Obblighi di controllo dei Fornitori esterni

Rischio tecnologico - Controlli tecnici

Versione 12.0, ottobre 2022

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, che influiscono 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 più gravi 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.	
Area di controllo	**Titolo del controllo**	**Descrizione del controllo**	**Perché è importante**
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. Non è possibile apportate modifiche senza ottenere l'autorizzazione di Barclays prima dell'implementazione. 2. Occorre separare le mansioni delle figure che propongono, approvano, implementano e si assumono la responsabilità della modifica.	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.

		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.	
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 IT utilizzati nella fornitura di servizi a Barclays, in linea con tutti i requisiti contrattuali. 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.
Area di controllo	**Titolo del controllo**	**Descrizione del controllo**	**Perché è importante**
4. Sviluppo di applicazioni tecnologiche	Strategia di test e completamento prima del lancio tecnico e/o di business	Il Fornitore deve determinare la qualità di tutti i componenti software prima di venderli o fornirli a Barclays. Tutto il codice del software deve essere presente nei sistemi di controllo delle versioni e firmati dal Provider di servizi del Fornitore prima di essere forniti a Barclays. In caso di modifiche alle applicazioni, il Fornitore deve testare il software per garantire che soddisfi i requisiti registrati, conservando anche le prove dei test eseguiti.	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 di business 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 controllo qualità e accettazione 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.
5. Disposizioni di backup per sistemi e dati	Utilizzo di processi di backup e ripristino appropriati ed efficaci	Il Fornitore deve garantire che tutti i sistemi e servizi IT utilizzati per la fornitura di servizi a Barclays dispongano di processi di backup e ripristino adeguati e funzionanti, in linea con le esigenze di Barclays, la cui efficienza deve essere comprovata periodicamente.	L'assenza di procedure di backup dei dati aziendali o un controllo inadeguato delle stesse possono determinare un arresto dei sistemi o servizi, una perdita di dati o una divulgazione di informazioni non autorizzata.
	Garantire supporti di backup sicuri, protetti e affidabili	Il Fornitore deve garantire che tutti i supporti di backup associati alla fornitura di servizi a Barclays, così come le disposizioni per la gestione e la conservazione di tali supporti, siano sempre sicuri e affidabili.	Sono necessari supporti di backup sicuri e affidabili per evitare un arresto dei sistemi o servizi, una perdita di dati o una divulgazione di informazioni non autorizzata.
Area di controllo	**Titolo del controllo**	**Descrizione del controllo**	**Perché è importante**
6. Gestione della configurazione	Isolamento dell'ambiente di produzione	Il Fornitore deve garantire che i servizi di produzione erogati a Barclays non dipendano da eventuali componenti non produttivi, al fine di evitare la realizzazione di servizi inaffidabili o non sicuri.	L'utilizzo di componenti non produttivi nell'erogazione dei servizi di produzione comporta un rischio in quanto non possono essere realizzati o gestiti secondo gli standard di produzione.
	Registrazione e mantenimento dei Componenti della configurazione	Il Fornitore deve mantenere un registro completo e accurato di tutti i Componenti della configurazione che influiscono sull'erogazione dei servizi a Barclays (comprese la titolarità, le dipendenze, così come le funzioni upstream e downstream). Il Fornitore deve provvedere a controlli atti a garantire il mantenimento costante dell'accuratezza e della completezza dei dati.	Le voci di registro (insieme alle dipendenze e mappature ad altri Componenti della configurazione) inappropriate o incomplete possono dare luogo a servizi e dati instabili o non sicuri, a causa di una valutazione inefficace degli effetti di incidenti e modifiche.

7. Gestione dei livelli di servizio	Definizione e monitoraggio delle Prestazioni dei servizi	Il Fornitore deve garantire che il servizio sia conforme ai livelli di servizio concordati, inclusi il monitoraggio e la generazione di report sui livelli di servizio.	I livelli di servizio garantiscono che i servizi IT siano forniti in linea con gli impegni di servizio IT concordati.

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.
Servizio IT	Servizio fornito a uno o più clienti da un provider di servizi IT. Un servizio IT, che richiede una combinazione di persone, processi e risorse IT, viene fornito ai clienti per supportare i loro processi aziendali.
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.
Problema	Causa sconosciuta di uno o più incidenti.