

External Supplier Control Obligations

Applications développées par
l'utilisateur final (EUDA)

Prière de noter que les applications « EUDA » telles que mentionnées dans les présentes Obligations de contrôle des fournisseurs, correspondent uniquement aux EUDA identifiées via l'arbre de décision EUDA de Barclays et à celles que le fournisseur utilise pour fournir ses services à Barclays.

Domaine de contrôle	Titre du contrôle	Description du contrôle	Raisons de l'importance
Gouvernance et assurance	1. Rôles et responsabilités	<p>Le fournisseur doit définir et communiquer les rôles et responsabilités relatives aux EUDA.</p> <p>Une révision sera nécessaire si des modifications sont apportées à la documentation associée au modèle d'exploitation ou aux activités du fournisseur.</p> <p>Les rôles clés doivent comprendre un cadre supérieur responsable des EUDA.</p>	<p>Les applications EUDA nécessitent un parrainage de haut niveau en vue d'assurer une conception, une implémentation et une exécution efficaces des contrôles.</p> <p>Une surveillance continue est indispensable pour fournir aux cadres supérieurs l'assurance requise quant à la conception et à l'exécution des contrôles des risques associés aux informations.</p>
Gouvernance et assurance	2. Signalement des risques associés aux informations	<p>Il est indispensable de mettre en place des procédures et contrôles documentés afin de s'assurer que les incidents concernant les risques associés aux EUDA sont signalés et gérés.</p> <p>Le fournisseur devrait réagir face aux incidents portant sur les applications EUDA et à toute violation des informations en les signalant sans délai à Barclays. Il est impératif d'établir une procédure de réaction en cas d'incident permettant de gérer et de signaler rapidement toute erreur ayant un impact sur les informations de Barclays et/ou les services utilisés par Barclays.</p> <p>Le fournisseur doit s'assurer que les actions correctives identifiées suite à un incident sont gérées par le biais d'un plan de résolution des problèmes (action, responsabilité, date de mise en œuvre) partagé et convenu avec Barclays.</p>	
Gouvernance et assurance	3. Surveillance continue	<p>Le fournisseur doit régulièrement et dans tous les cas au moins une fois par année civile évaluer, réviser et documenter sa conformité au présent programme.</p>	

Gouvernance et assurance	4. Conformité aux exigences législatives et réglementaires locales	Le fournisseur doit s'assurer que les exigences législatives et réglementaires portant sur les applications EUDA, en vigueur dans la juridiction d'activité du fournisseur, sont correctement documentées et respectées.	(comme ci-dessus)
Gouvernance et assurance	5. Éducation et sensibilisation concernant les EUDA	Le fournisseur doit identifier les employés ayant des responsabilités liées aux EUDA. Les employés qui ont reçu un rôle lié aux EUDA doivent suivre la formation d'éducation et de sensibilisation correspondant à leur rôle. Ce contrôle doit avoir lieu au moins une fois par an ; conserver un justificatif permettant de confirmer qu'il a bien été réalisé.	
Objectifs de contrôle concernant les EUDA	6. Identification des EUDA	Une procédure doit être mise en place et documentée afin d'identifier toutes les EUDA appartenant au fournisseur, ou que celui-ci exécute, pour fournir ses services à Barclays.	L'identification des EUDA est essentielle pour déterminer le niveau adéquat de contrôle requis pour toutes les EUDA.
Objectifs de contrôle concernant les EUDA	7. Évaluation de la criticité des EUDA	La criticité de chaque EUDA doit être mesurée avant sa première utilisation et avant d'implémenter des modifications au niveau de chaque EUDA. L'évaluation de criticité du fournisseur devrait tenir compte d'éléments tels que les atteintes à la réputation et les impacts réglementaires et financiers sur le service fourni par le fournisseur à Barclays. L'évaluation de criticité devrait également prendre en considération la probabilité d'erreur et la signification. Veuillez consulter l'Annexe C <i>En termes de signification, les critères suivants sont pertinents :</i> <ul style="list-style-type: none"> • <i>Est-ce que l'EUDA permet de réaliser des activités essentielles associées au produit/service fourni à Barclays ?</i> 	Comprendre la criticité de l'EUDA peut permettre à notre fournisseur de déterminer et mettre en œuvre le niveau adéquat de contrôle de l'EUDA.

