BARCLAYS

Obligations de contrôle pour les fournisseurs externes

EUDA – Applications développées par un utilisateur final (« End User Developed Applications »)

Version 13.0 – Septembre 2023

Veuillez noter que le terme « EUDA » utilisé tout au long du présent document s'applique uniquement à l'EUDA identifiée par l'arbre décisionnel EUDA de Barclays et aux EUDA utilisées pour prendre en charge le service et que le fournisseur procure à Barclays.

Suite à l'introduction des SCO en matière de contrôle de gestion, trois EUDA de gouvernance et de contrôle (Rôles et responsabilités, Signalement des risques liés aux EUDA, Formation et sensibilisation aux EUDA) ont été supprimés des SCO, car il s'agit de fonctions communes qui sont désormais couvertes par les SCO en matière de contrôle de gestion.

Domaine du contrôle	Intitulé du contrôle	Description du contrôle	Raisons de l'importance
Gouvernance et assurance	1. Surveillance continue	Le fournisseur doit mesurer, vérifier et documenter son respect des présentes dispositions régulièrement, et en aucun cas moins d'une fois par année civile.	Les EUDA nécessitent un soutien de haut niveau afin de s'assurer que les contrôles sont conçus, mis en œuvre et appliqués efficacement. Une surveillance continue est nécessaire pour pouvoir assurer la direction d'une conception et d'une utilisation correctes des contrôles sur les risques liés aux EUDA.
Gouvernance et assurance	2. Respect des exigences législatives et réglementaires	Le fournisseur doit s'assurer que les exigences législatives et réglementaires liées aux EUDA applicables dans la juridiction dans laquelle le fournisseur exerce ses activités sont correctement documentées et respectées.	*(Même remarque que ci-dessus)*
Objectifs du contrôle des EUDA	3. Identification des EUDA	Un processus doit être mis en place et documenté pour identifier toutes les EUDA détenues ou exécutées par le fournisseur sur lesquelles s'appuient les services de Barclays.	L'identification des EUDA est essentielle pour déterminer le niveau de contrôle correct qu'il est nécessaire d'appliquer à l'ensemble des EUDA.

Objectifs du contrôle des EUDA	4. Évaluation de la criticité des EUDA	La criticité de chaque EUDA doit être évaluée avant sa première utilisation en production et avant toute modification. L'évaluation de la criticité menée par le fournisseur doit inclure des éléments tels que les impacts réglementaires, financiers et sur la réputation du service qu'il fournit à Barclays. L'évaluation de la criticité doit impérativement prendre en compte l'importance et la probabilité d'erreur. Veuillez vous reporter à l'annexe C. En ce qui concerne l'importance, les critères pertinents sont notamment : • L'EUDA soutient-elle les activités critiques liées au produit/service fourni à Barclays ? • Le résultat de l'EUDA a-t-il un impact financier pour Barclays ? • Les clients de Barclays peuvent-ils être négativement impactés si les informations, les calculs ou les résultats de l'EUDA sont inexacts, obsolètes ou corrompus ? En ce qui concerne la probabilité d'erreur, les critères pertinents sont notamment : • Complexité perçue de l'EUDA (aucun calcul significatif jusqu'à des formules avancées et complexes de haut niveau) • Fréquence d'utilisation ; • Fréquence des modifications de la formule ou de la logique de l'EUDA ; et • Nombre d'utilisateurs. La criticité des EUDA doit être convenue avec Barclays.	Comprendre la criticité des EUDA peut permettre au fournisseur de déterminer et mettre en œuvre le niveau de contrôle approprié pour les EUDA.
Objectifs du contrôle des EUDA	5. Exigences de contrôle minimales fondées sur la criticité des EUDA	Le fournisseur doit mettre en œuvre des contrôles qui satisfont aux exigences des objectifs de contrôle fondées sur le niveau de criticité convenu avec Barclays. Les objectifs de contrôle pour lesquels est indiquée la mention « O » sont obligatoires en application de la présente annexe. Tous les autres objectifs de contrôle sont uniquement facultatifs (mention « F »). Voir le tableau des contrôles exposé en annexe B	Le niveau de contrôle approprié doit être appliqué d'une manière adaptée au risque que présente l'EUDA, afin d'éviter d'exercer un contrôle excessif sur une EUDA présentant des risques moindres.

