Obblighi di controllo dei Fornitori esterni

Rischio tecnologico

Versione 11.0 ottobre 2021

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	I processi di modifica inadeguati volti a evitare modifiche non autorizzate, gestite in modo inadeguato o non appropriato a servizi tecnologici possono comportare

		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	interruzione del servizio, corruzione o perdita di dati, errori di elaborazione o frode.
5a. Resilienza tecnologica	Piano di Recupero del Sistema (System Recovery Plan - SRP)	Il Fornitore deve disporre di Piani di Recupero del Sistema (SRP) per ogni sistema/servizio tecnologico necessario a supportare la fornitura di servizi di Barclays con Categoria di Resilienza 0-3 e dei corrispondenti Obiettivi del Tempo di Recupero (RTO) e Obiettivi del Punto di Recupero (RPO). Il piano o i piani devono essere rivisti per verificarne l'accuratezza almeno una volta ogni 12 mesi. **Nota:** Per i sistemi/servizi tecnologici con Categoria di Resilienza 0-1, che sono progettati con una configurazione attiva/passiva per misure di resilienza, la convalida del piano SRP richiede che il sistema rimanga nell'ambiente recuperato per un periodo prolungato e che operi come attività operativa ordinaria, per confermare che tutti	In seguito a un incidente, l'assenza o l'inadeguatezza di Piani di Recupero del Sistema potrebbe causare l'interruzione inaccettabile dei servizi tecnologici forniti all'azienda o ai clienti. Mantenere la documentazione sulla resilienza aggiornata e pronta all'uso garantisce il costante allineamento dei piani di recupero alle esigenze aziendali.

		gli elementi funzionino in modo efficace. Di fatto di tratta di un'azione coordinata (Production Crossover - PCO)	
5b. Resilienza tecnologica	Piano di Recupero e Integrità dei Dati (Data Integrity Recovery Plan - DIRP)	Il Fornitore deve disporre di uno o più Piani di Recupero e Integrità dei Dati (DIRP) per ogni sistema/servizio tecnologico necessario a supportare la fornitura di servizi Barclays con Categoria di Resilienza 0-1. Il piano o i piani devono essere rivisti per verificarne l'accuratezza almeno una volta ogni 12 mesi.	La perdita di dati è una delle più grandi minacce che dobbiamo affrontare, perché può avvenire a causa di atti dolosi o di malfunzionamenti del sistema. Avere un piano per questo scenario è fondamentale e aiuta a identificare e comprendere le fonti di dati e le dipendenze.
5c. Resilienza tecnologica	Data Centre Diversity	Il Fornitore deve garantire che ogni sistema/servizio tecnologico necessario a supportare la fornitura di servizi di Barclays con Categoria di Resilienza 0-3 sia resiliente nei vari data centre e che questi ultimi siano abbastanza distanti tra loro in modo da ridurre il rischio che siano colpiti contemporaneamente da un singolo evento.	I data centre dovrebbero avere fonti di alimentazione, collegamenti di rete, ecc. alternativi ed essere abbastanza distanti tra loro in modo da ridurre il rischio che siano colpiti contemporaneamente da un singolo evento.
5d. Resilienza tecnologica	Convalida SRP	Il Fornitore deve testare e convalidare il/i Piano/i di Recupero del Sistema (SRP) per dimostrare che i sistemi/servizi tecnologici possono essere recuperati per soddisfare i requisiti della Categoria di Resilienza 0-3 previsti da Barclays. Per ogni sistema/servizio tecnologico necessario a supportare la fornitura di servizi con Categoria di Resilienza 0-1, che sono progettati con una configurazione attiva/passiva per misure di resilienza, l'ambiente passivo deve essere attivato seguendo il piano SRP documentato e utilizzato come ambiente di produzione per attività operative ordinarie, per una durata	I sistemi tecnologici distribuiti dal Fornitore possono avere un impatto sui viaggi dei clienti Barclays. È fondamentale accertarsi che i Fornitori che supportano le operazioni commerciali di Barclays abbiano piani di resilienza adeguati e testati, ed è essenziale che Barclays disponga della necessaria autorizzazione per l'applicazione di una corretta governance nella gestione dei propri Fornitori. Production Crossover (PCO) è un metodo per dimostrare che l'istanza passiva di un sistema configurato attivo-passivo funzioni come previsto e alla portata richiesta per le attività operative ordinarie. Inoltre, PCO può dimostrare anche che qualsiasi dipendenza dai sistemi a monte o a valle continua a funzionare come previsto.

