Kontrollpflichten externer Lieferanten

EUDA – von Endbenutzern entwickelte Anwendungen (End User Developed Applications)

Version 11.0, Oktober 2021

Bitte beachten Sie, dass sich der Begriff „EUDA“, wie er in dieser SCO verwendet wird, nur auf EUDAs, die innerhalb des EUDA-Entscheidungsbaums von Barclays identifiziert wurden, und solche bezieht, die den/die vom Lieferanten für Barclays erbrachten Dienst(e) unterstützen.

Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
Geschäfts- und Sicherheitskontrollen	1. Funktionen und Verantwortlichkeiten	Der Lieferant muss Funktionen und Verantwortlichkeiten für EUDAs festlegen und kommunizieren. Diese müssen nach jeder wesentlichen Änderung am Betriebsmodell oder Geschäft des Lieferanten überprüft werden. Zu den Hauptfunktionen muss ein leitender Angestellter gehören, der für EUDAs zuständig ist.	EUDAs erfordern ein Sponsorship auf höherer Ebene, um sicherzustellen, dass Kontrollmechanismen entwickelt, implementiert und effektiv umgesetzt werden. Um die Geschäftsleitung hinreichend über die Entwicklung und den Ablauf der EUDA -Risikokontrollen in Kenntnis zu setzen, ist eine fortlaufende Überwachung nötig.
Geschäfts- und Sicherheitskontrollen	2. EUDA-Risikoberichterstattung	Um sicherzustellen, dass EUDA-Risikovorfälle gemeldet und verwaltet werden, müssen dokumentierte Kontrollmechanismen und Prozesse vorhanden sein. Der Lieferant sollte EUDA-Vorfälle und Datenschutzverletzungen unverzüglich behandeln und Barclays melden. Es sollte ein Vorfallbehandlungsprozess für die zeitnahe Bearbeitung und Meldung von Fehlern, die Auswirkungen auf Informationen von Barclays und/oder auf von Barclays genutzte Dienste haben, eingerichtet sein. Der Lieferant muss dafür sorgen, dass die festgelegten Abhilfemaßnahmen nach einem Vorfall gemäß einem Abhilfeplan (Aktion, Zuständigkeit, Frist) ausgeführt und mit Barclays abgesprochen und vereinbart werden.	
Geschäfts- und Sicherheitskontrollen	3. Fortlaufende Überwachung	Der Lieferant muss regelmäßig (mindestens jedoch einmal in jedem Kalenderjahr) seine Einhaltung dieses Zeitplans messen, auswerten und dokumentieren.	

Geschäfts- und Sicherheitskontrollen	4. Einhaltung der rechtlichen und gesetzlichen Bestimmungen vor Ort	Der Lieferant stellt sicher, dass auf EUDA bezogene gesetzliche wie satzungsmäßige Bestimmungen des Geltungsbereichs, in welchem der Lieferant arbeitet, angemessen dokumentiert sind und eingehalten werden.	*(siehe oben)*
Geschäfts- und Sicherheitskontrollen	5. EUDA-Weiterbildung und -Awareness	Der Lieferant muss Mitarbeiter mit EUDA-Verantwortlichkeiten benennen. Mitarbeiter, denen eine EUDA-Funktion zugewiesen wurde, müssen an einer für ihre Funktion geeigneten Weiterbildung und Awareness-Schulung teilnehmen. Diese Kontrollmaßnahme sollte mindestens einmal jährlich durchgeführt werden und ein entsprechender Nachweis ist aufzubewahren.	
EUDA-Kontrollziele	6. EUDA-Identifizierung	Es muss ein Prozess zur Identifizierung sämtlicher im Besitz des Lieferanten befindlichen bzw. von diesem betriebenen EUDAs, die Dienste von Barclays unterstützen, dokumentiert und vorhanden sein.	Die Identifizierung von EUDAs ist von oberster Bedeutung für die Bestimmung der richtigen Kontrollstufe für sämtliche EUDAs.
EUDA-Kontrollziele	7. EUDA-Kritikalitätsbewertung	Vor ihrem ersten Einsatz in der Produktion und vor Umsetzung beliebiger Änderungen an einer EUDA muss die Kritikalität jeder EUDA bewertet werden. In die Kritikalitätsbewertung des Lieferanten sollten Überlegungen zu Faktoren einfließen, wie die regulatorischen, finanziellen und reputationsspezifischen Auswirkungen des Dienstes, den der Lieferant für Barclays erbringt. Bei der Kritikalitätsbewertung sollte zudem auch die Tragweite und Wahrscheinlichkeit von Fehlern berücksichtigt werden. Lesen Sie hierzu bitte Anhang C.	Ein Verständnis der EUDA-Kritikalität kann es unserem Lieferanten ermöglichen, eine geeignete Kontrollstufe für die EUDA zu bestimmen und zu implementieren.