		Tous les éléments de preuve permettant de démontrer que les objectifs de contrôle applicables ont été atteints doivent être conservés, le cas échéant.	
Objectifs du contrôle des EUDA	6. Justification des EUDA	Chaque EUDA doit faire l'objet d'une procédure de justification avant sa première utilisation, pour évaluer si l'EUDA est effectivement nécessaire ou si d'autres manières de prendre en charge les processus métiers associés (par ex. passage à un service géré) seraient plus efficaces et/ou poseraient moins de risques que la gestion d'une EUDA. Cette procédure doit être réalisée à la création de l'EUDA (c'est-à-dire avant sa première utilisation), et régulièrement par la suite. Les résultats et justificatifs de cette procédure doivent être conservés et transmis à Barclays avant la première utilisation de l'EUDA, et à chaque fois que la procédure est appliquée par la suite.	La procédure de justification des EUDA offre au fournisseur l'occasion d'évaluer si l'EUDA est effectivement nécessaire.
Objectifs du contrôle des EUDA	7. Enregistrement des EUDA	Un inventaire des EUDA doit être mis en place en vue d'offrir au fournisseur une vision transparente et exhaustive du groupe des EUDA concerné et d'enregistrer les attributs clés nécessaires à l'appui des dispositions de la présente annexe. Un processus doit être documenté et mis en place pour assurer l'existence d'un inventaire complet, exact et à jour des EUDA. L'inventaire des EUDA doit être révisé au moins une fois par an pour en assurer l'exactitude et en vérifier l'exhaustivité.	L'exhaustivité de l'inventaire des EUDA est essentielle pour s'assurer que les EUDA présentent le niveau de sécurité adéquat et fonctionnent correctement.
Objectifs du contrôle des EUDA	8. Accès	L'accès aux données et à la logique commerciale de tous les EUDA doit être limité aux utilisateurs appropriés disposant des droits d'accès adéquats. L'accès doit être vérifié suivant une approche fondée sur les risques.	L'existence de contrôles appropriés de l'accès protège les EUDA contre tout accès non autorisé, inapproprié ou non susceptible d'être rattaché à une personne donnée.
Objectifs du contrôle des EUDA	9. Disponibilité	Des contrôles doivent être mis en place pour assurer que les EUDA sont disponibles conformément aux exigences convenues avec Barclays.	La disponibilité des EUDA assure la continuité de l'application des processus commerciaux.

Objectifs du contrôle des EUDA	10. Gestion des modifications	Le respect des principes de gestion des modifications permet de s'assurer que les EUDA fonctionnent comme prévu à la suite de changements de la logique commerciale. Les modifications apportées à la logique commerciale de l'EUDA ou aux données statiques clés ne doivent pas entraîner d'erreurs de sortie ou de rapport. Les utilisateurs de l'EUDA ne doivent pouvoir accéder qu'aux versions pertinentes de l'EUDA à des fins opérationnelles. L'exhaustivité et l'exactitude des données d'entrée, des calculs et des données de sortie sont validées par des tests (automatisés et/ou manuels) afin de s'assurer que les modifications apportées ont produit le résultat escompté. Les étapes de test doivent être identifiées et convenues avec Barclays pour toute EUDA dont la criticité est déterminée comme « Moyenne » ou « Élevée » lors de l'évaluation de la criticité de l'EUDA, afin de s'assurer que les modifications n'entraînent pas le signalement d'erreurs. Les versions pour archivage ne doivent pas être stockées au même endroit que la/les version(s) de production. Une seconde personne doit être désignée par le fournisseur pour prendre en charge l'utilisation et la maintenance continue de l'EUDA en l'absence de l'utilisateur principal (ou des utilisateurs principaux).	L'existence d'une gestion des modifications appropriée est cruciale pour que l'EUDA continue à fonctionner de la manière attendue après la mise en œuvre d'une modification.
Objectifs du contrôle des EUDA	11. Exigences relatives à la documentation	La connaissance des entrées, des calculs, des sorties et la capacité de les modifier ne doivent pas être limitées à une seule personne. En outre, il doit exister une documentation appropriée susceptible d'être utilisée par un individu spécifique compétent en matière d'EUDA à des fins de modification et de maintenance de l'EUDA.	L'EUDA étant gérée par les utilisateurs finaux, il est important de disposer d'une documentation adéquate pour garantir la conservation des informations critiques concernant l'EUDA, afin de permettre le transfert de connaissances et la réduction des risques de pertes de connaissances à un minimum.

