Obligations de contrôle pour les fournisseurs

Processus de paiement

Version 12.0 – Octobre 2022

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Respect des exigences législatives et réglementaires locales	Le fournisseur doit s'assurer que les exigences légales et réglementaires applicables aux paiements traités par le fournisseur sont documentées et observées de manière appropriée.	Assurer le traitement des paiements en conformité avec les exigences légales et réglementaires applicables. Le non-respect des exigences légales et réglementaires peut engendrer des amendes et des problèmes liés à la réputation.
2. Intégrité des instructions de paiement	Le fournisseur doit s'assurer que l'intégrité et l'exactitude des informations de paiement sont préservées, du déclenchement au règlement du paiement. Cela inclut le respect des critères suivants : • Les informations de paiement doivent rester intactes tout au long de leur cycle de vie et toute modification doit être détectée ; • Les informations de paiement doivent être traitées et gérées conformément à la requête d'origine, aux réglementations applicables et aux exigences du programme ; et • Les informations de paiement ne sont pas dupliquées (ainsi, les paiements effectués deux fois sont identifiés et empêchés/corrigés).	En cas de non-respect de cette exigence, Barclays est dans l'incapacité d'avoir la certitude que le fournisseur dispose des contrôles adaptés pour assurer la préservation de l'intégrité des instructions de paiement tout au long du cycle de vie du paiement. Le non-respect de cette exigence pourrait se traduire par le versement de paiements potentiellement frauduleux, par des contrôles des crimes financiers n'étant pas effectués de manière efficace, par des erreurs dans le traitement des paiements, ainsi que par l'atteinte à la réputation qui en découlerait et/ou par une amende/sanction réglementaire.
3. Authentification de l'expéditeur	Le fournisseur doit s'assurer qu'une validation appropriée de l'authenticité de la demande de paiement est en place. Le fournisseur devrait confirmer, conformément aux exigences légales, que la demande de paiement provient d'une source légitime (par exemple en appliquant la procédure « Identification et vérification » (« ID&V »)), et confirmer la validité de l'intégrité des instructions de paiement (à savoir, confirmer que les instructions de paiement n'ont pas été modifiées).	Cette exigence permet de confirmer la légitimité des instructions de paiement en s'assurant que l'instruction de paiement est authentique. Ce contrôle réduit le risque de perte associé aux paiements frauduleux, d'atteinte à la réputation qui en découlerait et/ou d'imposition d'une amende/sanction par l'organisme de réglementation.
4. Pouvoirs de l'expéditeur	Le fournisseur doit s'assurer que chaque demande de paiement a été approuvée et autorisée par les personnes physiques prédéfinies et pré-approuvées.	Cette exigence permet de confirmer l'authenticité des instructions de paiement en s'assurant que les signataires des instructions de paiement disposent d'un mandat à cette fin. Ce contrôle limite le risque de perte associé aux paiements frauduleux ou entachés d'erreurs, d'atteinte à la

		réputation qui en découlerait et/ou d'imposition d'une amende/sanction par l'organisme de réglementation.
5. Autorisation tout au long du cycle de paiement	Le fournisseur doit s'assurer que, tout au long du cycle de paiement, la personne qui approuve le paiement le fait dans le cadre de la limitation de pouvoirs établie (limitation de pouvoirs prédéfinie et pré-approuvée). La limitation de pouvoirs doit être révisée au moins une fois par an et dès que nécessaire.	Cette exigence permet de confirmer la validité des instructions de paiement en s'assurant que le niveau de pouvoirs différent exercé tout au long du processus de paiement est conforme à la délégation de pouvoirs établie et approuvée au sein de l'entreprise. Ce contrôle limite le risque de perte associé aux paiements frauduleux/erronés, d'atteinte à la réputation qui en découlerait et/ou d'imposition d'une amende/sanction par l'organisme de réglementation.
6. Indépendance des niveaux tout au long du cycle de paiement	Le fournisseur doit s'assurer que la personne qui approuve le paiement est indépendante et ne dispose pas des droits d'accès nécessaires pour créer et modifier une instruction.	Ce contrôle assure que tous les risques d'erreur ou de problèmes seront identifiés de manière proactive par une personne physique indépendante. Ce contrôle atténue le risque de perte associé aux paiements frauduleux/erronés, d'atteinte à la réputation qui en découlerait et/ou d'imposition d'une amende/sanction par l'organisme de réglementation.
7. Retards dans le traitement des paiements	Le fournisseur doit s'assurer que chaque paiement est traité et versé en temps opportun, et dans le respect de délais d'exécution maximums convenus ou exigés par la loi, afin d'assurer la conformité aux SLA (Accords de niveau de service) (exigences concernant le client et le système de paiement).	Cette exigence assure que tous les paiements traités par le fournisseur le sont conformément aux systèmes de paiement/de carte applicables convenus et conformément aux exigences des clients. Elle permet, par là même, de réduire le risque de traitement tardif de paiements. Le traitement tardif d'instructions de paiement pourrait provoquer une augmentation des cas de mécontentement des clients et des réclamations, qui conduirait à un risque de départs de clients et d'atteinte à la réputation.
8. Méthodes de communication et de transmission admissibles pour le transfert d'instructions de paiement	Le fournisseur doit s'assurer que toutes les méthodes de communication et de transmission pour procéder au transfert d'instructions de paiement sont documentées et que seules les méthodes acceptables sont utilisées avec les niveaux de contrôle appropriés.	Barclays a défini des méthodes de transmission d'instructions de paiement interdites, soumises à des restrictions et approuvées en vue de limiter de nombreux risques comme les risques liés aux informations (confidentialité des données), les risques liés à la fraude (manipulation des données), les cyber-risques (cybermenaces), etc.

