BARCLAYS

Pflichten zur Kontrolle externer Lieferanten

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

Version 9.0, April 2019

Bitte beachten Sie, dass der Begriff „EUDA“, der in diesem SCO erwähnt wird, nur für die EUDA gilt, die durch den EUDA-Entscheidungsbaum identifiziert wurden und für diejenigen, die für Dienstleistungen verwendet werden, die der Lieferant für Barclays erbringt.

Kontrollbereich	Kontrolltitel	Kontrollbeschreibung	Warum das wichtig ist
Steuerung und Sicherung	1. Rollen und Verantwortungen	Der Lieferant muss die Aufgaben und Verantwortungen für die EUDAs definieren. Diese müssen nach jeder wesentlichen Änderung am Betriebsmodell oder Geschäft des Lieferanten überprüft werden. Schlüsselpositionen müssen eine Führungskraft beinhalten, die für EUDAs verantwortlich ist.	EUDAs erfordern hochrangiges Sponsorship, um sicherzustellen, dass Kontrollen entworfen, implementiert und effektiv betrieben werden. Laufende Überwachung ist notwendig, um der Geschäftsleitung eine Sicherung über das Design und den Betrieb von Informationsrisikokontrollen bereitzustellen.
Steuerung und Sicherung	2. Information Risk Reporting (Informationsrisikomeldung)	Dokumentierte Kontrollen und Verfahren müssen vorhanden sein, um sicherzustellen, dass EUDA-Risikovorfälle berichtet und bewältigt werden. Auf EUDA-Vorfälle und Verstöße gegen Informationssicherheit muss der Lieferant reagieren und diese sollten sofort an Barclays gemeldet werden. Ein Vorfallsreaktionsverfahren für zeitnahe Handhabung und Meldung von Fehlern, die sich auf Barclays-Informationen und/oder von Barclays genutzte Dienste auswirken, sollte eingerichtet werden. Der Lieferant muss sicherstellen, dass identifizierte Abhilfemaßnahmen nach einem Vorfall mit einem Maßnahmenplan (Aktion, Verantwortung, Lieferdatum) angegangen und Barclays mitgeteilt und mit Barclays abgestimmt werden.	
Steuerung und Sicherung	3. Laufende Überwachung	Der Lieferant muss regelmäßig und auf jeden Fall nicht weniger als einmal pro Kalenderjahr seine Einhaltung mit diesem Plan messen, prüfen und dokumentieren.	

Steuerung und Sicherung	4. Befolgung lokaler gesetzgebender und gesetzlich vorgeschriebener Anforderungen	Der Lieferant muss sicherstellen, dass die gesetzgebenden und gesetzlich vorgeschriebenen Anforderungen bezüglich EUDA, die für das Land gelten, in dem der Lieferant tätig ist, entsprechend dokumentiert und eingehalten werden.	*(wie vorstehend)*
Steuerung und Sicherung	5. EUDA-Ausbildung und –Bewusstsein	Der Lieferant muss Mitarbeiter mit EUDA-Verantwortung identifizieren. Die Mitarbeiter, denen eine EUDA-Funktion zugewiesen ist, müssen die Ausbildung und Bewusstseinsschulung entsprechend ihrer Funktion abschließen. Diese Kontrolle sollte mindestens einmal pro Jahr durchgeführt werden und der Nachweis muss aufbewahrt werden, um dies zu aufzuzeigen.	
EUDA-Kontrollziele	6. EUDA-Identifikation	Ein Verfahren muss dokumentiert und vorhanden sein, um alle EUDAs, die dem Lieferanten gehören, oder vom Lieferanten betrieben werden, zu identifizieren, die Barclays-Dienste unterstützen.	Die Identifikation von EUDAs ist von zentraler Bedeutung bei der Festlegung der richtigen Kontrollstufe, die für alle EUDAs benötigt wird.
EUDA-Kontrollziele	7. EUDA-Kritikalitätsbewertung	Die Kritikalität jeder EUDA muss bewertet werden, bevor sie zum ersten Mal in der betrieblichen Leistung verwendet wird und bevor irgendwelche Änderungen an jeder EUDA implementiert werden. Die Kritikalitätsbewertung des Lieferanten sollte die Berücksichtigung von Elementen, wie aufsichtsrechtliche, finanzielle und Reputationsauswirkungen auf die Dienstleistungen, die der Lieferant an Barclays erbringt, beinhalten. Die Kritikalitätsbewertung sollte auch die Bedeutung und Wahrscheinlichkeit von Fehlern berücksichtigen. Siehe dazu auch Anhang C. Im Sinne der Bedeutung beinhalten die maßgeblichen Kriterien das Folgende: • Unterstützt die EUDA kritische Tätigkeiten in Verbindung mit dem Produkt/der Dienstleistung, die Barclays angeboten wird?	Durch Verständnis der Kritikalität der EUDA kann unser Lieferant die angemessene Kontrollstufe für die EUDA feststellen und implementieren.