		<ul style="list-style-type: none"> • <i>Est-ce que les résultats de l'EUDA peuvent avoir un impact financier sur Barclays ?</i> • <i>Les clients de Barclays risquent-t-ils d'être affectés de manière négative si des informations, calculs ou résultats de l'EUDA sont inexacts, obsolètes ou corrompus ?</i> <p><i>En termes de probabilité d'erreur, les critères suivants sont pertinents :</i></p> <ul style="list-style-type: none"> • <i>Complexité apparente de l'EUDA (aucun calcul important jusqu'à un degré élevé de formules complexes et avancées) ;</i> • <i>Fréquence d'utilisation ;</i> • <i>Fréquence des modifications apportées à la formule/logique de l'EUDA ; et</i> • <i>Nombre d'utilisateurs.</i> <p>La criticité de l'EUDA est à convenir avec Barclays.</p>	
Objectifs de contrôle concernant les EUDA	8. Impératifs minimum de contrôle en fonction de la criticité de l'EUDA	<p>Le fournisseur doit adopter des contrôles qui répondent aux impératifs des objectifs de contrôle selon le degré de criticité convenu avec Barclays.</p> <p>Les objectifs de contrôle marqués d'un « I » sont impératifs dans ce programme. Les autres objectifs de contrôle sont seulement optionnels et marqués d'un « O ». Consulter l'annexe B où les contrôles sont répertoriés dans un tableau.</p> <p>Il est indispensable de conserver un justificatif, le cas échéant, afin de pouvoir confirmer que les objectifs de contrôle applicables sont en voie d'être atteints.</p>	Le risque que représente l'EUDA sert de point de repère pour appliquer le niveau de contrôle adéquat afin d'éviter un contrôle excessif alors que l'EUDA ne présente en réalité qu'un faible risque.
Objectifs de contrôle des EUDA	9. Justification des EUDA	<p>Chaque EUDA doit être soumise à une procédure de justification avant sa première utilisation afin d'évaluer si elle est réellement nécessaire ou bien si d'autres moyens visant à appuyer le processus opérationnel associé (par ex. la transition vers un service de gestion) s'avèreraient plus efficaces et/ou poseraient un moindre risque comparés au maintien d'une EUDA.</p> <p>La procédure de justification de l'EUDA doit avoir lieu lors de sa création initiale (c'est-à-dire avant sa première utilisation) puis à intervalles réguliers par la suite.</p>	L'exécution de la procédure de justification de l'EUDA permet au fournisseur d'évaluer si l'EUDA est réellement nécessaire.

		<p>Conserver les résultats et les éléments justificatifs de la procédure est indispensable ainsi que de les communiquer à Barclays avant la première utilisation de l'EUDA, et chaque fois que la procédure est renouvelée par la suite.</p>	
Objectifs de contrôle des EUDA	10. Enregistrement des EUDA	<p>Un inventaire des EUDA est indispensable afin de donner de manière claire une idée du nombre total des EUDA du fournisseur tout en y associant des attributs clés en vue de répondre aux dispositions du présent programme.</p> <p>Une procédure doit être documentée et mise en place pour assurer la présence d'un inventaire complet, précis et actualisé des EUDA. Une révision de l'inventaire des EUDA doit avoir lieu au moins une fois par an pour vérifier qu'il est complet et exact.</p>	L'intégralité de l'inventaire des EUDA est primordiale pour garantir un fonctionnement correct et une sécurité adéquate des EUDA.
Objectifs de contrôle des EUDA	11. Accès	L'accès aux données et à la logique applicative des EUDA doit être limité aux utilisateurs adéquats disposant des droits d'accès appropriés. La révision des droits d'accès repose sur une approche basée sur les risques.	Des contrôles d'accès adéquats protègent les EUDA contre les accès non autorisés, inappropriés ou non vérifiables.
Objectifs de contrôle des EUDA	12. Disponibilité	Des contrôles doivent permettre de s'assurer que les EUDA sont disponibles en accord avec les impératifs convenus avec Barclays.	La disponibilité des EUDA garantit la continuité des processus opérationnels.
Objectifs de contrôle des EUDA	13. Gestion des modifications	<p>Le suivi de principes de gestion des modifications garantit un fonctionnement correct des EUDA si des modifications sont apportées à la logique applicative.</p> <p>Une modification de la logique applicative ou des données statiques clés des EUDA ne doit pas engendrer d'erreurs dans les résultats, ni d'erreurs de signalement. Les utilisateurs des EUDA doivent accéder uniquement aux (à la) version(s) pertinente(s) de l'EUDA pour assurer une utilisation opérationnelle.</p> <p>L'exactitude et l'intégralité des données d'entrée, des calculs et des données de sortie sont validées par des essais (automatisés et/manuels) afin d'assurer que les modifications appliquées ont produit les résultats escomptés.</p> <p>Identifier et convenir des étapes d'essai avec Barclays pour toute EUDA classée Moyenne ou Élevée dans l'évaluation de criticité des EUDA. Cela permet d'éviter que les modifications engendrent des erreurs de signalement.</p> <p>Les versions archivées ne doivent pas être stockées au même endroit que la (les) version(s) de production.</p>	Une gestion adéquate des modifications est primordiale pour que l'EUDA continue de fonctionner comme prévu après une modification

