External Supplier Control Obligations

Plan de rétablissement

Version 11.0 - Octobre 2021

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.
« **Incident** »	désigne une perturbation qui peut être gérée dans le cadre des activités quotidiennes, en déclenchant des plans de rétablissement.
« **Plan de rétablissement** »	Le processus ou planification du rétablissement des services d'entreprise, des processus d'entreprise et des dépendances sous-jacentes
« **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
« **Délai de rétablissement visé** »	désigne le temps écoulé entre une défaillance ou une interruption imprévue des services et la reprise des activités.

2. 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 engagés. Le Fournisseur doit définir les événements perturbateurs à planifier et le niveau de planification 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. Les catégories d'Événements perturbateurs doivent au minimum tenir compte des éléments suivants : ▪ Perte d'un ou de plusieurs bâtiments sur plusieurs sites ne pouvant pas soutenir les opérations commerciales ; ▪ Scénario de perte de données, notamment les cyberévénements et l'impact potentiel sur la prestation de services à Barclays. Perte de ressources de collaborateurs qui aurait un impact sur la prestation des niveaux de service convenus ; ▪ Indisponibilité des services à Barclays en raison d'événements cybernétiques ou non cybernétiques potentiels et impact potentiel sur la prestation de services à Barclays ; ▪ Rétablissement unique et simultané des services technologiques (par exemple, perte du centre de données)	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 minimiser leur impact (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 afin de s'assurer qu'elles sont tout aussi résilientes pour le fournisseur. Ces dépendances doivent être maintenues et examinées tous les 12 mois. Les dépendances à prendre en compte sont les suivantes : ▪ Perte de toutes les technologies et données ▪ Indisponibilité des services du ou des sous-traitants matériels (ceux qui sont essentiels à la fourniture du service à Barclays) ▪ Perte de main-d'œuvre (perte de bâtiments et/ou perte de personnes ; envisager l'absence de stratégie de récupération des zones de travail ou de possibilité de travail à domicile) Ces éléments doivent être testés et validés dans le cadre du Plan de rétablissement de l'activité, afin de démontrer que les services répondent aux exigences de la catégorie de résilience stipulées par Barclays pour garantir qu'ils sont également résilients et qu'ils répondent aux niveaux de service requis.	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 reprise	Le fournisseur doit mettre en place des Plans de rétablissement de l'activité pour les 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 du service fourni à Barclays. Au minimum, il convient de tenir compte des éléments suivants :	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

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
	▪ 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 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).	assurés, et que les services répondent aux exigences de résilience stipulées par Barclays.
4. Test intégré	Le fournisseur doit participer, à la demande de Barclays, 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 des modifications significatives ont été apportées aux 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 minimiser l'impact sur les clients de Barclays et le système financier dans son ensemble.
5. Procédure de gestion des incidents/crises	Le fournisseur doit disposer d'une procédure de gestion des Incidents et des Crises documentée qui comprend le processus de signalement des incidents/crises à Barclays. Les procédures de gestion des Incidents et des Crises doivent être approuvées après la conduite de tests et d'une validation fructueux par le Fournisseur tous les 12 mois. La procédure doit définir les activités et résultats minimum requis pour gérer et traiter l'Incident/la Crise tout au long de son cycle de vie, de son apparition à sa conclusion. Le fournisseur désignera : (i) une personne chargée d'approuver la procédure et de confirmer son adéquation à l'objectif ;	Il est nécessaire que le fournisseur établisse clairement les procédures de traitement et de gestion de ses services en cas d'Incident ou de Crise. Le fournisseur et Barclays doivent s'entendre sur la procédure de signalement des Incidents et situations de Crise. Des tests et une validation doivent être exécutés pour s'assurer que la personne/l'équipe concernée bénéficie de compétences, de connaissances et d'une organisation suffisantes pour gérer les Incidents et les Crises lorsqu'ils/elles surviennent.

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
	(ii) un interlocuteur principal et un adjoint (en cas d'absence de l'interlocuteur principal) pour chaque rôle afférent à la Crise ;	
6. Rapports post-incident/crise	Suite à une perturbation du service, un rapport post-incident/crise doit être soumis à Barclays dans les quatre semaines civiles suivant le rétablissement du service à des niveaux de fonctionnement normaux. Ce rapport doit comprendre, au minimum, un examen de ce qui suit : ▪ la cause principale de l'Incident ou de la Crise ▪ les mesures correctives mises en œuvre et toutes les actions d'amélioration continue pour éviter que cela ne se reproduise ▪ tout impact sur les clients de Barclays connu du Fournisseur	Un rapport post-incident/crise est requis pour garantir à Barclays que les problèmes sont identifiés/corrigés, et que les enseignements ont été tirés, dans les plus brefs délais.
7. Plan 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 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 systèmes/services 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).	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. 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.
8. 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, et elle peut résulter être 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
9. 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.
10. Validation des plans de rétablissement des systèmes	Le Fournisseur doit tester et valider les Plans de rétablissement des systèmes pour démontrer que les systèmes/services technologiques peuvent être rétablis pour 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 utilisés 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 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. 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.	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 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
11. 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 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.
12. Plans de reconstruction et de reconstitution de la plateforme et des applications	Pour soutenir la reprise après des Événements perturbateurs, tels qu'une cyberexploitation, le Fournisseur doit disposer d'un Plan de reconstruction/reconstitution de la plateforme et des applications pour chaque service/système technologique requis pour assurer la fourniture des services de Catégorie de résilience Barclays 0 à 1 et faire l'objet d'une révision, d'une approbation et d'un test 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 services technologiques et les dispositifs de soutien disposent de plans de rétablissement appropriés en cas d'événement lié à la cyberintégrité des données.

3. 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 spécifié ci-dessous pour la catégorie de résilience applicable stipulée par Barclays :

		ERMF - Risk Impact Assessment	Exceptional Impact	High Impact	Moderate Impact	Low Impact	Insignificant Impact
		Resilience Category	0	1	2	3	4
		Resilience Type	Continuous	Highly Resilient	Resilient	Recover	Suspend / Backup Only
Disruption Event	Application	RTO for Application Recovery (non-data events)	Up to 1 hour	Up to 4 hours	Up to 12 hours	up to 24 hours	No planned recovery
		RPO	Up to 5 minutes	Up to 15 mins	Up to 30 mins	Up to 24 hours	No planned recovery