		• Kann die Ausgabe der EUDA eine finanzielle Auswirkung auf Barclays haben? • Können Kunden von Barclays negativ betroffen werden, falls die Informationen, Berechnungen oder Ergebnisse der EUDA falsch, veraltet oder beschädigt sind? Im Sinne der Fehlerwahrscheinlichkeit beinhalten die maßgeblichen Kriterien das Folgende: • Wahrgenommene Komplexität der EUDA (keine bedeutsamen Berechnungen bis hin zu hochgradig komplexen und hochentwickelten Formeln); • Nutzungshäufigkeit; • Häufigkeit von Änderungen an der Formel/Logik der EUDA; und • Anzahl der Benutzer. Die Kritikalität der EUDA muss mit Barclays abgestimmt werden.	
EUDA-Kontrollziele	8. Mindestkontrollanforderungen gestützt auf EUDA-Kritikalität	Der Lieferant muss Kontrollen umsetzen, die die Anforderungen der Kontrollziele, gestützt auf die Kritikalitätsstufe, die mit Barclays abgestimmt wurde, erfüllen. Kontrollziele, die mit einem „M“ markiert wurden, werden von diesem Plan vorgeschrieben. Alle anderen Kontrollziele sind nur optional „O“. Siehe Anhang B für die Tabelle mit den Kontrollen. Nachweise müssen gegebenenfalls aufbewahrt werden, um aufzuzeigen, dass die geltenden Kontrollziele erreicht wurden.	Die richtige Kontrollstufe muss entsprechend des Risikos, das die EUDA darstellt, angewandt werden, um exzessive Kontrollen bei einer EUDA mit geringerem Risiko zu vermeiden.
EUDA-Kontrollziele	9. EUDA-Berechtigung	Jede EUDA sollte vor ihrer Erstverwendung ein Berechtigungsverfahren durchlaufen, um zu bewerten, ob sie erforderlich ist oder ob alternative Mittel zur Unterstützung des zugehörigen Geschäftsprozesses (z. B. Umstellung auf einen Managed Service) effizienter wären und/oder weniger Risiko darstellen würden als die Beibehaltung einer EUDA. Das EUDA-Berechtigungsverfahren muss durchgeführt werden, wenn eine EUDA erstmals erstellt wird (d. h. vor ihrer ersten Nutzung), und muss später regelmäßig erneut durchgeführt werden.	Indem ein EUDA-Berechtigungsverfahren durchlaufen wird, erhält der Lieferant die Gelegenheit zur Bewertung, ob die EUDA tatsächlich erforderlich ist.

