Obblighi di controllo dei Fornitori esterni

Rischio tecnologico - Controlli tecnici

Versione 14.0, ottobre 2024

Area di controllo	Titolo del controllo	Descrizione del controllo	Perché è importante
1. Gestione dei problemi	Identificazione e registrazione del problema	Il Fornitore deve garantire che venga condotta un'indagine tempestiva delle cause alla radice per tutti gli incidenti più gravi, sia isolati che ricorrenti, il cui impatto combinato influisce in modo significativo sulle attività operative.	Se le cause alla radice degli incidenti più gravi non vengono identificate e risolte tempestivamente, il servizio rimane a rischio di guasti ripetuti ed evitabili, provocando l'arresto di sistemi e servizi, danni alla reputazione e/o danneggiamenti o perdite di dati.
	Gestione e risoluzione dei problemi	Il Fornitore deve garantire che le cause alla radice degli incidenti sopra descritti vengano eliminate in modo tempestivo o, qualora non fosse possibile, che Barclays abbia accettato formalmente tale rischio e che vengano applicati i controlli di mitigazione appropriati per limitare la probabilità che si ripresenti.	
2. Gestione delle modifiche	Rispetto di rigorosi controlli delle modifiche	Il Fornitore deve garantire che tutti i componenti IT utilizzati per la fornitura di servizi a Barclays siano gestiti secondo un rigoroso programma di controllo delle modifiche, che deve soddisfare i requisiti seguenti: 1. Il Fornitore deve informare Barclays riguardo a tutte le modifiche significative prima dell'implementazione delle stesse, in modo da poter procedere alla valutazione del relativo impatto e adottare opportune misure di mitigazione, come richiesto. 2. Occorre separare le mansioni delle figure che propongono, approvano, implementano e si assumono la responsabilità della modifica. 3. Le modifiche devono essere pianificate e gestite in base al livello di rischio associato al mantenimento del livello minimo di servizio richiesto per Barclays. 4. Le modifiche devono tenere in debita considerazione il potenziale impatto sulle prestazioni e/o sulla capacità dei componenti tecnologici interessati. 5. Le modifiche devono essere sottoposte ai test tecnici e di business appropriati prima dell'implementazione, conservando tutte le prove quando richiesto. 6. Dopo l'implementazione le modifiche devono essere verificate per garantire che siano state eseguite correttamente e non producano effetti imprevisti.	I processi di modifica inappropriati con lo scopo di evitare le modifiche non autorizzate, gestite in modo inadeguato o non appropriato ai servizi tecnologici possono determinare un'interruzione del servizio, il danneggiamento o la perdita dei dati, errori di elaborazione o frodi.

Area di controllo	Titolo del controllo	Descrizione del controllo	Perché è importante
3. Gestione delle prestazioni e della capacità	Allineamento costante alle esigenze tecnologiche di Barclays	Il Fornitore deve definire, mantenere e documentare livelli idonei di prestazioni e capacità per tutti i componenti chiave IT utilizzati nella fornitura di servizi a Barclays, in linea con tutti i requisiti contrattuali, tenendo conto dell'effettiva domanda aziendale e dell'utilizzo corrente della capacità, per garantire che la capacità disponibile continui a soddisfare i requisiti. Il Fornitore deve inoltre garantire che i componenti chiave sono dotati di indicatori di soglia e generano avvisi in caso di potenziale superamento delle soglie. Inoltre, tali dispositivi devono essere controllati periodicamente per garantire che l'erogazione del servizio sia in linea con tutti i requisiti contrattuali e con le esigenze di Barclays.	L'adozione di misure inadeguate con lo scopo di definire, documentare e monitorare il controllo dei livelli di prestazioni e/o capacità delle risorse IT, e l'omissione degli aggiornamenti necessari per mantenerle in linea con i requisiti attuali e futuri, potrebbe comportare una riduzione inaccettabile e/o l'interruzione dei servizi tecnologici, oltre a una perdita di business.
4. Sviluppo di applicazioni tecnologiche	Strategia di test e completamento prima del lancio tecnico e/o di business	Il Fornitore deve garantire che il software/servizio funzioni come descritto dallo stesso prima di vendere o fornire tale software o servizio basato su software a Barclays, oppure presentare una panoramica in merito ai difetti noti e al relativo impatto sulla fornitura del software/servizio. Tutto il codice del software deve risultare presente nei sistemi di controllo delle versioni e deve essere firmato dal Fornitore prima della relativa consegna a Barclays. Il Fornitore deve sottoporre tutte le modifiche apportate alle applicazioni a opportuni test del software, per garantire che il software in questione soddisfi i requisiti stabiliti. Il Fornitore deve conservare le prove dei test effettuati.	I sistemi e i servizi che sono stati testati in modo inadeguato e non presentano garanzie di qualità idonee possono generare un'importante e imprevedibile perdita di funzionalità per i servizi tecnologici e le procedure aziendali.
	Conferma dei requisiti di sistema	Quando fornisce software conforme alle specifiche di Barclays, il Fornitore deve garantire che i requisiti in termini di business tecnologico siano chiaramente definiti e concordati con Barclays.	I requisiti di business non adeguatamente definiti possono causare un comportamento scorretto del sistema, con conseguenti rischi per i processi aziendali e operativi.
	Accettazione dell'azienda prima dell'implementazione	Quando fornisce software conforme alle specifiche di Barclays, il Fornitore deve concordare e seguire un processo di accettazione aziendale concordato con Barclays.	Una procedura di accettazione inadeguata da parte dell'azienda prima del deployment può causare un comportamento scorretto del sistema, con conseguenti rischi per i processi aziendali e operativi.

Definizioni tecnologiche

Componenti della configurazione	Qualsiasi componente che deve essere gestito allo scopo di fornire un servizio IT. I componenti della configurazione possono essere fisici (ad esempio, computer o router), virtuali (ad esempio, server virtuali) o logici (ad esempio, servizi). Le modifiche (aggiunte, variazioni o dismissioni) devono essere effettuate sotto il controllo della gestione delle modifiche.
Incidente	Interruzione non pianificata di un servizio IT o riduzione della qualità di un servizio IT, incluso, a titolo di esempio non esaustivo, il guasto di un Componente della configurazione che non ha ancora prodotto effetti negativi sul servizio.
Incidente grave	Incidente che comporta un rischio/impatto significativo per Barclays e può produrre conseguenze gravi, come una grave perdita di produttività, danni reputazionali, conseguenze legali ed effetti negativi sui principali processi di business, sui controlli o sui sistemi chiave.
Modifiche significative	Modifiche che avranno un impatto, o che hanno il potenziale per esercitare un impatto, sull'efficacia del funzionamento del servizio/dei servizi fornito/i a Barclays, e/o modifiche in ragione delle quali Barclays dovrà o potrà intraprendere adeguate azioni di mitigazione del rischio a supporto della relativa implementazione.