		sufficientemente lunga da dimostrare capacità e piena funzionalità di integrazione (Production Crossover - PCO). I requisiti di frequenza di convalida devono essere supportati dalla Categoria di Resilienza associata, vale a dire: - Categoria di Resilienza 0: La convalida SRP deve essere eseguita ogni 12 mesi e la convalida PCO ogni 3 mesi - Categoria di Resilienza 1: Le convalide SRP e PCO devono essere eseguite ogni 12 mesi - Categoria di Resilienza 2-3: La convalida SRP deve essere eseguita ogni 24 mesi Se un test non riesce a raggiungere i requisiti minimi di recupero per la Categoria di Resilienza applicabile, il Fornitore deve immediatamente informare Barclays e fornire un piano di rimedio dettagliato (che comprenda le azioni da intraprendere e le relative date di completamento). Il fornitore deve informare Barclays prima di eseguire le azioni PCO.	
5e. Resilienza tecnologica	Convalida DIRP	Il Fornitore deve testare e confermare il Piano o i Piani di Recupero e Integrità dei Dati (DIRP) per ogni sistema/servizio tecnologico necessario a supportare la fornitura di servizi Barclays con Categoria di Resilienza 0-1, per dimostrare l'integrità dei dati durante il recupero. La convalida deve essere eseguita ogni 12 mesi. Se un piano non riesce a raggiungere i requisiti minimi di recupero per la Categoria di Resilienza applicabile, il Fornitore deve immediatamente informare Barclays e fornire un piano di rimedio dettagliato (che comprenda le azioni da intraprendere e le relative date di completamento).	I dati sono un elemento critico che può essere influenzato negativamente in molti modi. È necessario mettere in pratica il piano documentato per ripristinare, recuperare o ricreare i dati al fine di confermarne l'accuratezza e la fattibilità.

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 superamento delle soglie, e che tali dispositivi sono controllati periodicamente per garantire che l'erogazione del servizio sia allineata con le esigenze di Barclays.	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. Una definizione e/o documentazione inadeguate delle esigenze dell'impresa/dei clienti può condurre a prestazioni inaccettabili a livello di servizi tecnologici e alla perdita di attività.
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	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.

		garantire che i risultati aziendali siano accettati completamente o in parti reciprocamente concordate, da realizzarsi una 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 provvedere a controlli atti a garantire il mantenimento costante dell'accuratezza e della 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 provvedere a controlli atti a garantire la registrazione e la manutenzione continua dei dati degli hardware durante l'intero ciclo di vita dei beni. Il Fornitore deve mantenere un registro completo e accurato per tutti gli Hardware IT utilizzati nella fornitura di servizi a Barclays).	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.
	Smaltimento dei beni	Tutti i Beni smaltiti devono essere completamente 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.	È fondamentale che il Fornitore ottenga e registri la conferma formale che i beni sono stati smaltiti correttamente (compresa la distruzione sicura dei dati bancari). La mancata cancellazione e il mancato smaltimento dei beni Hardware in modo sicuro può comportare danni economici, reputazionali e normativi.
	Beni mancanti	È necessario indagare adeguatamente in caso di Beni "smarriti o rubati" e segnalare a Barclays il rischio se non vengono ritrovati.	È fondamentale che il Fornitore esegua gli opportuni controlli per garantire che siano svolte indagini accurate sui beni mancanti e, se non sono stati trovati, informi Barclays segnalando il rischio. La perdita e quindi la mancata cancellazione e il mancato smaltimento dei beni Hardware in modo sicuro può comportare danni economici, reputazionali e normativi.
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	Registrazioni inadeguate di beni tecnologici software 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.

		software rimanga allineato alle condizioni della relativa Licenza.	

Definizioni per la Resilienza tecnologica:

Recovery Time Objective (RTO)	RTO è il periodo di tempo tra un guasto o un'interruzione imprevisti dei servizi e la ripresa delle operazioni.
Recovery Point Objective (RPO)	RPO è lo stato target con riferimento alla disponibilità dei dati all'inizio del processo di recupero. È una misurazione della perdita massima di dati tollerabile in una situazione di recupero.
Production Crossover (PCO)	PCO è l'atto di attivare l'istanza alternativa (DR) per sistemi progettati in una configurazione Attiva-Passiva e di utilizzarla come istanza di produzione per un periodo di tempo prolungato per convalidare la piena funzionalità e capacità.
Piano di Ripristino del Sistema (System Recovery Plan)	Il piano di ripristino del sistema è un documento che definisce gli elementi tecnici e i dettagli per il ripristino allo stato operativo di un sistema o di qualsiasi componente guasto.
Piano di Ripristino e Integrità dei Dati	Il piano di integrità e ripristino dei dati è un documento che indica le misure da adottare per recuperare i dati persi a causa di un guasto del sistema o di un intento doloso. Il piano dovrebbe affrontare scenari con opzioni pertinenti (ad es. riproduzione di dati da altri sistemi, ripristino di dati da archivi su nastro o ricreazione di dati).

Requisiti di resilienza Barclays per matrice della categoria di resilienza

Categoria di resilienza	0	1	2	3
Recovery Time Objective (RTO)	Fino a 5 minuti	Fino a 4 ore	Fino a 12 ore	Fino a 24 ore

Recovery Point Objective (RPO)	Fino a 5 minuti	Fino a 15 minuti	Fino a 30 minuti	Fino a 24 ore