

# Obblighi di controllo dei Fornitori esterni

EUDA – Applicazioni sviluppate per  
l'utente finale

Si prega di notare che il termine “EUDA” come citato nel presente SCO, si applica solo alle EUDA come individuate nello schema decisionale EUDA di Barclays e alle applicazioni utilizzate per supportare il servizio (o i servizi) che il Fornitore eroga a Barclays.

Area di controllo	Titolo di controllo	Descrizione del controllo	Perché è importante?
Governance e assicurazione di qualità	1. Ruoli e responsabilità	<p>Il Fornitore deve definire e comunicare i ruoli e le responsabilità rispetto a EUDA che devono essere rivisti dopo ogni modifica rilevante del modello operativo o dell'attività del fornitore.</p> <p>I ruoli principali devono comprendere un senior executive, responsabile delle EUDA.</p>	<p>Le EUDA richiedono un sostegno ad alto livello per assicurare l'efficacia della progettazione, dell'implementazione e dell'applicazione dei controlli.</p> <p>È necessario un monitoraggio costante per garantire al senior management la corretta progettazione e applicazione dei controlli sui rischi relativi alle informazioni.</p>
Governance e assicurazione di qualità	2. Segnalazione dei rischi relativi alle informazioni	<p>Occorre implementare controlli e processi documentati per garantire che gli incidenti derivanti da rischi legati alle EUDA vengano opportunamente segnalati e gestiti.</p> <p>Il Fornitore deve intervenire in caso di incidenti e violazioni in materia di informazioni attinenti alle EUDA, che devono essere immediatamente comunicati a Barclays. Deve essere istituita una procedura di risposta agli incidenti per la tempestiva gestione e segnalazione degli errori che interessano i dati di Barclays e/o i servizi utilizzati da Barclays.</p> <p>Il Fornitore deve aver cura di eliminare le carenze individuate con un piano di intervento correttivo (azione, proprietà, data di esecuzione) comunicato a Barclays e da questa approvato.</p>	
Governance e assicurazione di qualità	3. Monitoraggio costante	<p>Il Fornitore deve valutare, riesaminare e documentare la propria conformità al presente Programma con cadenza regolare e, in ogni caso, almeno una volta l'anno.</p>	

Governance e assicurazione di qualità	4. Rispetto delle disposizioni normative e legislative locali	Il Fornitore deve assicurare che i requisiti legislativi e statutari relativi alle EUDA in vigore nella giurisdizione in cui opera siano adeguatamente documentati e rispettati.	(come sopra)
Governance e assicurazione di qualità	5. Educazione e sensibilizzazione EUDA	Il Fornitore deve individuare i dipendenti che hanno responsabilità EUDA.  I dipendenti a cui è stato assegnato un ruolo EUDA devono completare il corso di formazione su educazione e sensibilizzazione idoneo al rispettivo ruolo.  Questo controllo deve essere svolto almeno una volta all'anno, conservandone le evidenze a comprova.	
Obiettivi di controllo EUDA	6. Identificazione di EUDA	Occorre implementare e documentare una procedura mirata a individuare tutti le EUDA proprietarie o gestite dal Fornitore che supportano i servizi di Barclays.	L'identificazione delle EUDA è essenziale per determinare il giusto livello di controllo per tutte le EUDA.
Obiettivi di controllo EUDA	7. Valutazione delle criticità EUDA	La criticità di ogni EUDA deve essere valutata prima della rispettiva messa in produzione e prima dell'implementazione di eventuali modifiche da apportare a EUDA.  La valutazione delle criticità del Fornitore deve prendere in considerazione elementi come gli impatti normativi, finanziari e reputazionali sul servizio che il Fornitore eroga a Barclays.  La valutazione delle criticità deve tenere conto anche della rilevanza e della probabilità di errore.  Si prega di consultare l'Appendice C  In termini di rilevanza, i criteri pertinenti includono quanto segue: <ul style="list-style-type: none"> <li>• EUDA supporta le attività critiche relative al prodotto/servizio offerto a Barclays?</li> <li>• I risultati forniti da EUDA possono avere un impatto finanziario su Barclays?</li> <li>• I clienti di Barclays possono essere influenzati negativamente se le informazioni, i calcoli o i risultati prodotti dalle EUDA risultano approssimativi, non aggiornati o corrotti?</li> </ul>	La comprensione delle criticità di EUDA può consentire ai fornitori di stabilire e implementare i livelli di controllo di EUDA adeguati.

