Obblighi di controllo dei Fornitori esterni

Pianificazione del ripristino

Versione 13.0 settembre 2023

1. Definizioni:

"Evento di disturbo"	Una serie di effetti dell'incidente, indipendente dalla causa, che i Fornitori hanno scelto di mitigare attraverso l'implementazione di nuove capacità e la pianificazione del ripristino e della resilienza.
"Incidente"	Indica un evento di disturbo che può essere gestito tramite l'adozione di piani di ripristino nell'ambito delle operazioni quotidiane.
"Pianificazione del ripristino"	I Piani di ripristino sono documenti che descrivono in dettaglio le fasi e le azioni da intraprendere per ripristinare l'operatività di un servizio. Possono essere denominati anche Piani di Continuità operativa o con altri termini simili.
"Pianificazione del ripristino"	Processo o pianificazione del ripristino dei servizi e dei processi aziendali, insieme alle dipendenze sottostanti.
"Recovery Time Objective"	Indica il tempo che intercorre fra un guasto, o un'interruzione imprevista dei servizi, e la ripresa delle operazioni.
"Categoria di resilienza"	La Categoria di resilienza rappresenta una classificazione utilizzata da Barclays per applicare i requisiti di resilienza a un determinato servizio. La specifica Categoria di resilienza determina l'RTO (Recovery Time Objective), l'RPO (Recovery Point Objective) e il requisito inerente alla frequenza di convalida.

2. Matrice di criticità della resilienza:

I servizi del Fornitore vengono assegnati da Barclays a una specifica Categoria di resilienza (0-4), la quale riflette l'impatto che un'interruzione del servizio potrebbe causare su Barclays. Una Categoria di Resilienza superiore (ovvero un numero inferiore) richiede uno standard di resilienza o di ripristino più elevato, proporzionato all'importanza del servizio. Il Fornitore deve garantire che i propri servizi raggiungano gli RTO (Recovery Time Objective) ed RPO (Recovery Point Objective) specificati di seguito per la Categoria di resilienza applicabile stabilita da Barclays per i servizi a contratto: La tabella seguente specifica quali Controlli del Fornitore sono applicabili in base alla Categoria di resilienza definita. I dettagli relativi a tali Controlli sono riportati nella successiva sezione 3 (*Controllo*).

Valutazione dell'impatto dei rischi	Impatto eccezionale	Impatto rilevante	Impatto moderato	Impatto limitato	Impatto insignificante
Categoria di Resilienza	0	1	2	3	4
Obiettivo RTO	Fino a 1 ora	Fino a 4 ore	Fino a 12 ore	Fino a 24 ore	Nessun ripristino
Obiettivo RPO	Fino a 5 minuti	Fino a 15 minuti	Fino a 30 minuti	Fino a 24 ore	Nessun ripristino

Frequenza dei test tecnologici	Categoria di Resilienza 0	Categoria di Resilienza 1	Categoria di Resilienza 2	Categoria di Resilienza 3	Categoria di Resilienza 4
Convalida del Piano di ripristino dei sistemi	Almeno due volte l'anno	Almeno due volte l'anno	Almeno ogni 12 mesi	Almeno ogni 24 mesi	Nessun ripristino pianificato
Convalida del Piano di ripristino dei dati	Convalida annuale del piano in un ambiente simile alla produzione	Convalida annuale tramite procedura virtuale dettagliata su desktop	Opzionale	Opzionale	Nessun ripristino pianificato
Convalida del Piano di ricostruzione di piattaforme e applicazioni	Convalida annuale tramite procedura virtuale dettagliata su desktop	Convalida annuale tramite procedura virtuale dettagliata su desktop	Opzionale	Opzionale	Nessun ripristino pianificato