Annexe A : définitions utilisées par Barclays

Définitions	
EUDA	Les EUDA sont des applications et des outils créés, utilisés et gérés par les utilisateurs finaux. Les EUDA sont généralement développées au moyen de logiciels de bureau standard (Microsoft Excel ou Access, le plus couramment) et d'autres types de bases de données, requêtes, macros, scripts, outils de notification, exécutables et ensembles de codes. Les EUDA exécutent ou font partie d'un processus commercial sur une base continue (et non pas une utilisation ponctuelle), qui, si ses calculs ou ses résultats sont inexacts, indisponibles, périmés ou corrompus, pourrait avoir un impact financier, réglementaire ou de réputation pour la Banque ou pourrait causer un préjudice au client.

Annexe B : exigences de contrôle minimales

L'applicabilité de chaque contrôle est déterminée par le tableau suivant (F = Facultatif, O = Obligatoire) :

Intitulé du contrôle	Criticité de l'EUDA			
	Très faible	Faible	Moyenne	Élevée
1. Rôles et responsabilités	O	O	O	O
2. Signalement des risques d'information	O	O	O	O
3. Surveillance continue	O	O	O	O
4. Respect des exigences législatives et réglementaires locales	O	O	O	O
5. Formation et sensibilisation aux EUDA	O	O	O	O
6. Identification des EUDA	O	O	O	O
7. Évaluation de la criticité des EUDA	O	O	O	O
8. Exigences de contrôle minimales fondées sur la criticité des EUDA	O	O	O	O
9. Justification des EUDA	O	O	O	O
10. Enregistrement des EUDA	F	O	O	O
11. Accès	F	O	O	O
12. Disponibilité	F	F	O	O
13. Gestion des changements	F	F	O	O
14. Exigences relatives à la documentation	F	F	F	O

Annexe C : Évaluation de la criticité des EUDA

L'évaluation de la criticité des EUDA se compose de deux sous-évaluations. Les utilisateurs principaux des EUDA doivent réaliser ces deux sous-évaluations pour en déterminer la criticité.

- Évaluation de l'importance de l'EUDA pour Barclays
- Évaluation de la probabilité d'erreur de l'EUDA

L'importance d'une EUDA correspond à la note la plus élevée obtenue pour les critères ci-dessous.

