Obligations de contrôle pour les fournisseurs externes

Risque lié à la technologie – contrôles techniques

Version 12.0 – Octobre 2022

Domaine du contrôle	Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Gestion des problèmes	Identification et enregistrement des problèmes	Le fournisseur doit s'assurer de la mise en œuvre d'un examen en temps opportun des causes profondes de tous les incidents majeurs ponctuels et des incidents répétés lorsque l'impact combiné est suffisant pour entraîner un impact opérationnel significatif.	Lorsque la cause profonde des Incidents importants n'est pas identifiée et résolue en temps opportun, le service risque de connaître des défaillances répétées et évitables, se traduisant par une perturbation des systèmes/du service, une atteinte à la réputation et/ou une corruption/perte de données
	Gestion et résolution des problèmes	Le fournisseur doit s'assurer que la cause profonde des Incidents importants est résolue en temps opportun ou, si cela n'est pas possible, que l'acceptation du risque est fournie par Barclays et que des contrôles d'atténuation appropriés sont appliqués pour limiter la probabilité d'une récurrence.	
Domaine du contrôle	**Intitulé du contrôle**	**Description du contrôle**	**Raisons de l'importance**
2. Gestion des modifications	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 fournie à Barclays sont gérés dans le cadre d'un régime de contrôle des changements rigoureux incluant les objectifs suivants : 1. Aucune modification ne peut être apportée sans autorisation appropriée de Barclays avant sa mise en œuvre 2. Une séparation des tâches doit être mise en place entre la personne qui	L'inadéquation des processus de changement visant à prévenir les modifications non autorisées, mal gérées ou inappropriées de la technologie peut entraîner une interruption de service, une corruption des données, une perte de données, une erreur de traitement ou une fraude.

		initie un changement, le propriétaire, celle qui l'approuve et celle qui le met en œuvre 3. Les changements doivent être planifiés et gérés en fonction du niveau de risque associé au maintien du niveau de service minimum requis pour Barclays 4. Il convient de tenir compte de manière adaptée de l'impact éventuel des changements sur la performance et/ou la capacité des composants technologiques concernés 5. Les changements doivent faire l'objet de tests techniques et professionnels pertinents avant la mise en œuvre et les éléments de preuve issus des tests doivent être conservés si cela est requis 6. Les changements doivent être testés après la mise en œuvre pour s'assurer qu'ils ont été exécutés avec succès sans impact imprévu	
3. Gestion des performances et des capacités	Assurer la conformité constante aux besoins de Barclays en matière de technologie	Le fournisseur doit définir, maintenir et documenter des niveaux de performance et de capacité adaptés pour tous les composants informatiques clés utilisés dans le cadre de la prestation de services fournie à Barclays, conformément à toutes les exigences contractuelles. Il doit également s'assurer que des alertes et des seuils appropriés sont mis 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 toutes les exigences contractuelles et les besoins de Barclays.	Des mesures inadéquates pour définir, documenter et surveiller les niveaux de performance et/ou de capacité des ressources informatiques et l'incapacité à les maintenir en phase avec les exigences actuelles et futures peuvent entraîner une réduction et/ou une interruption inacceptable des services technologiques et une perte d'activité.
Domaine du contrôle	**Intitulé du contrôle**	**Description du contrôle**	**Raisons de l'importance**
4. Développement d'applications technologiques	Stratégie de test et réalisation avant la mise en service technique et/ou commerciale	Le fournisseur doit comprendre la qualité de tous les logiciels avant de les vendre ou de les fournir à Barclays. Tous les codes logiciels doivent être dans le(s) système(s) de contrôle de version et approuvés par le Prestataire de services du fournisseur avant d'être fournis à Barclays. Les modifications apportées aux applications doivent faire l'objet de tests logiciels par le fournisseur afin de s'assurer que les logiciels répondent aux exigences saisies. Les preuves des tests doivent être conservées.	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 commerciaux.
	Confirmation de la configuration système requise	Lors de la livraison du logiciel conformément aux spécifications de Barclays, le fournisseur doit s'assurer que les exigences commerciales sont clairement définies et convenues avec Barclays.	Des exigences d'entreprise mal définies peuvent entraîner un comportement incorrect du système, ce qui peut entraîner un risque pour les processus opérationnels et commerciaux.

