Obblighi di controllo dei Fornitori esterni

Rischio tecnologico

Versione 9.0 aprile 2019

Area di controllo	Titolo di controllo	Descrizione del controllo	Perché è importante?
1. Gestione obsolescenza	Garantire continue disposizioni di supporto	Il Fornitore deve tempestivamente avvisare Barclays quando viene a conoscenza di cambiamenti nella propria capacità di fornire supporto, diretto o indiretto, su risorse IT utilizzate nella fornitura di servizi a Barclays anche quando i prodotti presentano vulnerabilità in materia di sicurezza e deve garantire tempestivamente l'upgrade o il ritiro di tali risorse.	Dati e/o procedure inadeguate su risorse hardware e software non più supportate o servizi tecnologici basati su hardware o software obsoleti possono condurre a prestazioni inaccettabili, instabilità, vulnerabilità della sicurezza, perdita di attività ed eccessivi costi di migrazione.
2. Gestione degli incidenti	Registrazione, classificazione e risoluzione degli incidenti	Il Fornitore deve disporre di un programma di gestione degli incidenti relativamente al funzionamento dei propri sistemi e servizi IT che garantisca che tali incidenti operativi vengano opportunamente identificati, registrati, suddivisi per priorità, classificati e tempestivamente risolti al primo contatto o con tempestiva e adeguata escalation. Il programma deve prevedere una solida procedura per l'immediata ed efficace gestione dei Principali Incidenti.	Gli incidenti tecnologici non segnalati per tempo o con dettagli sufficienti, o la mancata attuazione delle azioni correttive necessarie, possono comportare un'interruzione inevitabile dei sistemi/servizi oppure corruzione o perdita dei dati. I Principali Incidenti richiedono una risposta urgente e approfondita poiché si tratta di incidenti che comportano un rischio significativo per l'azienda e possono procurare gravi conseguenze tra cui gravi interruzioni, perdita di reputazione, impatto finanziario ed effetto sulle principali procedure aziendali.
3. Gestione dei problemi	Identificazione, valutazione/analisi e soluzione di problemi tecnologici	Il Fornitore deve disporre di un programma di indagine tempestiva di problemi alla base di importanti incidenti tecnologici, che garantisca l'individuazione e la registrazione di tali problemi tramite l'analisi della cause e la loro risoluzione efficace per ridurre al minimo le probabilità e l'impatto della ripetizione dell'incidente. Il Fornitore deve inoltre garantire che esiste una procedura di analisi proattiva degli incidenti di routine mirata a identificare e risolvere le cause degli incidenti comuni ripetuti di grande portata.	Se i problemi sottostanti alla base di possibili incidenti con conseguenze sulla fornitura di servizi tecnologici non vengono identificati e risolti in modo tempestivo, possono comportare interruzioni evitabili di sistemi/servizi oppure corruzione o perdita di dati.

4. Gestione delle modifiche	Rispetto di rigorosi controlli delle modifiche	Il Fornitore deve garantire che tutti i componenti IT utilizzati nella fornitura di servizi a Barclays siano gestiti secondo un rigoroso programma di controllo delle modifiche, che tenga in piena considerazione i seguenti obiettivi: 1. Nessuna modifica può avere luogo prima dell'implementazione senza la dovuta autorizzazione - approvazione 2. Suddivisione dei doveri tra chi propone, chi detiene, chi approva e chi attua la modifica 3. Modifiche pianificate e gestite secondo il livello di rischio associato 4. Modifiche che tengano in debita considerazione il potenziale impatto sulle prestazioni e/o sulla capacità dei componenti tecnologici interessati 5. Le modifiche sono soggette a test tecnici e di attività pertinenti prima dell'implementazione, con conservazione della prova qualora richiesto 6. Le modifiche devono essere verificate dopo l'implementazione per garantire che siano state realizzate con successo senza impatti non previsti	Misure inadeguate per il controllo delle prestazioni e/o dei livelli di capacità delle risorse IT e il loro mancato aggiornamento in linea con i requisiti attuali e futuri potrebbe comportare una riduzione inaccettabile e/o l'interruzione dei servizi tecnologici e la perdita di attività. Inoltre, processi di modifica inadeguati volti a evitare modifiche non autorizzate o inadeguate a servizi tecnologici possono comportare interruzione del servizio, corruzione o perdita di dati, errori di elaborazione o frode.
5. Continuità del servizio	Fornire e convalidare disposizioni idonee di resilienza/recupero	Il Fornitore deve prende atto di e concordare le esigenze di resilienza/recupero di Barclays per ciascuno dei sistemi e servizi IT che fornisce a Barclays. L'accuratezza dei piani di resilienza e recupero deve essere mantenuta e confermata e gli accordi sulla continuità del servizio devono essere adeguatamente documentati e implementati/verificati per garantirne l'affidabilità e la corrispondenza con le esigenze aziendali.	L'assenza o l'inadeguatezza della pianificazione della continuità del servizio potrebbero causare l'interruzione inaccettabile del servizio tecnologico all'impresa o ai clienti, a seguito di un incidente. Mantenere la documentazione sulla resilienza aggiornata e pronta all'uso garantisce il costante allineamento dei piani di recupero alle esigenze aziendali.
6. Gestione delle prestazioni e della capacità	Rimanere allineati alle esigenze tecnologiche di Barclays	Il Fornitore deve definire livelli idonei di prestazioni e capacità per tutti i componenti IT utilizzati nella fornitura di servizi a Barclays, in linea con le esigenze dichiarate di Barclays. Il Fornitore deve inoltre garantire che i componenti chiave sono dotati di segnalatori di soglia che avvisano in caso di potenziale	Una definizione o documentazione inadeguata delle esigenze dell'impresa/dei clienti può condurre a prestazioni inaccettabili a livello di servizi tecnologici e alla perdita di attività.