		In Bezug auf die Tragweite lauten die relevanten Kriterien beispielsweise: • Unterstützt die EUDA kritische Aktivitäten in Verbindung mit dem Barclays angebotenen Produkt bzw. Dienst? • Kann das Ergebnis der EUDA finanzielle Auswirkungen für Barclays haben? • Können Barclays-Kunden negativ beeinflusst werden, wenn die Informationen, Berechnungen oder Ergebnisse der EUDA ungenau, nicht aktuell oder fehlerhaft wären? In Bezug auf die Fehlerwahrscheinlichkeit lauten die relevanten Kriterien beispielsweise: • Wahrgenommene Komplexität der EUDA (keine signifikanten Berechnungen bis hin zu einem hohen Maß komplexer und fortschrittlicher Formeln); • Nutzungshäufigkeit, • Häufigkeit von Änderungen an der Formel/Logik der EUDA, und • Anzahl der Benutzer. Die Kritikalität der EUDA muss mit Barclays vereinbart werden.	
EUDA-Kontrollziele	8. Mindestanforderungen an Kontrollen ausgehend von der Kritikalität der EUDA	Der Lieferant muss Kontrollen implementieren, die den Anforderungen der Kontrollziele ausgehend von der mit Barclays vereinbarten Kritikalitätsstufe entsprechen. Die mit „V“ gekennzeichneten Kontrollziele sind gemäß diesem Dokument als Verbindlich vorgeschrieben. Alle anderen Kontrollziele sind nur Optional („O“). Die Übersicht zu Kontrollen ist Anhang B zu entnehmen. Es sind gegebenenfalls Nachweise aufzubewahren, um zu zeigen, dass die betreffenden Kontrollziele erreicht werden.	Entsprechend dem Risiko, mit dem die EUDA verbunden ist, muss die richtige Kontrollstufe angewendet werden, damit die Kontrollen bei einer EUDA mit geringerem Risiko nicht zu umfangreich sind.
EUDA-Kontrollziele	9. EUDA-Begründung	Jede EUDA sollte vor ihrer ersten Verwendung ein Begründungsverfahren durchlaufen, um zu beurteilen, ob sie notwendig ist oder ob alternative Mittel zur Unterstützung des jeweiligen	Mit der Durchführung eines EUDA-Begründungsverfahrens erhält der Lieferant die Möglichkeit zu beurteilen, ob die EUDA noch immer benötigt wird.