	Les méthodes interdites sont les suivantes : supports amovibles (disquette, CD, DVD) et mémoires externes (clés USB, disques durs USB, etc.). Les méthodes acceptables se divisent en deux catégories : 1. Les méthodes soumises à des restrictions sont les suivantes : en personne, fax, e-mail, téléphone/oral, papier, feuille de calcul, etc. Ces méthodes sont utilisées uniquement lorsque des obligations de contrôle du fournisseur pour le processus de paiement sont en place et appliquées de manière adéquate afin de réduire les risques associés à la méthode appliquée. 2. Les méthodes préférées sont les suivantes : systèmes automatisés et en ligne, où personne ne peut créer ni modifier un paiement.	Les formats tels que les supports amovibles (USB, CD, etc.) sont interdits et les formats tels que les e-mails sont soumis à des restrictions. Les e-mails sont acceptés uniquement si les contrôles adaptés sont en place.
9. Rôles et responsabilités	Le fournisseur doit définir et communiquer les rôles et responsabilités relatifs au Risque lié aux processus de paiement Ceux-ci doivent être révisés après chaque changement important apporté à l'activité ou au modèle d'exploitation du fournisseur.	Cette exigence assure que les rôles et responsabilités de chaque partie sont établis, documentés et approuvés. Ces informations seront utiles en cas de litige.
10. Risque lié au système de paiement/de carte	Le fournisseur doit s'assurer que tous les paiements traités au nom de Barclays le sont conformément aux exigences du système de paiement/de carte.	En cas de non-respect de cette exigence, Barclays est dans l'incapacité d'avoir la certitude que le fournisseur dispose des procédures documentées adéquates pour répondre aux risques associés au défaut de respect des exigences du système de paiement/de carte. Tous les paiements dont le traitement, d'une part, présente un caractère erroné, un caractère tardif ou des défaillances en matière d'authentification ou d'autorisation et, d'autre part, conduit à un défaut de respect des règlements relatifs au paiement applicables doivent être signalés au regard des risques de niveau 3 associés. En outre, tout défaut de respect des règlements relatifs aux paiements doit entraîner l'application du processus de gouvernance applicable pour signaler des violations de la réglementation au titre du Risque lié au comportement.
11. Évaluation des risques liés au système	**Cette exigence de contrôle ne concerne que les fournisseurs qui sont des membres directs ou indirects de Systèmes de paiement ou de carte.**	L'expression « Risque lié au système de paiement/de carte » fait référence aux risques liés à une gestion déficiente de l'adhésion au système.