		<p>In termini di probabilità di errore, i criteri pertinenti includono quanto segue:</p> <ul style="list-style-type: none"> <li>• Apparente complessità di EUDA (nessun calcolo significativo che denoti un livello di complessità elevato e la presenza di formule avanzate);</li> <li>• Frequenza di utilizzo;</li> <li>• Frequenza di modifiche a formule/logica di EUDA; e</li> <li>• Numero di utenti.</li> </ul> <p>La criticità delle EUDA deve essere concordata con Barclays.</p>	
Obiettivi di controllo EUDA	8. Requisiti minimi di controllo basati sulle criticità EUDA	<p>Il Fornitore deve adottare i controlli che soddisfino i requisiti degli obiettivi di controllo basati sul livello di criticità concordato con Barclays.</p> <p>Gli obiettivi di controllo contrassegnati con "M" sono imposti da questo programma. Tutti gli altri obiettivi di controllo sono solo opzionali (contrassegnati con "O"). Vedere la tabella dei controlli nell'Appendice B.</p> <p>Quando appropriato, occorre conservare le prove per dimostrare il raggiungimento degli obiettivi dei controlli applicabili.</p>	Il giusto livello di controllo deve essere applicato in linea con il rischio rappresentato dalle EUDA, al fine di evitare un controllo eccessivo sui rischi EUDA di minore entità
Obiettivi di controllo EUDA	9. Giustificazione EUDA	<p>Prima di iniziarne l'utilizzo, ogni EUDA deve essere sottoposta a una procedura di giustificazione per valutare se è necessaria, oppure se eventuali mezzi alternativi di supporto ai processi aziendali collegati (ad es. il passaggio a un servizio gestito) potrebbero essere più efficaci e/o comportare meno rischi rispetto al mantenimento di EUDA.</p> <p>All'atto della creazione iniziale di EUDA (ovvero prima del primo utilizzo), deve essere eseguita la relativa procedura di giustificazione che in seguito dovrà essere ripetuta periodicamente.</p> <p>I risultati e le evidenze della procedura di giustificazione devono essere conservati e notificati a Barclays prima del primo utilizzo di EUDA e in occasione delle ripetizioni periodiche della procedura.</p>	Lo svolgimento della procedura di giustificazione EUDA offre al Fornitore la possibilità di valutare se l'EUDA in questione è effettivamente necessaria.

Obiettivi di controllo EUDA	10. Registrazione EUDA	<p>Per garantire la trasparenza di tutte le applicazioni EUDA pertinenti per il Fornitore e per registrare gli attributi chiave a supporto delle disposizioni di questo programma, è necessario un inventario EUDA.</p> <p>Occorre implementare e documentare un processo per garantire un inventario completo, accurato e aggiornato delle EUDA. L'inventario EUDA deve essere verificato almeno annualmente per preservarne l'accuratezza e verificarne la completezza.</p>	La completezza dell'inventario EUDA è fondamentale per garantire la sicurezza e il funzionamento adeguati delle EUDA.
Obiettivi di controllo EUDA	11. Accesso	L'accesso ai dati e la logica di business di tutte le EUDA devono essere limitati agli utenti idonei, in possesso dei necessari diritti di accesso. L'accesso deve essere controllato utilizzando un approccio basato sul rischio.	Controlli di accesso adeguati proteggono le EUDA da un accesso non autorizzato, improprio o non attribuibile.
Obiettivi di controllo EUDA	12. Disponibilità	Devono essere attivati gli opportuni controlli per garantire che le EUDA siano disponibili secondo i requisiti concordati con Barclays.	La disponibilità delle EUDA garantisce il funzionamento continuo dei processi aziendali.
Obiettivi di controllo EUDA	13. Gestione delle modifiche	<p>Il monitoraggio dei principi di gestione delle modifiche garantisce il funzionamento delle EUDA secondo le aspettative, in seguito a modifiche della logica di business.</p> <p>Le modifiche alla logica di business delle EUDA o ai dati statici principali non devono generare errori di dati in uscita o di segnalazione. Gli utenti EUDA devono essere in grado di accedere solo alla(e) versione(i) di EUDA dedicata all'uso pertinente.</p> <p>La completezza e la precisione dei dati in ingresso, dei calcoli e dei dati in uscita sono convalidate attraverso attività di testing (automatiche e/o manuali) per garantire che le modifiche eseguite abbiano prodotto i risultati attesi.</p> <p>Per garantire che le modifiche non generino errori di segnalazione, le fasi dei test devono essere individuate e concordate con Barclays per le EUDA classificate di livello Medio ed Elevato nella valutazione delle criticità EUDA.</p> <p>Le versioni da archiviare non devono essere conservate nello stesso luogo della(e) versione(i) in produzione.</p>	Una gestione appropriata delle modifiche è fondamentale affinché l'EUDA continui a funzionare come previsto dopo eventuali modifiche.

