Obligations de contrôle pour les fournisseurs externes

Plan de rétablissement

Version 13.0 – Septembre 2023

1. Définitions :

« Événement perturbateur »	Un registre des impacts d'Incidents, qu'elle qu'en soit la cause, que les Fournisseurs ont choisi d'atténuer par la mise en œuvre de la planification et des capacités de rétablissement et de résilience.
« **Incident** »	Désigne une perturbation qui peut être gérée dans le cadre des activités quotidiennes, en déclenchant des plans de rétablissement.
« Plan de rétablissement »	Les Plans de rétablissement sont des documents qui décrivent en détail les étapes et les actions à entreprendre pour rétablir l'état opérationnel d'un service. Il peut s'agir d'un Plan de rétablissement de l'activité ou de termes similaires.
« **Planification du rétablissement** »	Le processus ou la planification du rétablissement des services d'entreprise, des processus d'entreprise et des dépendances sous-jacentes
« **Délai de rétablissement visé** »	Désigne le temps écoulé entre une défaillance ou une interruption imprévue des services et la reprise des activités.
« Catégorie de résilience »	La Catégorie de résilience est une évaluation qu'utilise Barclays pour appliquer les exigences de résilience à un service. La catégorie de résilience détermine le délai de rétablissement visé (RTO), le point de rétablissement visé (RPO) et les exigences relatives à la fréquence de validation.

2. Matrice de criticité en matière de résilience :

Barclays attribue une Catégorie de résilience spécifique (0-4) aux services du fournisseur, qui reflète l'impact qu'une interruption du service pourrait avoir sur Barclays. Une Catégorie de résilience plus élevée (à savoir, désignée par un chiffre de valeur moindre) devra répondre à une norme de résilience ou de rétablissement plus stricte, proportionnelle à l'importance des services. Le Fournisseur s'assurera que ses services respectent le Délai de rétablissement visé (RTO) et le Point de rétablissement visé (RPO) spécifiés ci-dessous pour la Catégorie de résilience applicable stipulée par Barclays pour les services demandés. Le tableau suivant indique les contrôles fournisseurs applicables en fonction de la Catégorie de résilience définie. Ces contrôles sont détaillés à la section 3 (*Contrôle*) ci-dessous.

Évaluation de l'impact des risques	Impact exceptionnel	Impact élevé	Impact modéré	Impact faible	Impact insignifiant
Catégorie de résilience	0	1	2	3	4
Objectif RTO	Jusqu'à 1 heure	Jusqu'à 4 heures	Jusqu'à 12 heures	Jusqu'à 24 heures	Pas de rétablissement
Objectif RPO	Jusqu'à 5 minutes	jusqu'à 15 minutes	jusqu'à 30 minutes	Jusqu'à 24 heures	Pas de rétablissement

Fréquence des tests technologiques	Catégorie de résilience 0	Catégorie de résilience 1	Catégorie de résilience 2	Catégorie de résilience 3	Catégorie de résilience 4
Validation des plans de rétablissement des systèmes	Deux fois par an min.	Deux fois par an min.	Tous les 12 mois min.	Tous les 24 mois min.	Pas de rétablissement planifié
Validation des plans de rétablissement des données	Validation annuelle du plan dans un environnement de type production	Validation annuelle via une démonstration du bureau	Facultatif	Facultatif	Pas de rétablissement planifié
Validation du plan de reconstruction de la plateforme et des applications	Validation annuelle via une démonstration du bureau	Validation annuelle via une démonstration du bureau	Facultatif	Facultatif	Pas de rétablissement planifié

Applicabilité des contrôles pour les fournisseurs	Catégorie de résilience 0	Catégorie de résilience 1	Catégorie de résilience 2	Catégorie de résilience 3	Catégorie de résilience 4
1. Exigences de cartographie des dépendances à inclure dans le Plan de rétablissement	✓	✓	✓	✓	O
2. Événements perturbateurs pour les exigences de Planification du rétablissement	✓	✓	✓	✓	O
3. Exigences de validation et de planification du rétablissement	✓	✓	✓	✓	O
4. Exigences de test intégré	✓	✓	O	O	O
5. Exigences de validation et des plans de rétablissement des systèmes	✓	✓	✓	✓	O
6. Exigences de validation et des plans de rétablissement des données	✓	✓	O	O	O
7. Exigences en matière de diversité des centres de données et des fournisseurs de services cloud	✓	✓	✓	✓	O
8. Exigences des plans de reconstruction de la plateforme et des applications	✓	✓	O	O	O

✓ = obligatoire	O = facultatif

Si des problèmes sont identifiés lors de l'examen ou si les exigences ne sont pas respectées lors du test des contrôles, le fournisseur doit en informer Barclays rapidement (généralement sous 10 jours) et résoudre les problèmes à une date convenue.