		Geschäftsprozesses (z. B. Umstellung auf einen Managed Service) effizienter und/oder weniger riskant als eine EUDA wären. Das EUDA-Begründungsverfahren muss zunächst bei der erstmaligen Entwicklung einer EUDA (d. h. vor ihrer ersten Verwendung) und danach in regelmäßigen Abständen erneut durchgeführt werden. Das Ergebnis und der Nachweis des Begründungsverfahrens müssen aufbewahrt und Barclays vor der ersten Verwendung der EUDA sowie bei jeder späteren Durchführung des Verfahrens vorgelegt werden.	
EUDA-Kontrollziele	10. EUDA-Registrierung	Zur Schaffung von Transparenz hinsichtlich des Gesamtbestands der im Geltungsbereich liegenden EUDAs für den Lieferanten und zur Erfassung wichtiger Merkmale in Bezug auf die Einhaltung der Bestimmungen dieses Dokuments muss eine EUDA-Bestandsliste vorhanden sein. Es muss ein Prozess dokumentiert und vorhanden sein, um sicherzustellen, dass die Bestandsliste der EUDAs vollständig, genau und aktuell ist. Die EUDA-Bestandsliste muss mindestens einmal jährlich auf Genauigkeit und Vollständigkeit überprüft werden.	Die Vollständigkeit der EUDA-Bestandsliste ist von grundlegender Bedeutung, damit die erforderliche Sicherheit und die Funktion von EUDAs gewährleistet sind.
EUDA-Kontrollziele	11. Zugriff	Der Zugriff auf Daten und Geschäftslogik für sämtliche EUDAs muss auf die entsprechenden Benutzer mit den entsprechenden Zugriffsrechten beschränkt sein. Der Zugriff muss anhand eines risikobasierten Ansatzes überprüft werden.	Entsprechende Zugriffskontrollen schützen EUDAs vor unbefugtem, unangemessenem oder nicht zuordenbarem Zugriff.
EUDA-Kontrollziele	12. Verfügbarkeit	Es müssen Kontrollen vorhanden sein, um sicherzustellen, dass EUDAs im Einklang mit den mit Barclays vereinbarten Anforderungen zur Verfügung stehen müssen.	Durch die Verfügbarkeit von EUDAs wird die kontinuierliche Funktion von Geschäftsprozessen sichergestellt.
EUDA-Kontrollziele	13. Änderungsmanagement	Durch die Beachtung von Prinzipien des Änderungsmanagements wird sichergestellt, dass EUDAs nach Änderungen der Geschäftslogik wie erwartet funktionieren. Änderungen der Geschäftslogik von EUDAs oder von wichtigen statischen Daten dürfen nicht zu Fehlern der Ausgabedaten oder der Berichterstattung führen. Benutzer der EUDA dürfen zu operationellen Zwecken nur auf die relevante(n) Version(en) der EUDA zugreifen können.	Ein angemessenes Änderungsmanagement ist von entscheidender Bedeutung dafür, dass die EUDA nach einer Änderung weiter wie erwartet funktioniert.

		Die Vollständigkeit und Genauigkeit der Eingabedaten, Berechnungen und Ausgabedaten wird durch (automatisierte und/oder manuelle) Tests überprüft, um zu gewährleisten, dass eventuell umgesetzte Änderungen zum gewünschten Ergebnis führen. Für alle EUDAs, deren Kritikalität mit „Mittel" oder „Hoch" bewertet wurde, sollten die Testschritte gemeinsam mit Barclays identifiziert und vereinbart werden, um sicherzustellen, dass sich durch Änderungen keine Fehler in der Berichterstattung ergeben. Archivversionen dürfen nicht am selben Ort gespeichert werden wie die Produktionsversion(en). Zur Unterstützung der fortlaufenden Nutzung und Pflege der EUDA bei Abwesenheit des/der Primärbenutzer(s) muss eine zweite Person benannt werden.	
EUDA-Kontrollziele	14. Dokumentationsanforderungen	Die Kenntnis von Eingabedaten, Berechnungen, Ausgabedaten sowie die Fähigkeit, selbige zu ändern, darf nicht auf eine einzelne Person beschränkt sein. Darüber hinaus muss eine hinreichende Dokumentation vorhanden sein, anhand derer eine Person, die mit einer spezifischen EUDA bewandert ist, die EUDA ändern und warten kann.	Da EUDAs von den jeweiligen Endbenutzern verwaltet werden, ist eine adäquate Dokumentation wichtig, um zu gewährleisten, dass kritische Informationen über die EUDA aufbewahrt und somit der Wissensaustausch ermöglicht und das Risiko von Datenverlusten minimiert werden.

Anhang A: Die von Barclays verwendete Definitionen

Definitionen	
EUDA	EUDAs sind Anwendungen und Tools, die von den Endbenutzern erstellt, genutzt und verwaltet werden. Entwickelt werden diese in der Regel mit Standard-Desktop-Software (meistens Microsoft Excel oder Access) und anderen Arten von Datenbanken, Abfragen, Makros, Skripten, Berichterstattungstools, ausführbaren Dateien und Code-Paketen. EUDAs führen einen Geschäftsprozess fortlaufend aus oder sind Bestandteil eines Geschäftsprozesses (keine nur einmalige Nutzung), was Auswirkungen in finanzieller, regulatorischer oder den Ruf betreffender Hinsicht auf die Bank oder nachteilige Folgen für den Kunden haben könnte, falls Berechnungen oder Ausgabedaten von EUDAs ungenau, nicht verfügbar, nicht aktuell oder fehlerhaft sind.