		In assenza dell'utente primario (o degli utenti primari) il Fornitore deve incaricare una seconda persona per supportare l'uso continuativo e la manutenzione di EUDA.	
Obiettivi di controllo EUDA	14. Obbligo di documentazione	<p>La conoscenza di dati in ingresso, calcoli, dati in uscita e la capacità di modificarli non deve essere limitata a un'unica persona.</p> <p>Inoltre, deve esistere una documentazione idonea utilizzabile da una persona esperta, in grado di modificare ed effettuare la manutenzione delle EUDA.</p>	Poiché la gestione di EUDA è affidata all'utente finale, è importante che esista la documentazione idonea al fine di garantire che le informazioni cruciali relative a EUDA siano custodite in modo da consentire il trasferimento delle conoscenze e ridurre al minimo le relative possibilità di perdita.

## Appendice A: Definizioni utilizzate da Barclays

Definizioni	
EUDA	Le EUDA sono applicazioni e strumenti creati, utilizzati e gestiti dagli utenti finali. Generalmente sono realizzate utilizzando un software desktop standard (perlopiù Microsoft Excel o Access) e altri tipi di database, interrogazioni, macro, script, strumenti di reporting, file eseguibili e pacchetti di codici. Le EUDA eseguono o fanno parte di un processo aziendale su base continuativa (non di uso occasionale), e nel caso in cui i calcoli o i dati in uscita risultino non accurati, non disponibili, obsoleti o corrotti, potrebbero avere un impatto finanziario, normativo o reputazionale sulla Banca o causare danni al cliente.

## Appendice B: Requisiti minimi di controllo

L'applicabilità di ciascun controllo è stabilita secondo la seguente tabella (O = Opzionale e M = Mandatory (obbligatorio)):

Titolo di controllo	Classificazione delle criticità EUDA			
	Molto basso	Basso	Medio	Alto
1. Ruoli e responsabilità	M	M	M	M
2. Segnalazione dei rischi relativi alle informazioni	M	M	M	M
3. Monitoraggio costante	M	M	M	M
4. Rispetto delle disposizioni normative e legislative locali	M	M	M	M
5. Educazione e sensibilizzazione EUDA	M	M	M	M
6. Identificazione di EUDA	M	M	M	M
7. Valutazione delle criticità EUDA	M	M	M	M
8. Requisiti minimi di controllo basati sulle criticità EUDA	M	M	M	M
9. Giustificazione EUDA	M	M	M	M
10. Registrazione EUDA	O	M	M	M
11. Accesso	O	M	M	M
12. Disponibilità	O	O	M	M
13. Gestione delle modifiche	O	O	M	M
14. Obbligo di documentazione	O	O	O	M



## Appendice C: Valutazione delle criticità EUDA

La Valutazione delle Criticità EUDA è composta da due sottovalutazioni; gli Utenti Primari EUDA devono completare ambedue le sottovalutazioni al fine di stabilire le criticità EUDA.

- Una valutazione della rilevanza di EUDA rispetto a Barclays.
- Una valutazione delle probabilità di errore di EUDA.

La rilevanza di ciascuna EUDA è stabilita secondo il livello più elevato ottenuto dai criteri elencati di seguito