		Das Ergebnis und der Nachweis des Berechtigungsverfahrens müssen aufbewahrt und vor der Erstbenutzung der EUDA, und wann immer das Verfahren im Anschluss durchgeführt wird, an Barclays gemeldet werden.	
EUDA-Kontrollziele	10. EUDA-Registrierung	Ein EUDA-Inventar muss bestehen, um Transparenz über den vollständigen Umfangs des EUDA-Bestands für den Lieferanten zu liefern und um die wichtigen Attribute zur Unterstützung der Bestimmungen dieses Plans zu erfassen. Ein Verfahren muss dokumentiert werden und vorhanden sein, um ein vollständiges, genaues und aktuelles Inventar der EUDAs zu gewährleisten. Das EUDA-Inventar muss mindestens jährlich überprüft werden, um die Genauigkeit zu erhalten und die Vollständigkeit zu bestätigen.	Die Vollständigkeit des EUDA-Inventars ist wesentlich, um die ordnungsgemäße Sicherheit und den ordnungsgemäßen Betrieb der EUDAs zu gewährleisten.
EUDA-Kontrollziele	11. Zugriff	Der Zugriff auf Daten und auf die Geschäftslogik für alle EUDAs muss auf die entsprechenden Benutzer mit den entsprechenden Zugriffsrechten beschränkt werden. Der Zugriff muss mit einem risikobasierten Ansatz überprüft werden.	Entsprechende Zugriffskontrollen schützen EUDAs vor unautorisiertem, unangemessenem oder nicht zurechenbarem Zugriff.
EUDA-Kontrollziele	12. Verfügbarkeit	Kontrollen müssen bestehen, um sicherzustellen, dass die EUDAs entsprechend den mit Barclays abgestimmten Anforderungen verfügbar sind.	Die Verfügbarkeit der EUDAs stellt den fortlaufenden Betrieb der Geschäftsprozesse sicher.
EUDA-Kontrollziele	13. Änderungsmanagement (Change-Management)	Die Befolgung der Änderungsmanagementgrundsätze stellt sicher, dass die EUDAs wie erwartet gemäß den Geschäftslogikänderungen funktionieren. Änderungen an der Geschäftslogik oder wichtigen statischen Daten der EUDAs dürfen nicht zu Ausgabe- oder Meldefehlern führen. Die EUDA-Benutzer dürfen nur auf die relevante(n) Version(en) der EUDA zur betrieblichen Nutzung zugreifen können. Die Vollständigkeit und Genauigkeit der Eingabedaten, Berechnungen und Ausgabedaten wird über Tests (automatisiert und/oder manuell)	Ein entsprechendes Änderungsmanagement ist entscheidend, damit die EUDA nach jeder Änderung weiter funktioniert wie erwartet.

		bestätigt, um sicherzustellen, dass alle angewandten Änderungen das erwartete Ergebnis erzeugen. Testschritte für jedwede EUDA, deren EUDA-Kritikalitätsbewertung als mittel oder hoch eingestuft wurde, sollten ermittelt und mit Barclays abgestimmt werden, um sicherzustellen, dass Änderungen nicht zu Auswertungsfehlern führen. Archivversionen dürfen nicht am gleichen Ort wie die Produktionsversion(en) gespeichert werden. Eine zweite Person muss vom Lieferant ernannt werden, um die fortlaufende Nutzung und Wartung der EUDA bei Abwesenheit des Hauptbenutzers/der Hauptbenutzer zu unterstützen.	
EUDA-Kontrollziele	14. Dokumentationsanforderung	Das Wissen um Eingaben, Berechnungen, Ausgaben und die Fähigkeit, diese zu ändern, darf nicht auf eine einzelne Person begrenzt sein. Außerdem muss eine adäquate Dokumentation bestehen, die durch eine spezifische, EUDA-erfahrene Person für die Änderung und Pflege der EUDA verwendet werden kann.	Da die EUDA von Endbenutzern verwaltet wird, ist eine adäquate Dokumentation wichtig, um sicherzustellen, dass kritische Informationen über die EUDA aufbewahrt werden, um einen Wissenstransfer zu ermöglichen und die Möglichkeiten von Wissensverlust zu minimieren.

Anhang A: Von Barclays verwendete Definitionen

Definitionen	
EUDA	EUDAs sind Anwendungen und Tools, die von den Endbenutzern erstellt, verwendet und verwaltet werden. Sie werden üblicherweise mit Standard-Desktop-Software (am häufigsten mit Microsoft Excel oder Access) und anderen Datenbanktypen, Abfragen, Makros, Skripten, Reporting-Tools und Code-Paketen entwickelt. EUDAs erbringen oder sind Teil eines Geschäftsprozesses auf fortlaufender Basis (keine einmalige Nutzung), die, falls ihre Berechnungen oder Ausgaben fehlerhaft, nicht verfügbar, veraltet oder beschädigt sind, eine finanzielle, aufsichtsrechtliche oder Reputationsauswirkung für die Bank haben oder einen Schaden für den Kunden verursachen könnten.

