外部サプライヤー管理義務

EUDA – エンドユーザー開発アプリケーション

2019 年 4 月付け　第 9.0 版

本 SCO（サプライヤー管理義務）内で述べる「EUDA」とは、Barclays の EUDA 決定木を通して特定される EUDA にのみ適応するものであり、サプライヤーが Barclays に提供するサービスをサポートするために使用されるものです。

管理領域	管理項目	管理内容	本件が重要である理由
ガバナンスと保証	1. 役職と責務	サプライヤーは、EUDA に対する役職と責務を定義し、周知しなければなりません。 サプライヤーの業務モデルや事業に対して重大な変更を行った後で、この件に関する見直しを実施しなければなりません。 主要な役職には、EUDA に対して責任を負う上級役員を含む必要があります。	EUDA は、管理者が効果的に計画、実行、実施されることを徹底するために、上級管理職レベルの支援を必要とします。 現行モニタリングは、上級管理に情報リスク管理の計画と運用に関する保証を提供するために必要です。
ガバナンスと保証	2. 情報リスク報告	書面管理とプロセスは、EUDA リスクインシデントを確実に報告、管理するために設定しなければなりません。 EUDA インシデントと情報漏えいはサプライヤーが対応を行い、迅速に Barclays へ報告されるべきものです。Barclays の情報および Barclays の使用するサービスに影響を及ぼすエラーの適時処理と報告のための、Barclays インシデント回答プロセスを設立すべきです。 サプライヤーは、インシデントに続く特定された是正措置が、改善計画（アクション、帰属、実行日）にしたがって取り扱われ、Barclays と共有、および同意することを保証しなければなりません。	
ガバナンスと保証	3. 現行モニタリング	サプライヤーは、定期的に、いかなる場合でも 1 年に 1 回以上の頻度で、本付属書にしたがって遵守状況を測定、再調査、および記録しなければなりません。	
ガバナンスと保証	4. 現地の法令および法定基準の遵守	サプライヤーは、サプライヤーが運用を行う管轄権に適用される法令および法定基準に関連した EUDA を、適切に記録、および遵守しなければなりません。	*（上記と同様）*

ガバナンスと保証	5. EUDA の教育および啓発	サプライヤーは、従業員を EUDA の責務に割り当てる必要があります。 EUDA の役職を任命された従業員は、その役職に適応する教育および啓発研修を完了しなければなりません。 この管理業務は、少なくとも 1 年に 1 回の頻度で実施し、これを実証するための証明書を保管しなければなりません。	
EUDA 管理目標	6. EUDA 識別	サプライヤーの所有権すべてを識別し、または Barclays サービスをサポートする EUDA を実行するために、プロセスは記録され、配置されなければなりません。	EUDA の識別は、すべての EUDA に必要な管理の正確なレベルを決定する際に最重要な項目となります。
EUDA 管理目標	7. EUDA クリティカリティ評価	それぞれの EUDA クリティカリティは、製造で最初に使用される前、および各 EUDA の変更が実施される前に評価しなければなりません。 サプライヤーのクリティカリティ評価では、サプライヤーが Barclays へ提供するサービスに対する、規制、財務、風評への影響を考慮すべきです。 クリティカリティ評価では、エラーの重要性と発生見込みについても考慮すべきです。 添付資料 C を参照してください 重要性という観点には、以下の関連基準が含まれます: • EUDA は、Barclays へ提供される製品やサービスに関連したクリティカル・アクティビティをサポートしていますか？ • EUDA のアウトプットには、Barclays に対する財務影響を含むことができますか？ • 情報、見積もり、EUDA のアウトプットが正確でなかったり、期限切れや不正があった場合、Barclays のカスタマーが不利益を被ることはありますか？ エラーの発生見込みという観点には、以下の関連基準が含まれます: • EUDA において認識された複雑性（複雑で高度な数式レベルまで有意な計算ではない）、 • 使用頻度、 • EUDA の数式や理論の変更頻度、および • 使用者数。	EUDA クリティカリティの理解は、当社のサプライヤーが EUDA のための適切な管理レベルを決定し、実行することを可能にします。