	Le fournisseur doit effectuer une évaluation complète des risques liés au système, au moins une fois par an, pour chacun des systèmes de paiement/de carte dont il est directement ou indirectement membre. L'évaluation des risques doit être contresignée par le propriétaire du système et par sa direction. Des évaluations supplémentaires des risques liés au système doivent être réalisées en cas de modification significative des processus ou réglementations, ou avant de souscrire ou d'adhérer à un nouveau système de paiement/de carte.	Définition d'un système de paiement/de carte : Administrateur système/externe d'un réseau de paiement qui établit les règles régissant le processus d'autorisation et de règlement des paiements (par ex. BACS, CHAPS, Faster Payments et sociétés d'autorisation de chèques et de crédit). Les systèmes de paiement/de carte (Visa et MasterCard, par exemple) contrôlent le transfert ou le paiement de sommes d'argent, mais ne facilitent pas l'exécution du contrat sous-jacent. Cette exigence de contrôle vise à garantir que les risques associés au système de paiement/de carte ont été gérés de manière appropriée. Le défaut d'identification des risques liés à l'adhésion pourrait se traduire par le versement de paiements potentiellement frauduleux, par des erreurs dans le traitement des paiements, ainsi que par l'atteinte à la réputation qui en découlerait et/ou par une amende/sanction réglementaire.
12. Propriétaire du système	Le fournisseur doit s'assurer de la désignation d'un propriétaire du système de paiement/de carte chargé d'entretenir la relation dans son ensemble et d'assurer la surveillance continue des risques liés aux modalités du système. En outre, le fournisseur doit s'assurer que le propriétaire du système surveille les risques liés au système et les signale en utilisant les canaux de gouvernance.	Cette exigence assure que le système de paiement/de carte concerné est rattaché à un propriétaire désigné en vue de parvenir à une meilleure gestion de la relation et d'assurer le signalement des informations pertinentes en temps opportun.

Acronymes	Définitions
Risque lié aux processus de paiement	L'expression « Risque lié aux processus de paiement » fait référence au risque de défaillance dans la mise en œuvre des processus de paiement. • Les paiements sont traités de manière inexacte • Les paiements sont traités sans autorisation appropriée • Les paiements sont traités sans authentification appropriée • Les paiements sont traités avec des retards En outre, le risque lié à l'incapacité de gérer la qualité de membre du système de paiement/de carte

Manuel(le)	Qualifie toute action qui nécessite une intervention humaine à toute étape de la transaction (envisagée de bout en bout)/du cycle de vie du processus de paiement.
Paiement manuel	L'expression « paiement manuel » désigne l'opération par laquelle une partie reçoit des fonds d'une autre partie, envoie des fonds à une autre partie ou effectue un transfert interne au bénéfice d'une autre partie et qui est effectuée par l'intermédiaire d'un système externe ou dans le cadre d'une relation avec une banque correspondante en application duquel/de laquelle une partie du processus de paiement, de l'émission jusqu'au règlement, y compris toute correction ou modification, est réalisée manuellement.
Méthodes de communication et de transmission admissibles pour le transfert d'instructions de paiement	Les méthodes interdites sont les suivantes : disques externes/clés USB/disquettes souples/CD/disquettes. Les méthodes soumises à des restrictions sont les suivantes : communications au sein de succursales/en personne/par fax/par e-mail.* Les méthodes admissibles sont les suivantes : banque en ligne/banque mobile/autres méthodes définies et convenues dans les limites du niveau d'appétence au risque approuvé. * Note concernant les méthodes soumises à des restrictions : ces canaux peuvent être utilisés pour autant que les contrôles appropriés prévus par le présent document aient été mis en place.
Cycle de paiement	Le cycle débute lors de l'émission du paiement et de sa saisie dans le canal de paiement et prend fin une fois que le paiement a été réglé à la contrepartie par l'intermédiaire du système de règlement externe.
Expéditeur	Une personne physique qui soumet une ou plusieurs demandes de paiement.
Risque lié au système de paiement/de carte	L'expression « Risque lié au système de paiement/de carte » fait référence de manière conjointe aux trois principales catégories de risques liés à la qualité de membre d'un système de paiement/de carte, à la structure du système et aux activités s'y rapportant : • risque lié à l'activité : le risque que le régime/système de paiement/de carte ou l'un de ses composants (par exemple le fournisseur d'infrastructure utilisé) ne puisse être maintenu de manière à assurer la continuité de service/d'exploitation en cas de chocs financiers défavorables ; • risque lié au règlement : le risque qu'un autre participant à un système se trouve dans l'incapacité d'exécuter ses obligations financières à leur date d'échéance prévue par le système, ou s'abstienne de les exécuter, ou qu'un autre établissement qui facilite la satisfaction de ces obligations – comme l'agent de règlement – se trouve en situation d'insolvabilité ; • risque opérationnel : le risque qu'un opérateur du système ou qu'un fournisseur essentiel du mécanisme soit dans l'incapacité, d'un point de vue opérationnel, d'assurer le traitement ou le règlement de paiements dans les conditions prévues en raison du caractère inadapté ou de défaillances de processus internes, de personnel et de systèmes.