Anhang B: Mindestanforderungen an Kontrollen

Die Anwendbarkeit jeder Kontrolle wird anhand der folgenden Tabelle bestimmt (O = Optional und V = Verbindlich):

Bezeichnung der Kontrolle	EUDA-Kritikalitätsbewertung			
	Sehr gering	Gering	Mittel	Hoch
1. Funktionen und Verantwortlichkeiten	V	V	V	V
2. EUDA-Risikoberichterstattung	V	V	V	V
3. Fortlaufende Überwachung	V	V	V	V
4. Einhaltung der rechtlichen und gesetzlichen Bestimmungen vor Ort	V	V	V	V
5. EUDA-Weiterbildung und -Awareness	V	V	V	V
6. EUDA-Identifizierung	V	V	V	V
7. EUDA-Kritikalitätsbewertung	V	V	V	V
8. Mindestanforderungen an Kontrollen ausgehend von der Kritikalität der EUDA	V	V	V	V
9. EUDA-Begründung	V	V	V	V
10. EUDA-Registrierung	O	V	V	V
11. Zugriff	O	V	V	V
12. Verfügbarkeit	O	O	V	V
13. Änderungsmanagement	O	O	V	V
14. Dokumentationsanforderungen	O	O	O	V

Anhang C: EUDA-Kritikalitätsbewertung

Die EUDA-Kritikalitätsbewertung umfasst zwei Unterbewertungen; EUDA-Primärbenutzer müssen beide Unterbewertungen vornehmen, um die Kritikalität der EUDA zu bestimmen.

- Eine Bewertung der Tragweite der EUDA für Barclays.
- Eine Bewertung der Fehlerwahrscheinlichkeit der EUDA.

Die Tragweite jeder einzelnen EUDA ist definiert als die höchste Bewertung, die anhand der folgenden Kriterien vergeben wurde

EUDA-Tragweite Kriterien[1]	**EUDA-Tragweitenbewertung**			
	Gering	**Mittel**	**Hoch**	**Außerordentlich**
1) Unterstützt die EUDA kritische Aktivitäten mit regulatorischen Auswirkungen (äquivalent zu risikogewichteten Ressourcen [RWA] oder direkt durch die EUDA beeinflusste Exposition)?	<50 Mio. £	≥50 Mio. £ ≤500 Mio. £	≥500 Mio. £ ≤1 Mrd. £	>1 Mrd. £
2) Hat das Ergebnis der EUDA Auswirkungen auf die Finanzberichterstattung von Barclays?	GuV-Auswirkungen <1 Mio. £ BS-Auswirkungen <1 Mrd. £	GuV-Auswirkungen ≥1 Mio. £ <10 Mio. £ BS-Auswirkungen ≥1 Mrd. £ <2 Mrd. £	GuV-Auswirkungen ≥10 Mio. £ <50 Mio. £ BS-Auswirkungen ≥2 Mrd. £ ≤3 Mrd. £	GuV-Auswirkungen ≥50 Mio. £ BS-Auswirkungen >3 Mrd. £
3) Wenn die Informationen, Berechnungen oder Ergebnisse der EUDA ungenau, nicht aktuell oder fehlerhaft wären, welche Auswirkungen hätte dies **wahrscheinlich** auf die Kunden der Bank[2]?	Betroffene Kunden < 100 Aggregierte Kundeneinbußen <1 Mio. £	Betroffene Kunden ≥100 <1.000 Aggregierte Kundeneinbußen ≥1 Mio. £ <10 Mio. £	Betroffene Kunden ≥1.000 <10.000 Aggregierte Kundeneinbußen ≥10 Mio. £ <50 Mio. £	Betroffene Kunden ≥10.000 <50.000 Aggregierte Kundeneinbußen ≥50 Mio. £
4) Wenn die Informationen, Berechnungen oder Ergebnisse der EUDA ungenau, nicht aktuell oder fehlerhaft wären, welche Auswirkungen hätte dies **wahrscheinlich** auf die Reputation der Bank?	Als unwesentlich beurteilte Auswirkungen auf Ebene der lokalen Geschäftseinheit. Keine Auswirkungen auf Marke oder Reputation des Unternehmens.	Als handhabbar beurteilte Auswirkungen auf Ebene der lokalen Geschäftseinheit. Keine Auswirkungen auf Marke oder Reputation des Unternehmens.	Nachteilige Auswirkungen auf mehr als eine Geschäftseinheit/Region. Auswirkungen auf die Marke des Unternehmens sind unwahrscheinlich.	Auswirkungen auf die Marke des Unternehmens sind wahrscheinlich.