		EUDA クリティカリティは、Barclays と合意していなければなりません。	
EUDA 管理目標	8. EUDA クリティカリティに基づいた最低管理要件	サプライヤーは、Barclays と合意したクリティカリティ・レベルに基づいた管理目標の要件を満たすよう、管理を実行しなければなりません。 「M」とマークされた管理目標は、本付属書による命令事項です。その他の全管理目標は、オプションの「O」のみです。添付資料 B の管理表をご確認ください。 適用する管理目標が達成されたことを実証するため、証明書は適切な場所へ保管しなければなりません。	管理の適正なレベルは、EUDA リスクが低い場合の過剰な管理を避けるため、EUDA によって表されるリスクに合わせて適用しなければなりません。
EUDA 管理目標	9. EUDA の正当性	それぞれの EUDA は、初めて使用する前に正当性評価手続きを経るべきであり、これにより本件が必要であるか、または事業プロセスに関してサポートする代替え手段（例えば、管理サービスへの移行）の方がより効果的であったり、EUDA を継続するよりもリスクを低減できるのではないかを評価します。 EUDA の正当性評価手続きは、EUDA が最初に作成されたとき（最初に使用する前）に行うべきであり、その後も定期的に再度実行すべきものです。 正当性評価手続きの成果と証明は保管する必要があり、また EUDA を最初に使用する前、およびその後も本手続きが実施されるときにはいつでも、Barclays に対して通知しなければなりません。	EUDA 正当性評価手続きを理解することにより、サプライヤーに対し、EUDA 管理目標が本当に必要であるかどうかを評価する機会を与えます。
EUDA 管理目標	10. EUDA 登録	EUDA 一覧は、サプライヤーに対して EUDA 母集団範囲での完了に対する透明性を提供し、本付属書の規定をサポートする主要な特性を捉えるために存在するべきものです。 プロセスは記録し、EUDA 一覧を完全、正確、最新の状態に確保するために実施しなくてはなりません。EUDA 一覧は、正確性を維持し、完全性を検証するために、少なくとも 1 年に 1 度の見直しを実施しなければなりません。	EUDA 一覧の完全性は、EUDA の適切な信頼と運用を確かなものとするための基盤となるものです。
EUDA 管理目標	11. アクセス	すべての EUDA のためのデータとビジネス・ロジックへのアクセスは、しかるべきアクセス権を持つ適切なユーザーに限定しなくてはなりません。アクセスは、リスクベースアプローチを使って見直さなくてはなりません。	適切なアクセス管理は、不正で、不適切な、特定できないアクセスから EUDA を守ります。

EUDA 管理目標	12. 可用性	EUDA が Barclays との合意による要件にしたがって利用できるよう、管理を確実にしなければなりません。	EUDA の可用性は、継続的な事業プロセスの実施を確実にします。
EUDA 管理目標	13. 変更管理	変更管理の基本方針に従うことで、EUDA がビジネス・ロジックの変更に続いて期待されるように動作することを確実にします。 EUDA のビジネス・ロジックや主要な静的データの変更が、エラーのアウトプットや報告の原因とならないようにしなければなりません。EUDA のユーザーは、運用目的のための EUDA の該当するバージョンにのみアクセスできるようにしなければなりません。 データのインプット、計算およびデータのアウトプットの完全性と正確性は、適用された変更が期待された結果を生じることを確認するための試験（自動式、またはマニュアル）を通して実証されます。 変更がエラーの報告という結果を生まないようにするため、試験段階では、EUDA クリティカリティ評価で中から高までランク付けされたあらゆる EUDA を特定し Barclays と合意するべきです。 アーカイブ・バージョンは、プロダクション・バージョンと同じ場所に保存してはいけません。 1 次ユーザーが不在の際に EUDA の現行使用とメンテナンスをサポートするため、2 次ユーザーがサプライヤーによって指名されなければなりません。	適切な変更管理は、いかなる変更後であっても期待通りに機能を継続させるための EUDA の根幹となります。
EUDA 管理目標	14. 記録要件	入力、計算、出力に関する知識およびこれらの修正能力は、1 人に限定されるべきものではありません。 加えて EUDA を変更および維持する特定の EUDA 熟練者が使用できるよう、十分記録が必要不可欠です。	EUDA がエンドユーザーによって管理されることから、知識の移行と知識損失のリスクを最小限度にするために、EUDA に関するクリティカル情報を確保する十分な記録が重要となります。

添付資料 A: Barclays によって使用される定義

定義	
EUDA	EUDA とは、エンドユーザーが作成、使用、管理するアプリケーションおよびツールのことです。これらは、標準的なデスクトップ・ソフトウェア（最も一般的に Microsoft Excel や Access）やその他のデータベース、クエリ、マクロ、スクリプト、レポートツール、実行可能ファイル、コードパッケージのタイプを使用して一般的に開発されたものです。 EUDA は実行または継続中の事業プロセス（一度限りではない）の一環であり、その計算やアウトプットが不正確、利用不可、期限切れ、または破損している場合には、銀行に対する財務、規制または風評への影響を与える可能性、もしくは顧客へ損害を与える可能性もあります。

添付資料 B: 最小管理要件

各管理の適用性は、以下の表にしたがって決定されます。(O = オプション、M = 必須):

管理項目	EUDA クリティカリティ格付け			
	とても低い	低	中	高
1. 役職と責務	M	M	M	M
2. 情報リスク報告	M	M	M	M
3. 現行モニタリング	M	M	M	M
4. 現地法令および法定基準の遵守	M	M	M	M
5. EUDA の教育および啓発	M	M	M	M
6. EUDA 識別	M	M	M	M
7. EUDA クリティカリティ評価	M	M	M	M
8. EUDA クリティカリティに基づいた最低管理要件	M	M	M	M
9. EUDA の正当性	M	M	M	M
10. EUDA 登録	O	M	M	M
11. アクセス	O	M	M	M
12. 可用性	O	O	M	M
13. 変更管理	O	O	M	M
14. 記録要件	O	O	O	M