Applicabilità dei controlli del Fornitore	Categoria di Resilienza 0	Categoria di Resilienza 1	Categoria di Resilienza 2	Categoria di Resilienza 3	Categoria di Resilienza 4
1. Requisito relativo alla mappatura delle dipendenze ai fini dell'inclusione nella Pianificazione	✓	✓	✓	✓	O
2. Eventi di disturbo in relazione al requisito di Pianificazione del ripristino	✓	✓	✓	✓	O
3. Requisito relativo alla Pianificazione e alla convalida del ripristino	✓	✓	✓	✓	O
4. Requisito relativo alla conduzione di un test integrato	✓	✓	O	O	O
5. Requisito riguardante i Piani di ripristino dei sistemi e la relativa convalida	✓	✓	✓	✓	O
6. Requisito riguardante i Piani di ripristino dei dati e la relativa convalida	✓	✓	O	O	O
7. Requisito relativo alla molteplicità dei data center e ai provider di servizi cloud	✓	✓	✓	✓	O
8. Requisito relativo ai Piani di ricostruzione di piattaforme e applicazioni	✓	✓	O	O	O

✓ = Richiesto	O = Opzionale

Se durante la revisione vengono identificati dei problemi, o se non vengono soddisfatti determinati requisiti durante la verifica dei controlli, il Fornitore dovrà informare tempestivamente Barclays (generalmente entro 10 giorni) e risolvere i problemi entro una data concordata.

3. Controlli:

Il Fornitore deve adottare un Approccio strutturato alla resilienza (Continuità aziendale e Disaster recovery) supportato da un apposito documento inerente a Policy e Standard che disciplina i requisiti di resilienza in ambito operativo e tecnico, in conformità con le migliori pratiche del settore e i requisiti normativi applicabili. L'Approccio strutturato alla resilienza deve essere supervisionato dal Senior management, nonché rivisto e testato annualmente **in relazione al livello di efficacia dimostrato.**

Titolo del controllo	Descrizione del controllo	Perché è importante
1. Requisito relativo alla mappatura delle dipendenze ai fini dell'inclusione nella Pianificazione del ripristino	Il Fornitore deve definire e documentare le dipendenze fondamentali per la fornitura del servizio a Barclays. Tali dipendenze devono essere mantenute e riesaminate ogni 12 mesi o in caso di modifiche sostanziali. Le dipendenze da considerare includono: ▪ Tecnologia e dati (forniti internamente e da Subappaltatori). ▪ Subappaltatori di particolare rilevanza (che potrebbero esercitare un impatto sostanziale sulle prestazioni e sulla fornitura del servizio a Barclays). ▪ Forza lavoro (perdita di personale, occorre considerare l'uso di strategie di ripristino senza aree di lavoro o che prevedono il lavoro a domicilio)	I Fornitori di servizi devono conoscere a fondo le dipendenze per l'erogazione dei propri servizi a Barclays. Le eventuali dipendenze dovranno essere incluse nel relativo Piano di ripristino aziendale al fine di garantire che siano prese in considerazione per mitigare l'impatto degli Incidenti e prevenire l'indisponibilità del servizio a Barclays.
2. Eventi di disturbo in relazione al requisito di Pianificazione del ripristino	Il Fornitore deve definire gli eventi di disturbo nell'ambito della pianificazione di ripristino e il livello di pianificazione necessario per garantire l'erogazione dei servizi entro i livelli di servizio concordati e gli RTO (Recovery Time Objective) corrispondenti. Il Fornitore deve garantire che tali Eventi di disturbo rimangano in linea con l'attuale panorama di rischi/minacce, siano valutati per la loro gravità e plausibilità, e siano supportati da informazioni di settore e intelligence. Come minimo, il Fornitore deve includere i seguenti Eventi di disturbo nell'ambito della propria pianificazione. ▪ La perdita di edifici in ubicazioni diverse, che influisce sulla fornitura dei servizi a Barclays (gli edifici e l'infrastruttura associata non sono disponibili). ▪ Scenario di perdita dei dati, compresi gli eventi informatici e il potenziale impatto sull'erogazione dei servizi a Barclays. ▪ Una perdita di risorse della forza lavoro, che potrebbe influire sull'erogazione dei livelli di servizio concordati (ad esempio pandemie, eventi geopolitici, guasti critici delle infrastrutture nazionali e così via).	Barclays ha l'esigenza aziendale (basata sul rischio) di evitare gli Eventi di disturbo e/o ripristinare tempestivamente il normale funzionamento dei processi in caso di interruzioni rilevanti, ovvero presentare un livello di resilienza adeguato. Barclays deve ricevere le garanzie necessarie ed essere a sua volta in grado di garantire ai soggetti interessati che, in caso di Eventi di disturbo, i servizi sono progettati in modo da ridurne al minimo gli effetti sui clienti, sulla gestione finanziaria e/o sulla reputazione.

