Obblighi di controllo dei fornitori esterni

EUDA – End User Developed Applications (Applicazioni e strumenti sviluppati per l'utente finale)

Versione 9.0 aprile 2019

Si prega di notare che il termine “EUDA” come citato nel presente SCO, si applica solo agli EUDA come individuati 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 garanzia	1. Ruoli e responsabilità	Il Fornitore deve definire e comunicare i ruoli e le responsabilità rispetto a EUDA. Tali ruoli e responsabilità devono essere rivisti dopo qualsiasi modifica sostanziale al modello operativo o alle attività del Fornitore. I ruoli principali devono includere un Direttore esecutivo, responsabile per gli EUDA.	Gli EUDA necessitano di un'elevata sponsorizzazione al fine di garantire che i controlli siano predisposti, implementati e realizzati in modo efficace. È necessario eseguire un monitoraggio costante per fornire ai dirigenti senior le garanzie sulla pianificazione e realizzazione dei controlli sui rischi delle informazioni.
Governance e garanzia	2. Segnalazione dei rischi relativi alle informazioni	I controlli documentati e le procedure devono essere attivi per garantire che gli Incidenti a rischio EUDA siano segnalati e gestiti. Il Fornitore è tenuto a rispondere degli Incidenti EUDA e delle violazioni di informazioni e a segnalarli immediatamente a Barclays. È necessario istituire una procedura di risposta agli incidenti per la segnalazione e la gestione tempestiva degli errori che influiscono sulle Informazioni di Barclays e/o sui Servizi utilizzati da Barclays. Il Fornitore deve garantire che le azioni di rimedio individuate in seguito a un incidente siano affrontate secondo un piano di rimedio (azione, titolarità, data di consegna) e condivise e concordate con Barclays.	
Governance e garanzia	3. Monitoraggio costante	Il Fornitore è tenuto a valutare, rivedere e documentare regolarmente e, in ogni caso, almeno una volta all'anno, la propria conformità con il presente Programma.	

Governance e garanzia	4. Osservanza delle disposizioni normative e legislative locali	Il Fornitore deve garantire che le disposizioni normative e legislative correlate agli EUDA che applicano la giurisdizione in cui il Fornitore opera siano opportunamente documentate e rispettate.	*(come sopra)*
Governance e garanzia	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	È necessario istituire e documentare una procedura mirata a individuare tutti gli EUDA proprietari o gestiti dal Fornitore che supportano i servizi di Barclays.	L'individuazione degli EUDA è essenziale per stabilire il giusto livello di controllo necessario per ogni 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:* • *EUDA supporta le attività critiche relative al prodotto/servizio offerto a Barclays?* • *I risultati forniti da EUDA possono avere un impatto finanziario su Barclays?* • *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?*	La comprensione delle criticità di EUDA può consentire ai fornitori di stabilire e implementare i livelli di controllo di EUDA adeguati.

		In termini di probabilità di errore, i criteri pertinenti includono quanto segue: • *Apparente complessità di EUDA (nessun calcolo significativo che denoti un livello di complessità elevato e la presenza di formule avanzate);* • *Frequenza di utilizzo;* • *Frequenza di modifiche a formule/logica di EUDA; e* • *Numero di utenti.* La criticità di EUDA deve essere concordata con Barclays.	
Obiettivi di controllo EUDA	8. Requisiti minimi di controllo basati sulle criticità EUDA	Il Fornitore deve implementare i controlli che soddisfino i requisiti degli obiettivi di controllo basati sul livello di criticità concordato con Barclays. Gli obiettivi di controllo obbligatori contrassegnati con 'M' sono stabiliti dal presente Programma. Tutti gli altri obiettivi di controllo sono esclusivamente Opzionali e contrassegnati con 'O'. Per il prospetto degli obiettivi di controllo consultare l'Allegato B. Per dimostrare che gli obiettivi di controllo applicabili sono stati raggiunti, è necessario conservare le evidenze, ove pertinente.	Per evitare controlli eccessivi su EUDA a basso rischio, deve essere applicato il livello di controllo corretto conformemente al rischio rappresentato dall'EUDA in questione.
Obiettivi di controllo EUDA	9. Giustificazione EUDA	Prima di iniziarne l'utilizzo, ogni EUDA deve essere sottoposto 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. 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. 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.	Lo svolgimento della procedura di giustificazione EUDA offre al Fornitore la possibilità di valutare se l'EUDA in questione è effettivamente necessario.

