informatiques matériels	Consignation et administration des informations relatives aux actifs informatiques matériels	Le fournisseur doit mettre en place des contrôles permettant d'assurer l'archivage et la préservation continue des données relatives aux actifs matériels tout au long du cycle de vie des actifs. Le fournisseur doit tenir des registres complets et exacts pour l'ensemble des actifs informatiques matériels utilisés dans le cadre de la fourniture des services à Barclays.	L'existence d'entrées de registre inappropriées concernant des actifs informatiques matériels technologiques, y compris la propriété et le recours à des composants de tiers, peut se traduire par un défaut de sécurité ou de fiabilité de services et de données. Si des actifs informatiques matériels ne sont pas nettoyés et mis au rebut de manière sécurisée, un préjudice financier, une atteinte à la réputation et une infraction à la réglementation peuvent survenir.

	Mise au rebut des actifs	Tous les actifs mis au rebut doivent être entièrement débarrassés de l'ensemble des données Barclays et mis au rebut de manière sécurisée selon un processus formel de mise au rebut, aligné sur les exigences des normes de sécurité Barclays pertinentes.	Il est essentiel que le fournisseur obtienne et consigne la confirmation officielle que les actifs ont été mis au rebut correctement (y compris la destruction sécurisée des données bancaires). Si des actifs informatiques matériels ne sont pas nettoyés et mis au rebut de manière sécurisée, un préjudice financier, une atteinte à la réputation et une infraction à la réglementation peuvent survenir.
	Actifs manquants	Une enquête doit être correctement menée en cas de perte ou de vol d'actifs. Les actifs perdus ou volés qui ne sont pas retrouvés doivent être signalés à Barclays pour contresignature du risque.	Il est essentiel que le fournisseur mette en place des contrôles pour s'assurer qu'une enquête minutieuse a été menée pour retrouver les actifs manquants et que, s'ils ne sont pas retrouvés, ces actifs soient signalés à Barclays pour contresignature du risque. Si des actifs informatiques matériels ne sont pas nettoyés et mis au rebut de manière sécurisée suite à leur perte, cela peut entraîner un préjudice financier, une atteinte à la réputation et une infraction à la réglementation.
Domaine du contrôle	**Intitulé du contrôle**	**Description du contrôle**	**Raisons de l'importance**
11. Gestion des actifs informatiques logiciels	Consignation et administration des informations relatives aux actifs informatiques logiciels/installations. Octroi de licences pour les actifs informatiques logiciels	Le fournisseur doit tenir des registres complets et exacts pour définir l'ensemble des actifs informatiques logiciels relevant du champ d'application et des installations de ces derniers utilisés dans le cadre de la prestation de services auprès de Barclays (y compris propriété). Le fournisseur doit s'assurer de l'exactitude et du caractère exhaustif des données, de l'achat à la mise au rebut (et de l'installation à la désinstallation). Le fournisseur doit également s'assurer que l'utilisation de logiciels reste conforme aux conditions de la licence définie.	La présence d'entrées de registre inappropriées concernant des actifs logiciels technologiques, y compris la propriété définie, peut se traduire par un défaut de sécurité ou de fiabilité de services et de données. Si l'utilisation des logiciels n'est pas gérée conformément aux droits d'utilisation, un préjudice financier, une atteinte à la réputation et une infraction à la réglementation peuvent survenir.

Définitions liées à la résilience technologique :

Délai de rétablissement visé	Désigne le temps écoulé entre une défaillance ou une interruption imprévue des services et la reprise des activités.
Point de rétablissement visé	Désigne le statut visé de disponibilité des données au début du processus de rétablissement. Il s'agit d'une mesure de la perte de données maximale tolérable en situation de rétablissement.
Croisement de production	Désigne l'activation d'une instance alternative (reprise après sinistre) pour les systèmes conçus selon une configuration active/passive et l'utilisation de cette instance comme instance production pendant une période suffisamment longue pour valider le fonctionnement de toutes ses capacités et fonctionnalités.
Plan de rétablissement des systèmes	Document définissant les éléments et informations techniques relatives au rétablissement d'un système ou de tout composant qui échoue à retrouver un état opérationnel.
Plan de rétablissement de l'intégrité des données	Document décrivant les étapes à suivre pour récupérer les données perdues suite à une défaillance d'un système ou à un acte malveillant. Le plan doit couvrir divers scénarios avec les options pertinentes (par exemple, lecture des données depuis d'autres systèmes, rétablissement des données à partir de bandes archivées ou recréation des données).

Exigences de résilience Barclays par catégorie de résilience

Catégorie de résilience	0	1	2	3
Délai de rétablissement visé	jusqu'à 5 minutes	jusqu'à 4 heures	jusqu'à 12 heures	jusqu'à 24 heures
Point de rétablissement visé	jusqu'à 5 minutes	jusqu'à 15 minutes	jusqu'à 30 minutes	jusqu'à 24 heures