	Acceptation par l'entreprise avant le déploiement	Lors de la livraison du logiciel conformément aux spécifications de Barclays, le fournisseur doit accepter et suivre un processus de qualité/d'acceptation convenu avec Barclays.	Une acceptation inadéquate de la part de l'entreprise avant le déploiement peut conduire à un comportement incorrect du système, entraînant un risque pour les processus commerciaux et opérationnels.
5. Modalités concernant la sauvegarde des systèmes et des données	Mettre en œuvre des processus de sauvegarde et de restauration appropriés et efficaces	Le fournisseur doit s'assurer que des processus de sauvegarde et de restauration appropriés ont été mis en place pour tous les services et systèmes informatiques utilisés dans le cadre de la prestation de services fournie à Barclays, qu'ils sont appliqués en conformité avec les besoins de Barclays et que leur efficacité est périodiquement démontrée.	L'absence de sauvegarde des données de l'entreprise ou un contrôle insuffisant de cette sauvegarde peut entraîner une interruption des systèmes/services, une perte de données ou une 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 fournie à Barclays, ainsi que les modalités de traitement et de stockage de ces supports, sont à tout moment sûrs et fiables.	Des supports de sauvegarde sécurisés et fiables sont nécessaires pour éviter les interruptions de systèmes/services, une perte de données ou la divulgation inappropriée de données.
Domaine du contrôle	**Intitulé du contrôle**	**Description du contrôle**	**Raisons de l'importance**
6. 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'utilisation de composants non destinés à la production dans la prestation de services de production crée un risque dans la mesure où ils peuvent ne pas être construits ou gérés selon les normes de production.
	Consignation et administration des éléments de configuration	Le fournisseur doit tenir des registres complets et exacts pour l'ensemble des Éléments de configuration relevant du champ d'application utilisés dans la fourniture de la prestation de services fournie à Barclays (y compris la propriété et les dépendances/mappages en amont/aval). Le fournisseur doit avoir mis en place des contrôles garantissant le maintien permanent de l'exactitude et de l'exhaustivité des données.	Des entrées de registre inappropriées ou incomplètes (ainsi que des 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 des incidents et des changements.

7. Gestion des niveaux de service	Définition et surveillance des performances du service	Le fournisseur doit s'assurer que le service est conforme aux niveaux de service convenus, y compris la surveillance et le signalement des niveaux de service.	Les niveaux de service garantissent que les services informatiques sont fournis conformément aux engagements pris en la matière

Définitions liées à la technologie :

Élément de configuration	Tout composant devant être géré pour fournir un service informatique. Les Éléments de configuration peuvent être physiques (par ex. un ordinateur ou un routeur), virtuels (par ex. un serveur virtuel) ou logiques (par ex. un service). Les changements (ajouts, modifications ou cessations) doivent être entrepris sous le contrôle de la gestion des changements.
Incident	Une interruption non planifiée d'un service informatique ou une réduction de la qualité d'un service informatique, y compris, sans s'y limiter, la défaillance d'un élément de configuration qui n'a pas encore eu d'impact sur un service.
Service informatique	Service fourni à un ou plusieurs Clients par un Prestataire de services informatiques. Un service informatique est constitué d'une combinaison de personnes, de processus et de technologies de l'information et est fourni aux clients pour soutenir leurs processus commerciaux.
Incident majeur	Incident qui présente un risque/un impact important pour Barclays et qui peut entraîner de graves conséquences, notamment une perte importante de productivité, des dommages à la réputation/réglementation et un impact sur les principaux processus d'entreprise, les contrôles ou les systèmes clés.
Problème	La cause inconnue d'un ou plusieurs Incidents.