Obiettivi di controllo EUDA	10. Registrazione EUDA	Per offrire al fornitore la trasparenza sull'intero campo di applicazione di EUDA nonché per acquisire gli attributi chiave al fine di supportare le disposizioni del presente Programma è necessario istituire un inventario EUDA. Deve essere creata e documentata una procedura per garantire che l'inventario EUDA sia completo, accurato e aggiornato. L'inventario EUDA deve essere controllato almeno una volta all'anno per mantenere l'accuratezza e verificare la completezza.	La completezza dell'inventario EUDA è essenziale per garantire l'opportuna sicurezza e l'operatività di EUDA.
Obiettivi di controllo EUDA	11. Accesso	L'accesso ai dati e alla logica operativa per tutti gli EUDA deve essere limitato agli utenti che hanno i permessi di accesso appropriati. L'accesso deve essere controllato usando un metodo basato sul rischio.	I controlli degli accessi appropriati proteggono EUDA dagli accessi non autorizzati, non appropriati o non attribuibili.
Obiettivi di controllo EUDA	12. Disponibilità	Devono essere attivati gli opportuni controlli per garantire che gli EUDA siano disponibili secondo i requisiti concordati con Barclays.	La disponibilità di EUDA garantisce il funzionamento costante delle procedure di business.
Obiettivi di controllo EUDA	13. Gestione delle modifiche	I principi di gestione del post-modifica garantiscono che gli EUDA siano pienamente operativi dopo le modifiche delle logiche di business. Le modifiche alla logica di business o ai dati chiave statici di EUDA non devono generare errori di elaborazione o segnalazione. Gli utenti EUDA devono essere in grado di accedere solo alla(e) versione(i) di EUDA dedicata all'uso pertinente. 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. Per garantire che le modifiche non generino errori di segnalazione, le fasi dei test devono essere individuate e concordate con Barclays per gli EUDA classificati di livello Medio ed Elevato nella valutazione delle criticità EUDA. Le versioni da archiviare non devono essere conservate nello stesso luogo della(e) versione(i) in produzione. 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.	Una corretta gestione delle modifiche è essenziale affinché EUDA continui a funzionare come previsto dopo qualsiasi modifica

Obiettivi di controllo EUDA	14. Obbligo di documentazione	La conoscenza dei dati in ingresso, dei calcoli e dei dati in uscita, nonché la capacità di modificarli, non deve essere limitata a un singolo individuo. Inoltre, deve esistere un'adeguata documentazione che possa essere utilizzata da uno specifico esperto EUDA per le modifiche e la manutenzione di EUDA.	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.

Allegato A: Definizioni utilizzate da Barclays

Definizioni	
EUDA	EUDA sono applicazioni e strumenti creati, utilizzati e gestiti dagli utenti finali. Generalmente sono sviluppati utilizzando software desktop standard (più comunemente Microsoft Excel o Access) e altri tipi di database, query, macro, script, strumenti di segnalazione, eseguibili e pacchetti di codice. Gli EUDA eseguono o sono parte di un processo aziendale su base costante (non utilizzo temporaneo); se i relativi calcoli o dati in uscita sono imprecisi, non disponibili, non aggiornati o corrotti, potrebbero avere un impatto finanziario, normativo o reputazionale sulla Banca o potrebbero causare danni al cliente.

Allegato 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 bassa	Bassa	Media	Elevata
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. Osservanza 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 ciascun EUDA è stabilita secondo il livello più elevato ottenuto dai criteri elencati di seguito

Rilevanza EUDA Criterio1	**Livello di rilevanza EUDA**			
	Basso	**Moderato**	**Elevato**	**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) L'elaborazione di EUDA ha 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 **probabile** 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 **probabile** impatto sulla reputazione della 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. Utilizzato 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	≥ 4 < 6	≥ 6 < 9	≥ 9 <12	≥ 12 ≤16

Valutazione della Criticità di EUDA

L'Utente Primario EUDA deve unire il Valore e la valutazione 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**	**Elevato**	**Elevato**
	Elevato	**Medio**	**Medio**	**Medio**	**Elevato**
	Moderato	**Basso**	**Basso**	**Medio**	**Medio**
	Basso	**Molto basso**	**Molto basso**	**Molto basso**	**Molto basso**
Probabilità di errore		Improbabile	Possibile	Probabile	Molto probabile