		Le fournisseur doit désigner une deuxième personne pour prendre en charge l'utilisation et la maintenance continues de l'EUDA en l'absence de l'utilisateur principal (ou utilisateurs principaux).	
Objectifs de contrôle des EUDA	14. Documents requis	<p>Les connaissances liées aux entrées, calculs, sorties et la capacité de modifier ces éléments ne doivent pas être limitées à un seul individu.</p> <p>Il faut en plus disposer d'une documentation appropriée utilisable par un individu spécifique compétent en matière d'EUDA qui lui permette de modifier et d'entretenir l'EUDA.</p>	Étant donné que les EUDA sont gérées par les utilisateurs finaux, une telle documentation est importante pour que les informations critiques concernant l'EUDA soient conservées en vue de garantir le transfert des connaissances et réduire le plus possible le risque de perdre de ces connaissances.

Annexe A : Définitions utilisées par Barclays

Définitions	
EUDA	Les EUDA sont des applications et outils créé(e)s, utilisé(e)s et géré(e)s par les utilisateurs finaux. Elles sont de manière générale développées à l'aide de logiciels de bureau standard (le plus souvent Microsoft Excel ou Access) et autres types de bases de données, requêtes, macros, scripts, outils d'établissement de rapports, exécutables et paquets de code. Les EUDA fonctionnent ou font partie d'un processus opérationnel de manière continue (il ne s'agit pas d'une utilisation ponctuelle). Par conséquent, si leurs calculs ou résultats sont inexacts, indisponibles, obsolètes ou corrompus, cela pourrait avoir un impact financier, ou réglementaire sur la banque, porter atteinte à sa réputation ou encore porter préjudice au client.

Annexe B : Impératifs de contrôle minimum

L'applicabilité de chaque contrôle est déterminée dans le tableau suivant (O = Optionnel et I = Impératif) :

Titre du contrôle	Degré de criticité des EUDA			
	Très faible	Faible	Moyen	Élevé
1. Rôles et responsabilités	I	I	I	I
2. Signalement des risques associés aux informations	I	I	I	I
3. Surveillance continue	I	I	I	I
4. Conformité aux exigences législatives et règlementaires locales	I	I	I	I
5. Éducation et sensibilisation concernant les EUDA	I	I	I	I
6. Identification des EUDA	I	I	I	I
7. Évaluation de la criticité des EUDA	I	I	I	I
8. Impératifs minimum de contrôle en fonction de la criticité de l'EUDA	I	I	I	I
9. Justification des EUDA	I	I	I	I
10. Enregistrement des EUDA	O	I	I	I
11. Accès	O	I	I	I
12. Disponibilité	O	O	I	I
13. Gestion des modifications	O	O	I	I
14. Documents requis	O	O	O	I

Annexe C : Évaluation de la criticité des EUDA

L'évaluation de la criticité des EUDA comprend deux sous-évaluations ; les utilisateurs principaux des EUDA doivent exécuter les deux sous-évaluations pour déterminer la criticité des EUDA.

- Une évaluation de la signification des EUDA pour Barclays.
- Une évaluation de la probabilité d'erreur des EUDA.

La signification de toute EUDA individuelle est définie comme la notation la plus élevée obtenue d'après les critères énumérés ci-dessous