Der EUDA-Primärbenutzer muss die Fehlerwahrscheinlichkeit der EUDA anhand der nachfolgenden Kriterien bewerten. Der EUDA-Primärbenutzer muss die Wertungen für alle Kriterien aggregieren, um die endgültige Bewertung der Fehlerwahrscheinlichkeit zu berechnen.

Kriterien der EUDA-Fehlerwahrscheinlichkeit	Wertung der Fehlerwahrscheinlichkeit			
	Eins	**Zwei**	**Drei**	**Vier**
1) Wie ist die wahrgenommene Komplexität der EUDA? (siehe Definition unten*)	Rudimentär	Leicht	Mittel	Fortgeschritten
2) Wie häufig wird die EUDA genutzt?	Seltener als ein Mal pro Quartal	Ein Mal pro Quartal oder öfter, aber seltener als ein Mal pro Monat	Ein Mal pro Monat oder öfter, aber nicht täglich	Ein Mal pro Tag oder öfter
3) Wie häufig werden Änderungen an der Formel/Logik der EUDA vorgenommen?	Nie oder sehr selten	Änderungen werden vorgenommen, aber nur in Ausnahmefällen	Regelmäßige Änderungen, aber nicht bei jeder Nutzung der EUDA	Bei jeder Nutzung der EUDA
4) Wie viele Benutzer hat die EUDA?	Einen einzigen Benutzer	Mehrere Benutzer im selben Team	Mehrere Benutzer in unterschiedlichen Teams innerhalb derselben BU oder Funktion	Mehrere Benutzer in unterschiedlichen BUs und/oder Funktionen

*Bezieht sich auf die Funktionalität der EUDA und wird wie folgt kategorisiert:

- **Rudimentär** – Keine signifikanten Berechnungen innerhalb der EUDA. Wird in erster Linie für Zusammenfassungen genutzt.
- **Leicht** – Ein Prüfer mit begrenzten Kenntnissen der Anwendung kann Zweck und Effektivität der Formeln durch Beobachtung und ohne Erklärung von außen deuten.
- **Mittel** – Besitzt eine komplexere Funktionalität. Ein Prüfer, der in der Nutzung der Anwendung (z. B. Excel, Access) geübt ist, benötigt unter Umständen zusätzliche Informationen, um Zweck und Effektivität der EUDA zu deuten.

- **Fortgeschritten** – Hohes Maß an Komplexität und fortgeschrittene Formeln. Kann auch mit anderen Kalkulationstabellen, Datenbanken, Websites, Tabellen usw. verknüpft sein.

Die endgültige Bewertung der Fehlerwahrscheinlichkeit berechnet sich anhand der aggregierten Wertung aus nachstehender Tabelle:

Bewertung der Fehlerwahrscheinlichkeit	**Unwahrscheinlich**	**Möglich**	**Wahrscheinlich**	**Sehr wahrscheinlich**
Aggregierte Wertung	≥4 <6	≥6 <9	≥9 <12	≥12 ≤16

EUDA-Kritikalitätsbewertung

Der EUDA-Primärbenutzer muss die Bewertungen zu Tragweite und Fehlerwahrscheinlichkeit kombinieren, um die Gesamtkritikalität der EUDA zu bestimmen. Die folgende Tabelle ist zu verwenden. Der EUDA-Primärbenutzer muss die EUDA-Kritikalitätsbewertung in der EUDA-Bestandsliste protokollieren.

Tragweite	Außerordentlich	**Mittel**	**Mittel**	**Hoch**	**Hoch**
	Hoch	**Mittel**	**Mittel**	**Mittel**	**Hoch**
	Mittel	**Gering**	**Gering**	**Mittel**	**Mittel**
	Gering	**Sehr gering**	**Sehr gering**	**Sehr gering**	**Sehr gering**
Fehlerwahrscheinlichkeit		Unwahrscheinlich	Möglich	Wahrscheinlich	Sehr wahrscheinlich