Titolo del controllo	Descrizione del controllo	Perché è importante
	▪ Una perdita di servizi tecnologici, come la perdita di data center o di una specifica regione geografica in cui opera un provider di servizi cloud. ▪ La perdita di un subappaltatore di particolare rilevanza (servizi o forniture). Gli Eventi di disturbo devono essere rivisti regolarmente una volta l'anno al fine di raccogliere informazioni per la pianificazione e i test, oltre che per dimostrarne l'evoluzione nel tempo.	
3. Requisito relativo alla Pianificazione e alla convalida del ripristino	Il Fornitore deve prevedere appositi Piani di ripristino in relazione agli Eventi di disturbo concordati. I Piani di ripristino devono documentare in dettaglio le fasi di ripristino e la risposta attuabile dal Fornitore per mitigare l'impatto e/o posticipare l'indisponibilità dei servizi forniti a Barclays. Come minimo, è necessario considerare quanto segue: ▪ Possibili soluzioni alternative ▪ Protocolli decisionali ▪ Comunicazione e assegnazione delle priorità aziendali allo scopo di riprendere/mantenere un servizio almeno accettabile ▪ Dipendenze I Piani di ripristino devono essere testati e convalidati ogni 12 mesi, o quando interviene un cambiamento sostanziale, al fine di dimostrare la possibilità di fornire i livelli di servizio concordati e garantire che i servizi soddisfino i requisiti della Categoria di resilienza stabiliti da Barclays. Qualora uno dei piani non presenti i livelli di servizio concordati o i requisiti della Categoria di resilienza applicabili, il Fornitore deve comunicarlo immediatamente a Barclays (generalmente entro 10 giorni) e presentare un piano correttivo dettagliato (che includa le misure da adottare e le relative date di completamento).	È necessario completare le attività di test e di convalida per garantire a Barclays che il design dei servizi e il piano funzionino come previsto e includano tutte le dipendenze, oltre a dimostrare la possibilità di garantire i livelli di servizio concordati e che i servizi soddisfino i requisiti di resilienza stabiliti da Barclays.
4. Requisito relativo alla conduzione di un test integrato	Al fine di garantire che le interdipendenze tra i servizi di Barclays e del Fornitore siano comprese in relazione al ripristino del servizio, il Fornitore, su richiesta di Barclays e in	Le esercitazioni congiunte contribuiscono a garantire l'esistenza di adeguati protocolli di Pianificazione del ripristino, che prevedono strategie di comunicazione efficaci, e che il Fornitore e Barclays adottino una risposta coordinata