Signification de l'EUDA Critère1	Notation de la signification de l'EUDA			
	Faible	Modérée	Élevée	Exceptionnelle
1) L'EUDA soutient-elle des activités critiques qui ont un impact réglementaire (équivalant à des actifs pondérés en fonction des risques (APR) ou exposition directement impactée par l'EUDA) ?	< 50 M £	≥ 50 M £ ≤ 500 M £	> 500 M £ ≤ 1 Mrd £	> 1 Mrd £
2) Le résultat de l'EUDA a-t-il un impact sur l'information financière ?	Impact sur le compte de résultat < 1 M £ Impact sur le bilan < 1 Mrd £	Impact sur le compte de résultat ≥ 1 M £ < 10 M £ Impact sur le bilan ≥ 1 Mrd £ < 2 Mrd £	Impact sur le compte de résultat ≥ 10 M £ < 50 M £ Impact sur le bilan ≥ 2 Mrd £ ≤ 3 Mrd £	Impact sur le compte de résultat ≥ 50 M £ Impact sur le bilan > 3 Mrd £
3) Si les informations, les calculs et les résultats de l'EUDA étaient inexacts, périmés ou corrompus, quel serait l'impact probable sur les clients de la banque ?	Clients affectés < 100 Perte clients cumulée < 1 M £	Clients affectés ≥ 100 < 1000 Perte clients cumulée ≥ 1 M £ < 10 M £	Clients affectés ≥ 1000 < 10000 Perte clients cumulée ≥ 10 M £ < 50 M £	Clients affectés ≥ 10000 < 50000 Perte clients cumulée ≥ 50 M £
4) Si les informations, les calculs et les résultats de l'EUDA étaient inexacts, périmés ou corrompus, quel serait l'impact probable sur la réputation de la banque ?	Impact jugé non substantiel au niveau d'une unité commerciale locale. Pas d'impact sur	Impact jugé gérable au niveau d'une unité commerciale locale. Pas d'impact sur la marque ou la réputation du Groupe.	Impact préjudiciable pour plusieurs unités commerciales/régions. Tout impact sur la marque du Groupe est improbable.	Impact probable sur la marque du Groupe.

	la marque ou la réputation du Groupe.			
--	---------------------------------------	--	--	--

L'utilisateur principal de l'EUDA doit utiliser les critères ci-dessous pour évaluer la probabilité d'erreur de l'EUDA.

L'utilisateur principal de l'EUDA doit additionner les scores sur l'ensemble des critères pour calculer la notation finale de probabilité d'erreur.

Critères de probabilité d'erreur de l'EUDA	Score de probabilité d'erreur			
	Un	Deux	Trois	Quatre
1) Quelle est la complexité perçue de l'EUDA ? (voir la définition ci-dessous*)	Rudimentaire	Faible	Intermédiaire	Avancée
2) Quelle est la fréquence d'utilisation de l'EUDA ?	Utilisation moins d'une fois par trimestre	Une fois ou plus par trimestre mais moins d'une fois par mois	Une fois ou plus par mois mais pas quotidiennement	Une fois ou plus par jour
3) Quelle est la fréquence des changements de formules/logiques dans l'EUDA ?	Jamais ou très rarement	Des changements sont apportés mais à titre exceptionnel	Changements réguliers mais pas à chaque fois que l'EUDA est utilisée	Chaque fois que l'EUDA est utilisée
4) Combien d'utilisateurs l'EUDA compte-t-elle ?	Utilisateur unique	Plusieurs utilisateurs dans la même équipe opérationnelle	Plusieurs utilisateurs dans différentes équipes au sein d'une UC ou d'un service	Plusieurs utilisateurs à travers différent(e)s UC et/ou services

*Elle désigne la fonctionnalité de l'EUDA et est classée comme suit :

- **Rudimentaire** – Pas de calculs significatifs dans l'EUDA. Principalement utilisée pour des rapports de synthèse.
- **Faible** – Un vérificateur ayant une connaissance limitée de l'application peut interpréter l'objet et l'efficacité des formules en observant et sans explication supplémentaire.
- **Intermédiaire** – Présente une fonctionnalité plus complexe. Un vérificateur compétent dans l'utilisation de l'application (par ex. Excel, Access) peut avoir besoin d'informations complémentaires pour interpréter l'objet et l'efficacité de l'EUDA.
- **Avancée** – Degré élevé de complexité et formules avancées. Peut également être liée à d'autres tableurs, bases de données, sites Internet, tableaux, etc.

La notation finale de probabilité d'erreur doit être calculée en appliquant le score cumulé au tableau ci-dessous :

Notation de probabilité d'erreur	Peu probable	Possible	Probable	Très probable
Score cumulé	$\geq 4 < 6$	$\geq 6 < 9$	$\geq 9 < 12$	$\geq 12 \leq 16$

Évaluation de la criticité des EUDA

L'utilisateur principal de l'EUDA doit combiner les évaluations de la signification et de la probabilité d'erreur pour déterminer la criticité globale de l'EUDA. Le tableau suivant doit être utilisé. L'évaluation de la criticité de l'EUDA doit être consignée dans l'inventaire des EUDA par l'utilisateur principal de l'EUDA.

Signification	Exceptionnelle	Moyenne	Moyenne	Élevée	Élevée
	Élevée	Moyenne	Moyenne	Moyenne	Élevée
	Modérée	Faible	Faible	Moyenne	Moyenne
	Faible	Très faible	Très faible	Très faible	Très faible
Probabilité d'erreur		Peu probable	Possible	Probable	Très probable