Importance de l'EUDA Critère 1	**Note de l'importance de l'EUDA**			
	Faible	**Moyenne**	**Élevée**	**Exceptionnelle**
1) L'EUDA prend-elle en charge les activités critiques ayant un impact réglementaire (actifs pondérés en fonction des risques équivalents 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 les rapports financiers ?	Impact pertes et profits < 1 M£ Impact bilan comptable < 1 Mrd£	Impact pertes et profits ≥ 1 M£ < 10 M£ Impact bilan comptable ≥ 1 Mrd£ < 2 Mrd£	Impact pertes et profits ≥ 10 M£ < 50 M£ Impact bilan comptable ≥ 2 Mrd£ < 3 Mrd£	Impact pertes et profits ≥ 50 M£ Impact bilan comptable > 3 Mrd£
3) Si les informations, les calculs ou les résultats de l'EUDA étaient inexacts, obsolètes ou corrompus, quel serait l'impact **probable** sur les clients de la banque ?	Préjudice pour les clients < 100 Perte consolidée clients < 1 M£	Préjudice pour les clients ≥ 100 < 1 000 Perte consolidée clients ≥ 1 M£ < 10 M£	Préjudice pour les clients ≥ 1000 < 10000 Perte consolidée clients ≥ 10 M£ < 50 M£	Préjudice pour les clients ≥ 10000 < 50000 Perte consolidée clients ≥ 50 M£
4) Si les informations, les calculs ou les résultats de l'EUDA étaient inexacts, obsolètes ou corrompus, quel serait l'impact **probable** sur la réputation de la banque ?	Impact jugé comme non significatif au niveau d'une unité commerciale locale . Aucun impact sur la marque ou la réputation du groupe.	Impact jugé comme gérable au niveau d'une unité commerciale locale . Aucun impact sur la marque ou la réputation du groupe.	Préjudice pour plusieurs entités/régions. Impact improbable sur la marque du groupe.	Impact probable sur la marque du groupe

L'utilisateur principal de l'EUDA doit évaluer la probabilité d'erreur de l'EUDA à l'aide des critères ci-dessous. L'utilisateur principal de l'EUDA doit rassembler les scores des critères pour calculer la probabilité d'erreur finale.

Critères de probabilité d'erreur de l'EUDA	Probabilité d'erreur			
	Un	**Deux**	**Trois**	**Quatre**
1) Quelle est la complexité perçue de l'EUDA ? (voir définition ci-dessous*)	Rudimentaire	Faible	Moyenne	Élevée
2) Quelle est la fréquence d'utilisation de l'EUDA ?	Moins d'une fois par trimestre	Plus d'une fois par trimestre, mais moins d'une fois par mois	Plus d'une fois par mois, mais moins d'une fois par jour	Plus d'une fois par jour
3) Quelle est la fréquence des modifications de la formule ou de la logique de l'EUDA ?	Jamais ou très rarement	Des modifications sont apportées exceptionnellement	Des modifications sont apportées régulièrement, mais pas à chaque utilisation de l'EUDA	Chaque fois que l'EUDA est utilisée
4) Combien d'utilisateurs sont associés à l'EUDA ?	Un seul utilisateur	Plusieurs utilisateurs de la même équipe opérationnelle	Plusieurs utilisateurs de différentes équipes au sein d'une même fonction ou unité commerciale	Plusieurs utilisateurs au sein de différentes fonctions et/ou unités commerciales

* Renvoie à la fonctionnalité de l'EUDA ; la classification est la suivante :

- **Rudimentaire** : aucun calcul significatif dans l'EUDA. Principalement utilisée comme rapport de synthèse.
- **Faible** : un réviseur avec une connaissance limitée de l'application peut interpréter le but et l'efficacité des formules en les observant et sans explications extérieures.
- **Moyenne** : possède des fonctionnalités plus complexes. Un réviseur qui maîtrise l'application (par ex. Excel ou Access) peut avoir besoin d'informations supplémentaires pour interpréter le but et l'efficacité de l'EUDA.

- **Élevée** : haut niveau de complexité et formules avancées. Peut également être liée à d'autres feuilles de calcul, bases de données, sites Web, tableaux, etc.

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

Probabilité d'erreur	**Improbable**	**Possible**	**Probable**	**Très probable**
Score agrégé	≥ 4 < 6	≥ 6 < 9	≥ 9 < 12	≥ 12 ≤ 16

Évaluation de la criticité des EUDA

L'utilisateur principal de l'EUDA doit combiner les évaluations de l'importance 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.

Importance	Exceptionnelle	**Moyenne**	**Moyenne**	**Élevée**	**Élevée**
	Élevée	**Moyenne**	**Moyenne**	**Moyenne**	**Élevée**
	Moyenne	**Faible**	**Faible**	**Moyenne**	**Moyenne**
	Faible	**Très faible**	**Très faible**	**Très faible**	**Très faible**
Probabilité d'erreur		Improbable	Possible	Probable	Très probable