3. Contrôles :

Le fournisseur doit adopter une approche structurée de la résilience (continuité des activités et reprise après sinistre), étayée par une politique et des normes qui régissent les exigences de résilience opérationnelle et technique conformément aux meilleures pratiques du secteur et aux exigences réglementaires applicables. L'approche structurée de la résilience doit être supervisée par la direction et examinée et testée chaque année pour vérifier son efficacité.

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Exigences de cartographie des dépendances à inclure dans le Plan de rétablissement	Le Fournisseur doit définir et documenter les dépendances essentielles pour fournir le service à Barclays. Ces dépendances doivent être entretenues et examinées tous les 12 mois ou en cas de changement important. Les dépendances à prendre en compte sont les suivantes : ▪ Technologie et données (fournies en interne et par le sous-traitant) ▪ Sous-traitant(s) important(s) (qui pourraient avoir un impact important sur l'exécution et la fourniture des services à Barclays). ▪ Main-d'œuvre (perte de personnes ; envisager l'absence de stratégie de récupération des zones de travail ou de possibilité de travail à domicile)	Les prestataires de services doivent comprendre les dépendances pour fournir leurs services à Barclays. Toutes les dépendances feront partie de leur Plan de rétablissement de l'activité pour s'assurer qu'elles sont prises en compte afin d'atténuer l'impact des incidents et d'empêcher l'indisponibilité du service pour Barclays.
2. Événements perturbateurs pour les exigences de Planification du rétablissement	Le Fournisseur doit définir les événements perturbateurs à planifier et le niveau de planification du rétablissement requis pour s'assurer que les services peuvent être fournis dans le respect des niveaux de service convenus et des objectifs correspondants en matière de Délai de rétablissement visé. Le fournisseur doit s'assurer que ces événements perturbateurs reflètent le paysage actuel des risques/menaces, qu'ils sont évalués en termes de gravité et de plausibilité, et qu'ils sont étayés par des informations sur l'industrie et des données en temps réel. Le fournisseur doit, au minimum, inclure les événements perturbateurs suivants dans le cadre de sa planification. ▪ Perte d'un ou plusieurs bâtiments sur plusieurs sites ayant un impact sur la prestation de services à Barclays. (Les bâtiments et l'infrastructure associée ne sont pas disponibles). ▪ Scénario de perte de données, notamment les cyber-événements et l'impact potentiel sur la prestation de services fournie à Barclays.	Barclays a l'obligation commerciale (et fondée sur les risques) d'éviter les Événements perturbateurs significatifs et/ou d'être en mesure de s'en remettre en temps voulu, c'est-à-dire d'être suffisamment résiliente. Barclays doit être assurée et doit être en mesure d'assurer à ses parties prenantes qu'en cas de perturbations, le service est conçu de manière à réduire leur impact à un minimum (qu'il s'agisse d'un impact pour les clients, financier et/ou sur la réputation).

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
	▪ Perte de ressources humaines qui aurait un impact sur la prestation des niveaux de service convenus (par ex. une pandémie, un événement géopolitique, une défaillance critique de l'infrastructure nationale, etc.). ▪ Perte de services technologiques (par ex. perte de centres de données ou région du fournisseur de services cloud). ▪ Perte de sous-traitant matériel (services ou fournitures). Les Événements perturbateurs doivent être examinés chaque année et de manière continue, afin d'informer la planification et les tests et de démontrer comment ils évoluent au fil du temps.	
3. Exigences de validation et de planification du rétablissement	Le Fournisseur doit mettre en place des Plans de rétablissement pour ses Événements perturbateurs convenus. Les Plans de rétablissement doivent documenter les étapes détaillées du rétablissement et la réponse du Fournisseur qui est possible pour atténuer l'impact et/ou différer l'indisponibilité des services fournis à Barclays. Au minimum, il convient de tenir compte des éléments suivants : ▪ Solutions de contournement possibles ▪ Protocoles de décision ▪ Communication et priorisation des activités pour reprendre/maintenir un service minimum viable ▪ Dépendances Les Plans de rétablissement doivent être testés et validés tous les 12 mois, ou à chaque changement significatif, pour démontrer que les niveaux de service convenus peuvent être fournis et que les services répondent aux exigences de la Catégorie de résilience stipulées par Barclays. Si un plan ne répond pas aux niveaux de service convenus ou aux exigences de la Catégorie de résilience applicables, le Fournisseur doit notifier Barclays dans les plus brefs délais (généralement sous 10 jours) et soumettre des plans correctifs détaillés (comprenant les mesures à prendre et les dates d'achèvement correspondantes).	Les tests et la validation sont exécutés pour garantir à Barclays que le plan et la conception du service fonctionnent comme prévu, qu'ils incluent toutes les dépendances et démontrent que les niveaux de service convenus peuvent être assurés, et que les services répondent aux exigences de résilience stipulées par Barclays.