		superamento delle soglie, e che tali dispositivi sono controllati periodicamente per garantire che l'erogazione del servizio sia allineata con le esigenze di Barclays.	
Area di controllo	**Titolo di controllo**	**Descrizione del controllo**	**Perché è importante?**
7. Sviluppo di applicazioni tecnologiche	Applicazione della garanzia di qualità ripetibile	Il Fornitore deve garantire che tutti i sistemi e i servizi IT utilizzati nell'erogazione dei servizi a Barclays siano sottoposti a una procedura dimostrabile, rigorosa, accurata e ripetibile sulla garanzia di qualità che comprenda, a titolo esemplificativo ma non esaustivo, test funzionali e non-funzionali, test sulla sicurezza delle applicazioni statiche e garanzia di qualità del codice tramite una revisione critica o una strumentazione automatica.	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.
	Accettazione dei risultati aziendali	Il Fornitore deve concordare le definizioni dei risultati aziendali accettabili, da realizzarsi una tantum o su base costante, per cui sono erogate e accettate da Barclays versioni di sistemi e servizi IT nuove o aggiornate. Il contenuto di tali definizioni deve includere sufficienti aspetti funzionali e non funzionali dei sistemi e servizi e può attingere da qualsiasi contenuto adeguato reciprocamente concordato come manuali dei sistemi esistenti, documentazione dettagliata dei requisiti reciprocamente concordati, storie e casistica degli utenti o qualsiasi altro contenuto appropriato. Il Fornitore deve collaborare con Barclays per garantire che i risultati aziendali siano accettati completamente o in parti reciprocamente concordate, da realizzarsi una	L'organizzazione non adeguata del comportamento funzionale e non funzionale del sistema può comportare una deviazione dal comportamento previsto del sistema di Barclays con possibili rischi per le attività e le procedure operative.

		tantum o su base costante, all'accettazione da parte di Barclays delle definizioni precedentemente concordate.	
8. 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 adeguati processi di backup e ripristino funzionanti, in linea con le esigenze di Barclays, la cui efficienza deve periodicamente essere comprovata.	L'assenza di backup dei dati aziendali o un controllo inadeguato degli stessi possono condurre all'interruzione del sistema/servizio, alla perdita di dati o alla divulgazione di dati indesiderata.
	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 e le disposizioni per la gestione e la conservazione di tali supporti, siano sempre sicuri e affidabili.	L'assenza di backup dei dati aziendali o un controllo inadeguato degli stessi possono condurre all'interruzione del sistema/servizio, alla perdita di dati o alla divulgazione di dati indesiderata.
9. 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 insicuri o inaffidabili.	Registrazioni inadeguate di componenti tecnologici (hardware e software) incluse la titolarità definita e le dipendenze da terzi possono causare servizi e dati insicuri o inaffidabili. 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 dati di configurazione	Il Fornitore deve mantenere un registro completo e accurato per tutte le Voci di Configurazione pertinenti utilizzate nell'erogazione dei servizi a Barclays (compresa la titolarità e le dipendenze/funzioni di upstream/downstream). Il Fornitore deve mantenere l'accuratezza e la completezza dei dati.	Le iscrizioni nel registro inappropriate o incomplete (insieme con le dipendenze/funzioni collegate al altre voci di configurazione) possono dare luogo a servizi e dati insicuri o instabili in seguito alla valutazione inefficace dell'impatto di incidente e modifica.
10. Gestione dell'Hardware	Registrazione e mantenimento dei dati Hardware	Il Fornitore deve mantenere un registro completo e accurato per tutti i beni Hardware IT pertinenti utilizzati nell'erogazione dei servizi a Barclays (compresa la titolarità e l'etichettatura se richiesto). Il Fornitore deve mantenere l'accuratezza e la completezza dei dati per tutto il ciclo vitale dei beni, dall'acquisizione allo smaltimento. Tutti i Beni Smaltiti devono essere completamente	Registrazioni inadeguate di beni tecnologici Hardware incluse la titolarità definita e le dipendenze da terzi possono causare servizi e dati insicuri o inaffidabili. La mancata cancellazione e il mancato smaltimento dei beni Hardware in modo sicuro può comportare danni economici, reputazionali e normativi.

		cancellati dai dati di Barclays e smaltiti in modo sicuro attraverso una procedura ufficiale di Smaltimento che rispetti i requisiti degli Standard di Sicurezza di Barclays pertinenti.	
Area di controllo	**Titolo di controllo**	**Descrizione del controllo**	**Perché è importante?**
11. Gestione dei Beni Software	Registrazione e mantenimento dei dati di Beni/Installazioni Software. Licenze Software	Il Fornitore deve mantenere un registro completo e accurato per tutti i beni software pertinenti e le relative installazioni utilizzati nell'erogazione dei servizi a Barclays (compresa la titolarità). Il Fornitore deve mantenere l'accuratezza e la completezza dei dati dall'acquisizione allo smaltimento (e dall'installazione alla disinstallazione). Il Fornitore deve inoltre garantire che l'uso dei software rimanga allineato alle condizioni della relativa Licenza.	Registrazioni inadeguate di beni tecnologici Hardware inclusa la titolarità definita possono causare servizi e dati insicuri o inaffidabili. La mancata gestione dell'uso dei software rispetto alle autorizzazioni può comportare danni economici, reputazionali e normativi.