

Obligations de contrôle pour les  
fournisseurs externes

Risque lié à la technologie – contrôles  
techniques

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/perde 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.	
2. Gestion des modifications	Appliquer un contrôle des changements rigoureux	<p>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 :</p> <ol style="list-style-type: none"> <li>1. Le fournisseur doit informer Barclays de tous les changements importants avant leur mise en œuvre afin que l'évaluation de l'impact puisse être effectuée et que des mesures d'atténuation appropriées soient mises en place, le cas échéant.</li> <li>2. Une séparation des tâches doit être mise en place entre la personne qui initie un changement, le propriétaire, celle qui l'approuve et celle qui le met en œuvre</li> <li>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</li> <li>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</li> <li>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</li> <li>6. Les changements doivent être testés après la mise en œuvre pour s'assurer qu'ils ont été exécutés avec succès sans impact imprévu</li> </ol>	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.

Domaine du contrôle	Intitulé du contrôle	Description du contrôle	Raisons de l'importance
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 les niveaux de performance et de capacité appropriés pour tous les composants informatiques clés utilisés dans le cadre des prestations de service fournies à Barclays, conformément à toutes les exigences contractuelles, en tenant compte de la demande métier connue et de l'utilisation actuelle de la capacité, afin de s'assurer que la capacité disponible continue à répondre aux exigences. 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.
4. Développement d'applications technologiques	Stratégie de test et réalisation avant la mise en service technique et/ou commerciale	Le fournisseur doit s'assurer que le logiciel/service fonctionne comme décrit par le fournisseur avant de vendre ou fournir ce logiciel ou service basé sur un logiciel à Barclays ou fournir une présentation des défauts connus et de l'impact sur la livraison du logiciel/service. Tous les codes logiciels doivent être dans les systèmes de contrôle de version et approuvés par le fournisseur avant d'être fournis à Barclays. Le fournisseur doit soumettre toutes les modifications d'application aux tests logiciels pour s'assurer que le logiciel répond aux exigences saisies. Le fournisseur doit conserver les preuves de test.	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 technologiques d'entreprise 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 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.

## 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.
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.
Changements significatifs	Changements qui auront un impact, ou qui pourraient avoir un impact, sur le fonctionnement effectif du ou des services fournis à Barclays, et/ou changements pour lesquels Barclays devra, ou pourrait avoir besoin de, prendre des mesures d'atténuation des risques appropriées pour soutenir leur mise en œuvre.