Titolo del controllo	Descrizione del controllo	Perché è importante
	occasione di una data concordata reciprocamente, deve partecipare a un test integrato per convalidare la resilienza/continuità collettiva sia del Fornitore che di Barclays. Barclays si impegna a non presentare tale richiesta più di una volta ogni 2 anni, a meno che i precedenti test integrati non abbiano evidenziato gravi carenze concrete o non si sia verificato un incidente che determina un'interruzione dei servizi.	per gestire gli eventi di disturbo e ridurre al minimo gli effetti sui clienti di Barclays e sul sistema finanziario in generale.
5. Requisito riguardante i Piani di ripristino dei sistemi e la relativa convalida	Il Fornitore deve disporre di un apposito Piano di ripristino dei sistemi, che specifichi nel dettaglio le azioni necessarie per ripristinare i sistemi al loro stato operativo dopo un'eventuale interruzione. I piani devono essere testati e convalidati, per dimostrare (con prove) che il sistema può essere ripristinato entro l'RTO e l'RPO definiti in precedenza, come richiesto in relazione alla Categoria di resilienza stabilita. Per quanto riguarda i sistemi progettati con una configurazione attiva/passiva, l'ambiente passivo deve essere attivato e utilizzato come ambiente di produzione BAU (Business As Usual) per una durata sufficiente a dimostrarne capacità e piena funzionalità di integrazione. Per i servizi progettati con una configurazione attiva/attiva, la convalida deve opportunamente dimostrare la continuità operativa in caso di perdita di un nodo, di un'istanza o di una zona di disponibilità del sistema (relativamente ai sistemi ospitati nel cloud), per una durata minima di 60 minuti. I requisiti di frequenza in termini di convalida sono definiti dalla Categoria di resilienza stabilita per il sistema. Consultare a tal proposito la Matrice di criticità della resilienza sopra riportata.	In seguito a un incidente, l'assenza o l'inadeguatezza dei Piani di ripristino dei Sistemi potrebbe causare un'interruzione inaccettabile dei servizi tecnologici forniti all'azienda o ai clienti. Mantenendo aggiornata e pronta all'uso la documentazione sulla resilienza è possibile garantire l'allineamento costante dei piani di ripristino alle esigenze aziendali.
6. Requisito riguardante i Piani di ripristino dei dati e la relativa convalida	Il Fornitore deve disporre di uno o più Piani di ripristino dei dati per ciascun sistema tecnologico necessario al fine di garantire la fornitura dei servizi a Barclays. I piani devono essere rivisti almeno una volta ogni 12 mesi o quando interviene un cambiamento sostanziale, per verificarne l'accuratezza, considerando come minimo quanto segue: ▪ Origini e flusso dei dati (a monte e a valle) ▪ Origini di backup e replica ▪ Requisiti di sincronizzazione dei dati dopo il ripristino	La perdita di dati è una delle minacce più gravi a cui Barclays si trova a far fronte, perché può essere dovuta ad atti dolosi o guasti di sistema. Avere un piano per questo scenario è fondamentale, perché aiuta a identificare e comprendere le origini e le dipendenze dei dati.

Titolo del controllo	Descrizione del controllo	Perché è importante
	Il Fornitore deve testare e convalidare i Piani di ripristino dei dati per ciascun sistema tecnologico necessario a garantire la fornitura di servizi a Barclays e deve inoltre dimostrare (con prove) che il processo di ripristino è in grado di recuperare i dati allo stato operativo previsto, entro l'RPO di fatto richiesto.	
7. Requisito relativo alla molteplicità dei data center e ai provider di servizi cloud	Il Fornitore deve garantire la resilienza di ogni sistema tecnologico necessario a garantire l'erogazione dei servizi a Barclays nei vari data center e che la distanza geografica fra questi ultimi sia sufficiente a ridurre il rischio che vengano colpiti contemporaneamente da un singolo evento. Se il sistema tecnologico è in hosting presso un provider di servizi cloud, tale sistema deve risultare disponibile in aree di disponibilità diverse, al fine di mitigare un'eventuale interruzione di tipo AZ. I sistemi critici devono necessariamente dimostrare la loro capacità di ripristino in caso di guasto intervenuto nella specifica regione geografica in cui opera il provider di servizi cloud.	I sistemi tecnologici devono essere implementati e distribuiti su più data center, per garantire un'adeguata protezione da eventuali interruzioni dell'operatività a livello di data center. Ciò si estende ai sistemi ospitati da provider di servizi cloud, in caso di guasto nella regione geografica.
8. Requisito relativo ai Piani di ricostruzione di piattaforme e applicazioni	Il Fornitore deve implementare un Piano di ricostruzione della piattaforma e delle applicazioni per ogni sistema tecnologico necessario per garantire la fornitura di servizi a Barclays. Tale piano deve essere rivisto, approvato e testato almeno una volta ogni 12 mesi, o nel momento in cui interviene un cambiamento sostanziale. Questi piani si riferiscono a situazioni in cui non è possibile utilizzare le opzioni di recupero/ripristino tradizionali e il sistema deve essere rigenerato dallo stato "bare metal". I piani devono considerare quanto segue: ▪ Sistema operativo/software dell'infrastruttura ▪ Distribuzione e configurazione delle applicazioni ▪ Controlli/configurazione di sicurezza ▪ Dipendenze e reintegrazione del sistema nell'ecosistema ▪ Requisiti dei dati (Piano di ripristino dei dati) ▪ Dipendenze delle apparecchiature per l'esecuzione dei piani di ripristino	È fondamentale prevedere piani di ripristino appropriati per i servizi tecnologici e i contratti di supporto, in relazione agli eventi che rischiano di compromettere la sicurezza informatica o l'integrità dei dati.