Anhang B: Mindestkontrollanforderungen

Die Anwendbarkeit jeder Kontrolle wird gemäß der folgenden Tabelle festgelegt (O = optional und M = vorgeschrieben):

Kontrolltitel	EUDA-Kritikalitätsbewertung			
	Sehr niedrig	Niedrig	Mittel	Hoch
1. Rollen und Verantwortungen	M	M	M	M
2. Information Risk Reporting (Informationsrisikomeldung)	M	M	M	M
3. Laufende Überwachung	M	M	M	M
4. Befolgung lokaler gesetzgebender und gesetzlich vorgeschriebener Anforderungen	M	M	M	M
5. EUDA-Ausbildung und -Bewusstsein	M	M	M	M
6. EUDA-Identifikation	M	M	M	M
7. EUDA-Kritikalitätsbewertung	M	M	M	M
8. Mindestkontrollanforderungen gestützt auf EUDA-Kritikalität	M	M	M	M
9. EUDA-Berechtigung	M	M	M	M
10. EUDA-Registrierung	O	M	M	M
11. Zugriff	O	M	M	M
12. Verfügbarkeit	O	O	M	M
13. Änderungsmanagement (Change-Management)	O	O	M	M
14. Dokumentationsanforderung	O	O	O	M

Anhang C: EUDA-Kritikalitätsbewertung

Die EUDA-Kritikalitätsbewertung beinhaltet zwei Teilbewertungen; EUDA-Hauptbenutzer müssen beide Teilbewertungen durchführen, um die EUDA-Kritikalität zu bestimmen.

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

Die Bedeutung einer einzelnen EUDA ist definiert als die ausgehend von den nachstehend aufgeführten Kriterien erreichte höchste Bewertung

Kriterien für die Bedeutung der EUDA	**Bewertung der Bedeutung der EUDA**			
	Niedrig	**Moderat**	**Hoch**	**Außerordentlich hoch**
1) Unterstützt die EUDA kritische Aktivitäten, die eine aufsichtsrechtliche Auswirkung haben (RWA-Äquivalent (Risk Weighted Assets) oder Exposure, auf das die EUDA direkte Auswirkungen hat)?	<50 Mio. GBP	≥ 50 Mio. GBP ≤ 500 Mio. GBP	>500 Mio. GBP ≤ 1 Mrd. GBP	>1 Mrd. GBP
2) Hat das Ergebnis der EUDA eine Auswirkung auf die Finanzberichterstattung?	Auswirkung auf die GuV < 1 Mio. GBP Auswirkung auf die Bilanz < 1 Mrd. GBP	Auswirkung auf die GuV ≥ 1 Mio. GBP < 10 Mio. GBP Auswirkung auf die Bilanz ≥ 1 Mrd. GBP < 2 Mrd. GBP	Auswirkung auf die GuV ≥ 10 Mio. GBP < 50 Mio. GBP Auswirkung auf die Bilanz ≥ 2 Mrd. GBP ≤ 3 Mrd. GBP	Auswirkung auf die GuV ≥ 50 Mio. GBP Auswirkung auf die Bilanz > 3 Mrd. GBP
3) Wie sieht die **wahrscheinliche** Auswirkung auf die Kunden der Bank aus, wenn die Informationen, Berechnungen bzw. Ergebnisse der EUDA falsch, veraltet oder beschädigt sind?	Betroffene Kunden < 100 Kundenverlust insgesamt < 1 Mio. GBP	Betroffene Kunden ≥ 100 < 1000 Kundenverlust insgesamt ≥ 1 Mio. GBP < 10 Mio. GBP	Betroffene Kunden ≥ 1000 < 10000 Kundenverlust insgesamt ≥ 10 Mio. GBP < 50 Mio. GBP	Betroffene Kunden ≥ 10000 < 50000 Kundenverlust insgesamt ≥ 50 Mio. GBP
4) Wie sieht die **wahrscheinliche** Reputationsauswirkung auf die Bank aus, wenn die Informationen, Berechnungen bzw. Ergebnisse der EUDA falsch, veraltet oder beschädigt sind?	Auswirkung wird als unwesentlich und auf der Ebene der Geschäftseinheit vor Ort bestehend eingeschätzt. Keine Auswirkung auf die Marke oder die Reputation des Konzerns.	Auswirkung wird als handhabbar und auf der Ebene der Geschäftseinheit vor Ort bestehend eingeschätzt. Keine Auswirkung auf die Marke oder die Reputation des Konzerns.	Negative Auswirkung für mehrere Geschäftsbereiche/Regionen. Auswirkungen auf die Marke des Konzerns sind unwahrscheinlich.	Wahrscheinliche Auswirkung auf die Marke des Konzerns.