添付資料 C: EUDA クリティカリティ評価

EUDA クリティカリティ評価には 2 つのサブ評価が含まれます。EUDA の 1 次ユーザーは、EUDA クリティカリティを決定するために両方のサブ評価を実施する必要があります。

- Barclays にとっての EUDA の重要性の評価
- EUDA のエラーの発生見込みの評価。

個々の EUDA の重要性は、以下の基準により得られた最も高い格付けと定義されます

EUDA の重要性 基準 1	**EUDA 重要性格付け**			
	低い	**中**	**高い**	**極めて高い**
1) EUDA は規制上の影響を与えるクリティカル・アクティビティをサポートしているか(リスク加重資産 (RWA) 相当または EUDA により直接影響を受けるエクスポージャー)?	£5000 万未満	£5000 万以上£5 億未満	£5 億以上£10 億以下	£10 億超
2) EUDA のアウトプットは財務報告に影響を与えるか?	P&L への影響 £100 万未満 BS への影響 £10 億未満	P&L への影響 £100 万以上 £1000 万未満 BS への影響 £10 億以上£20 億未満	P&L への影響 £1000 万以上 £5000 万未満 BS への影響 £20 億以上£30 億以下	P&L への影響 £5000 万以上 BS への影響 £30 億超
3) EUDA の情報、見積もり、アウトプットが正確でなかったり、期限切れや不正があった場合、破損していた場合、銀行の顧客に対してどのような影響が及ぶ**可能性**があるか?	影響を受ける顧客数 100 未満 顧客損失合計 £100 万未満	影響を受ける顧客数 100 以上 1000 未満 顧客損失合計 £100 万以上 £1000 万未満	影響を受ける顧客数 1000 以上 10000 未満 顧客損失合計 £1000 万以上 £5000 万未満	影響を受ける顧客数 10000 以上 50000 未満 顧客損失合計 £5000 万以上
4) EUDA の情報、見積もり、アウトプットが正確でなかったり、期限切れや不正があった場合、銀行の評判に対してどのような影響が及ぶ**可能性**があるか?	現地の事業部門レベルでは重大ではないと判断される影響。グローバルブランドまたは評判に対する影響はない。	現地の事業部門レベルで対処可能であると判断される影響が発生する可能性がある。グローバルブランドまたは評判に対する影響はない。	複数のビジネス/地域に悪影響が及ぶ可能性がある グループブランドに影響が及ぶ可能性はまずない。	グループブランドに影響が及ぶ可能性がある。

EUDA の 1 次ユーザーは、以下の基準を使用し、EUDA のエラー発生見込みを評価する必要があります。EUDA の 1 次ユーザーは、エラー発生見込みの最終的な格付けを計算するため、すべての基準のスコアを集計する必要があります。

EUDA のエラー発生見込みの基準	エラー発生見込みスコア			
	1	2	3	4
1) EUDA において認識された複雑性は？（以下の定義を参照*）	極めて低い	低い	中	高い
2) EUDA の使用頻度は？	四半期に 1 回未満	四半期に 1 回または 2 回、ただし月に 1 回未満	月に 1 回またはそれ以上、ただし毎日ではない	1 日に 1 回または複数回
3) EUDA の数式/理論の変更頻度は？	1 回未満または非常に稀である	変更は行われるが、例外的な場合である	定期的に変更されるが、EUDA が使用されるたびに毎回ではない	EUDA が使用されるたびに毎回
4) EUDA の使用者数は？	1 人	同一の業務運営チーム内の複数のユーザー	事業単位または部門内の複数のチームの複数のユーザー	複数の事業単位および/または複数の部門の複数のユーザー

*EUDA の機能性を指し、分類は以下の通りです：

- **極めて低い** –EUDA での重要な計算はない。主に要約レポートとして使用される。
- **低い** – 限られたアプリケーションの知識を持つレビューアーが、外部からの説明なしに、観察を通じて公式の目的と効果を解釈することができる。
- **中** –より複雑な機能性。アプリケーション（Excel、Access など）の使用に精通するレビューアーが、EUDA の目的と効果を解釈するための追加情報を必要とする場合がある。

- **高い** – 高度な複雑性と高度な数式。他のスプレッドシート、データベース、ウェブサイト、表などとリンクしている場合がある。

エラー発生見込みの最終的な格付けは、合計スコアを以下の表に適用して計算します:

エラー発生見込みの格付け	**低い**	**中**	**高い**	**非常に高い**
合計スコア	4 以上 6 未満	6 以上 9 未満	9 以上 12 未満	12 以上 16 以下

EUDA クリティカリティ評価

EUDA の 1 次ユーザーは、重要度とエラー発生見込みを統合し、全体的な EUDA のクリティカリティを決定する必要があります。決定には以下の表を使用します。EUDA の 1 次ユーザーは、EUDA クリティカリティ評価を EUDA インベントリーに記録します。

重要性	極めて高い	**中**	**中**	**高**	**高**
	高い	**中**	**中**	**中**	**高**
	中	**低**	**低**	**中**	**中**
	低い	**非常に低い**	**非常に低い**	**非常に低い**	**非常に低い**
エラー発生見込み		低い	中	高い	非常に高い