Rilevanza EUDA Criterio1	Livello di rilevanza EUDA			
	Basso	Moderato	Alto	Eccezionale
1) EUDA supporta le attività essenziali che hanno un impatto normativo (Attività di rischio ponderate - Risk-Weighted Assets - RWA) equivalente o un'esposizione che risente direttamente di EUDA)?	<£50M	≥ £50m ≤ £500m	>£500m ≤ £1bn	>£1bn
2) I risultati forniti da EUDA hanno un impatto sull'informativa finanziaria?	Impatto P&L < £1m  Impatto BS < £1bn	Impatto P&L ≥ £1m < £10m  Impatto BS ≥ £1bn < £2bn	Impatto P&L ≥ £10m < £50m  Impatto BS ≥ £2bn ≤ £3bn	Impatto P&L ≥ £50m  Impatto BS > £3bn
3) Se le informazioni, i calcoli, le elaborazioni di EUDA risultano imprecisi, non aggiornati o danneggiati quale potrebbe essere il <b>probabile</b> impatto sui clienti della banca?	Clienti interessati < 100  Perdita aggregata clienti < £1M	Clienti interessati ≥ 100 < 1000  Perdita aggregata clienti ≥ £1M < £10M	Clienti interessati ≥ 1000 < 10000  Perdita aggregata clienti ≥ £10M < £50M	Clienti interessati ≥ 10000 < 50000  Perdita aggregata clienti ≥ £50M
4) Se le informazioni, i calcoli, le elaborazioni di EUDA risultano imprecisi, non aggiornati o danneggiati quale potrebbe essere il <b>probabile</b> impatto reputazionale sulla banca?	Impatto considerato non determinante a livello di unità operative locali. Nessun impatto sul brand o sulla reputazione del Gruppo.	Impatto considerato gestibile a livello di unità operative locali. Nessun impatto sul brand o sulla reputazione del Gruppo.	Impatto negativo per più di una attività/regione. È improbabile un eventuale impatto sul brand del Gruppo.	Probabile impatto sul brand del Gruppo.

L'Utente Primario EUDA deve utilizzare i criteri indicati di seguito per valutare la probabilità di errore di EUDA. L' Utente Primario EUDA deve aggregare i punteggi del criterio per calcolare l'indice di probabilità di errore finale.

Criterio di probabilità di errore di EUDA	Punteggio di probabilità di errore			
	Uno	Due	Tre	Quattro
1) Qual è la complessità percepita di EUDA? (vedi definizione qui sotto*)	Elementare	Semplice	Intermedia	Avanzata
2) Qual è la frequenza di utilizzo di EUDA?	Uso meno che trimestrale	Una o più volte al trimestre ma meno di una volta al mese	Una o più volte al mese ma non ogni giorno	Una o più volte al giorno
3) Qual è la frequenza delle modifiche di formula/logiche di EUDA?	Mai o con frequenza molto bassa	Modifiche effettuate in via eccezionale	Modifiche effettuate regolarmente ma non ad ogni utilizzo di EUDA	Ad ogni utilizzo di EUDA
4) Quanti utenti ha EUDA?	Utente singolo	Più utenti nello stesso team operativo	Più utenti in team diversi all'interno di un'unica BU o Funzione	Più utenti in varie BU e/o Funzioni

\*Si riferisce alla funzionalità di EUDA ed è classificata come segue:

- **Elementare** – Nessun calcolo significativo in EUDA. Utilizzata principalmente come informativa sintetica.
- **Semplice** – Un revisore con conoscenza limitata dell'applicazione può interpretare lo scopo e l'efficacia delle formule attraverso l'osservazione e senza ulteriori spiegazioni.
- **Intermedia** – Ha una funzionalità più complessa. Un revisore esperto nell'uso dell'applicazione (ad es. Excel, Access) potrebbe aver bisogno di ulteriori informazioni per interpretare lo scopo e l'efficacia di EUDA.

- **Avanzata** – Un grado di complessità elevato e formule avanzate. Può anche essere collegato ad altri fogli di calcolo, database, siti Web, tabelle, ecc.

La valutazione finale della Probabilità di Errore deve essere calcolata applicando il punteggio aggregato alla tabella qui sotto:

Valutazione della probabilità di errore	Improbabile	Possibile	Probabile	Molto probabile
Punteggio aggregato	$\geq 4 < 6$	$\geq 6 < 9$	$\geq 9 < 12$	$\geq 12 \leq 16$

Valutazione delle criticità EUDA

L'Utente Primario EUDA deve unire le valutazioni della Rilevanza e della Probabilità di Errore per stabilire la criticità globale di EUDA. È necessario utilizzare la tabella seguente. La Valutazione della Criticità di EUDA deve essere registrata nell'inventario EUDA dall'Utente Primario EUDA.

Valore	Eccezionale	Medio	Medio	Alto	Alto
	Alto	Medio	Medio	Medio	Alto
	Moderato	Basso	Basso	Medio	Medio
	Basso	Molto basso	Molto basso	Molto basso	Molto basso
Probabilità di errore		Improbabile	Possibile	Probabile	Molto probabile