Der EUDA-Hauptbenutzer muss die Fehlerwahrscheinlichkeit der EUDA anhand der nachstehenden Kriterien bewerten. Zur Ermittlung der letztendlichen Bewertung der Fehlerwahrscheinlichkeit muss der EUDA-Hauptbenutzer die Punkte für die einzelnen Kriterien zusammenzählen.

Kriterien für die Fehlerwahrscheinlichkeit der EUDA	Punktzahl Fehlerwahrscheinlichkeit			
	Eins	**Zwei**	**Drei**	**Vier**
1) Wie hoch ist die empfundene Komplexität der EUDA? (siehe nachstehende Definition*)	Ansatzweise	Leicht	Mittel	Erweitert
2) Wie häufig wird die EUDA verwendet?	Verwendung weniger als einmal pro Quartal	Einmal oder mehrmals pro Quartal, aber weniger als einmal pro Monat	Einmal oder mehrmals pro Monat, aber nicht täglich	Einmal oder mehrmals pro Tag
3) Wie häufig sind Formel-/Logikänderungen in der EUDA?	Nie oder sehr selten	Änderungen werden vorgenommen, aber nur ausnahmsweise	In regelmäßigen Abständen vorgenommene Änderungen, aber nicht bei jeder Verwendung der EUDA	Bei jeder Verwendung der EUDA
4) Wie viele Benutzer hat die EUDA?	Einzelner Benutzer	Mehrere Benutzer im selben operativen Team	Mehrere Benutzer in unterschiedlichen Teams innerhalb einer Geschäfts- oder Funktionseinheit	Mehrere Benutzer in unterschiedlichen Geschäfts- und/oder Funktionseinheiten

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

- **Ansatzweise** – Keine bedeutenden Berechnungen in der EUDA. Wird hauptsächlich für zusammenfassende Berichte verwendet.
- **Leicht** – Ein Prüfer mit beschränkten Kenntnissen der Anwendung kann Zweck und Wirksamkeit der Formeln durch Beobachtung und ohne von außen gegebene Erläuterungen auslegen.
- **Mittel** – Weist eine komplexere Funktionalität auf. Ein im Gebrauch der Anwendung (z. B. Excel, Access) bewanderter Prüfer könnte zusätzliche Informationen benötigen, damit er Zweck und Wirksamkeit der EUDA auslegen kann.

- **Erweitert** – Hohes Maß an Komplexität sowie ausgeklügelte Formeln. Möglich sind auch Verknüpfungen mit anderen Kalkulationstabellen, Datenbanken, Websites, Übersichten usw.

Die letztendliche Bewertung der Fehlerwahrscheinlichkeit ist durch Anwendung der Gesamtpunktzahl auf die nachstehende Tabelle zu ermitteln:

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

EUDA-Kritikalitätsbewertung

Der EUDA-Hauptbenutzer muss die Bewertungen von Bedeutung und Fehlerwahrscheinlichkeit zusammenführen, um die Gesamtkritikalität der EUDA zu bestimmen. Dafür ist die nachstehende Tabelle zu verwenden. Die EUDA-Kritikalitätsbewertung muss vom EUDA-Hauptbenutzer im EUDA-Inventar erfasst werden.

Bedeutung	Außerordentlich hoch	**Mittel**	**Mittel**	**Hoch**	**Hoch**
	Hoch	**Mittel**	**Mittel**	**Mittel**	**Hoch**
	Moderat	**Niedrig**	**Niedrig**	**Mittel**	**Mittel**
	Niedrig	**Sehr niedrig**	**Sehr niedrig**	**Sehr niedrig**	**Sehr niedrig**
Fehlerwahrscheinlichkeit		Unwahrscheinlich	Möglich	Wahrscheinlich	Sehr wahrscheinlich