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
4. Exigences de test intégré	Afin de s'assurer que les interdépendances entre Barclays et les services du fournisseur sont comprises dans le cadre du rétablissement des services, le fournisseur, à la demande de Barclays et à une date convenue d'un commun accord, doit participer à un test intégré pour valider la résilience/continuité collective du fournisseur et de Barclays. Barclays ne soumettra pas cette demande plus d'une fois tous les deux ans, sauf si des tests intégrés précédents ont révélé des déficiences importantes ou si un incident provoque une interruption des services.	Ces exercices conjoints aident à s'assurer que les protocoles adéquats de Plan de rétablissement sont en place, que des stratégies de communication efficaces sont adoptées, et que le Fournisseur et Barclays répondent de manière coordonnée pour gérer les interruptions d'activité et réduire à minimum l'impact sur les clients de Barclays et le système financier dans son ensemble.
5. Exigences de validation et des plans de rétablissement des systèmes	Le fournisseur doit disposer d'un Plan de rétablissement des systèmes détaillant les actions requises pour rétablir l'état opérationnel des systèmes après une interruption. Les plans doivent être testés et validés pour démontrer (avec des preuves) que le système peut être rétabli conformément au Délai de rétablissement visé et au Point de rétablissement visé définis, tel que requis par la Catégorie de résilience définie. Pour les systèmes à configuration active/passive, l'environnement passif doit être activé et utilisé comme environnement de production normal pendant une durée suffisante pour démontrer la capacité et la fonctionnalité d'intégration complète. Pour les services à configuration active/active, la validation doit prouver la continuité des opérations avec la perte d'un nœud, d'une instance ou d'une zone de disponibilité (pour les services hébergés dans le cloud) du système (au moins 60 minutes). Les exigences de fréquence de validation sont définies par la Catégorie de résilience du système. Reportez-vous à la matrice de criticité en matière résilience ci-dessus	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 Barclays ou ses clients à la suite d'un Incident. La tenue à jour et la mise à l'épreuve de la documentation de résilience permettent de s'assurer que les plans de rétablissement restent alignés sur les besoins commerciaux.
6. Exigences de validation et des plans de rétablissement des données	Le fournisseur doit avoir mis en place un ou plusieurs Plans de rétablissement des données pour chaque système technologique requis, pour assurer la fourniture des services à Barclays. Ce ou ces plans doivent être révisés au moins une fois tous les 12 mois, ou à chaque changement significatif, pour s'assurer de leur exactitude, et doivent tenir compte au minimum des éléments suivants : ▪ Sources et flux de données (en amont et en aval) ▪ Sources de sauvegarde et de réplication ▪ Exigences de synchronisation des données après la restauration	La perte de données est l'une des principales menaces auxquelles Barclays est confrontée. Elle peut résulter d'actes malveillants ou d'une défaillance du 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.

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
	Le fournisseur doit tester et valider le(s) Plan(s) de rétablissement des données pour chaque système technologique requis pour assurer les prestations de service auprès de Barclays et démontrer (avec des preuves) la capacité du processus de rétablissement à rétablir les données dans l'état opérationnel prévu et au Point de rétablissement requis.	
7. Exigences en matière de diversité des centres de données et des fournisseurs de services cloud	Le Fournisseur doit s'assurer que chaque système technologique requis pour assurer la fourniture des services est résilient entre les centres de données, et que ces derniers sont suffisamment éloignés géographiquement les uns des autres pour réduire le risque que plusieurs centres de données soient affectés simultanément par un seul et même incident. Lorsque le système technologique est hébergé sur un fournisseur de services cloud, le service doit être disponible dans différentes zones de disponibilité afin d'éviter une panne de la zone de disponibilité. Les systèmes critiques doivent démontrer la capacité à effectuer un rétablissement après une défaillance d'une région du fournisseur de services cloud.	Les systèmes technologiques doivent être déployés dans plusieurs centres de données pour se protéger contre une panne de centre de données. Cela s'applique aux systèmes hébergés par un fournisseur de services cloud - défaillance régionale.
8. Exigences des plans de reconstruction de la plateforme et des applications	Le fournisseur doit disposer d'un Plan de reconstruction de la plateforme et des applications pour chaque système technologique requis pour assurer la fourniture des services à Barclays. Ce plan doit être révisé, approuvé et testé au moins une fois tous les 12 mois, ou lors de chaque changement significatif. Ces plans sont destinés aux situations où les options de rétablissement/restauration traditionnelles ne peuvent pas être utilisées et où le système doit être intégralement reconstruit. Les plans doivent tenir compte des éléments suivants : ▪ Système d'exploitation/logiciel d'infrastructure ▪ Déploiement et configuration des applications ▪ Contrôles/configuration de sécurité ▪ Dépendances et réintégration de l'écosystème système ▪ Exigences en matière de données (plan de rétablissement des données) ▪ Dépendances d'outillage pour exécuter les plans de rétablissement	Il est essentiel que les services technologiques et les dispositifs de soutien disposent de plans de rétablissement appropriés en cas d'événement lié à la cyber-intégrité des données.