Obligations de contrôle pour les fournisseurs externes

Plan de rétablissement

Version 12.0 – Octobre 2022

1. Définitions :

« **Crise** »	Désigne une perturbation ou une atteinte à la réputation exigeant une réponse qui dépasse le cadre de la structure et/ou des ressources habituelle(s) et nécessite une intervention de la direction pour la prise de décisions et la coordination.
« 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.
« Croisement de production »	Le terme « Croisement de production » est utilisé lorsqu'un système technologique est basculé vers un environnement alternatif (DR) et utilisé pour exécuter des fonctions de production pendant une période prolongée.
« 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 utilisée pour appliquer les exigences de résilience à un service. Il s'agit notamment du RTO, du RPO, des exigences de validation et de la fréquence.

2. Matrice de criticité en matière de résilience :

Barclays attribue une Catégorie de résilience spécifique (0-4) aux services du Fournisseur. 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 :

		Évaluation de l'impact des risques	Impact exceptionnel	Impact élevé	Impact modéré	Impact faible	Impact insignifiant
		Catégorie de résilience	0	1	2	3	4
		Type de résilience	Continu	Hautement résilient	Résilient	Récupération	Suspension/ Sauvegarde uniquement
Événement perturbateur	Application	Objectif de RTO (Délais de rétablissement visés) (événements non liés aux données/cybernétiques)	Jusqu'à 1 heure	Jusqu'à 4 heures	Jusqu'à 12 heures	Jusqu'à 24 heures	Pas de rétablissement planifié
		Objectif de RPO (Délais de rétablissement visés) (événements non liés aux données/cybernétiques)	Jusqu'à 5 minutes	jusqu'à 15 minutes	jusqu'à 30 minutes	Jusqu'à 24 heures	Pas de rétablissement planifié

3. Contrôles :

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Événements perturbateurs pour les exigences de Planification du rétablissement	Barclays stipule la catégorie de résilience des services demandés. 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. La planification d'Événements perturbateurs doit au minimum tenir compte des éléments suivants : ▪ 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. ▪ 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 de fournisseurs de services cloud ayant un impact sur tous les services technologiques). ▪ Perte de sous-traitant matériel (services ou fournitures).	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
	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. Le Fournisseur doit être en mesure de démontrer qu'un certain nombre de facteurs de gravité ont été pris en compte, testés et validés.	
2. 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 maintenues et examinées tous les 12 mois. Les dépendances à prendre en compte sont les suivantes : ▪ Technologie et données (fournies en interne et par le sous-traitant) ▪ Sous-traitants matériels (essentiels à la fourniture du service 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.
3. Validation des exigences du plan de rétablissement	Le Fournisseur doit mettre en place des Plans de rétablissement de l'activité pour ses Événements perturbateurs convenus. Les Plans de rétablissement de l'activité 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 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
	Les Plans de rétablissement doivent être testés et validés tous les 12 mois 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 et soumettre des plans correctifs détaillés (comprenant les mesures à prendre et les dates d'achèvement correspondantes).	
4. Test intégré	À la demande de Barclays et à une date convenue d'un commun accord, le Fournisseur de services de Catégorie de résilience 0 à 1 doit participer à un test intégré pour valider la continuité et la résilience 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. Plans de rétablissement des systèmes	Le Fournisseur doit avoir mis en place un ou plusieurs Plans de rétablissement des systèmes (SRT) pour chaque système/service technologique requis pour assurer la fourniture des services à Barclays, et respecter les Délais de rétablissement visés (RTO) et Points de rétablissement visés (RPO) correspondants. Ces plans doivent être révisés au minimum tous les 12 mois pour s'assurer de leur exactitude.	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. Plans de rétablissement des données	Le Fournisseur de services de Catégorie de résilience 0 à 1 doit avoir mis en place un ou plusieurs Plans de rétablissement des données pour chaque système/service 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 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 nous sommes confrontés et 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
7. Diversité des centres de données	Le Fournisseur doit s'assurer que chaque service/système technologique requis pour assurer la fourniture des services 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. 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 services de Catégories de résilience 0 à 1 doivent être résilients dans toutes les régions du Cloud.	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 un seul et même événement.
8. Validation des plans de rétablissement des systèmes	Le fournisseur doit tester et valider le(s) Plan(s) de rétablissement des systèmes pour démontrer que les systèmes/services technologiques peuvent être rétablis pour respecter le Délai de rétablissement visé et le Point de rétablissement visé, tels que définis par la Matrice de criticité en matière de résilience. 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 au Plan de rétablissement des systèmes documentés et utilisés comme environnement de production habituel, pour une durée suffisante pour démontrer la capacité et l'intégration complète (Croisement de production). Pour les services conçus comme actifs, la validation doit prouver le fonctionnement continu en cas de perte d'un environnement actif (scénario de ressources de traitement réduites). 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 au moins quatre fois par an via le PCO. - Catégorie de résilience 1 : les plans de rétablissement des systèmes et le PCO doivent être validés au moins deux fois par an via le PCO - Catégorie de résilience 2 : les plans de rétablissement des systèmes doivent être validés au minimum tous les 12 mois ; - Catégorie de résilience 3 : les plans de rétablissement des systèmes doivent être validés au minimum tous les 24 mois ;	Les systèmes technologiques fournis par des tiers peuvent avoir une incidence sur l'expérience des clients de Barclays. Il est essentiel de s'assurer que les tiers 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 puisse suivre les mesures de gouvernances correctes afin de gérer ses fournisseurs. Le croisement de production (PCO) 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.

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
	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).	
9. Validation des plans de rétablissement des données	Le Fournisseur de services de Catégorie de résilience 0 à 1 doit tester et valider le(s) Plan(s) de rétablissement des données pour chaque système/service technologique requis pour assurer la fourniture des services à Barclays et démontrer la capacité du processus de rétablissement à rétablir les données dans un état opérationnel. Cette validation doit être effectuée au moins une fois 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 préjudices. Le plan documenté pour rétablir, récupérer ou recréer des données doit être testé pour confirmer son exactitude et sa viabilité.
10. Plans de reconstruction de la plateforme et des applications	Le Fournisseur de services de Catégorie de résilience 0 à 1 doit disposer d'un Plan de reconstruction de la plateforme et des applications pour chaque service/système technologique requis pour assurer la fourniture des services à Barclays et faire l'objet d'une révision, d'une approbation et d'un test au moins une fois tous les 12 mois. 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.

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
	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).	