Obblighi di controllo dei Fornitori esterni

Pianificazione del ripristino

Versione 12.0, ottobre 2022

1. Definizioni:

"Crisi"	Indica un evento di disturbo o un problema reputazionale che richiede una risposta in grado di andare oltre la struttura, e/o le risorse normalmente utilizzate per le attività operative ordinarie, oltre a interventi esecutivi per il processo decisionale e il coordinamento.
"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.
"Crossover della produzione"	Si parla di "crossover della produzione" in caso di failover di un sistema tecnologico a un ambiente alternativo (DR), che viene quindi utilizzato per eseguire funzioni di produzione per un periodo di tempo prolungato.
"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 resilienza è una classificazione utilizzata per applicare i requisiti di resilienza a un servizio, che includono RTO, RPO, requisiti di convalida e frequenza.

2. Matrice di criticità della resilienza:

Barclays suddivide i servizi erogati dal Fornitore in base alla Categoria di Resilienza specifica (0-4). 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:

		Valutazione dell'impatto dei rischi	Impatto eccezionale	Impatto rilevante	Impatto moderato	Impatto limitato	Impatto insignificante
		Categoria di Resilienza	0	1	2	3	4
		Tipo di Resilienza	Continuo	Resilienza elevata	Resiliente	Ripristino	Sospensione/ solo backup
Evento di disturbo	Applicazione	Target RTO (non relativo a dati/eventi informatici)	Fino a 1 ora	Fino a 4 ore	Fino a 12 ore	Fino a 24 ore	Nessun ripristino pianificato
		Target RPO (non relativo a dati/eventi informatici)	Fino a 5 minuti	Fino a 15 minuti	Fino a 30 minuti	Fino a 24 ore	Nessun ripristino pianificato

3. Controlli:

Titolo del controllo	Descrizione del controllo	Perché è importante
1. Eventi di disturbo per i requisiti di pianificazione del ripristino	Barclays si impegna a stabilire le Categorie di Resilienza per i servizi a contratto. 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. La pianificazione per gli Eventi di disturbo deve includere come minimo: ▪ 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). ▪ Una perdita di servizi tecnologici, come la perdita di data center o provider di servizi cloud, che influisce su tutti i servizi tecnologici. ▪ La perdita di un subappaltatore importante per servizi o materiali di consumo. 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.	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
	Il Fornitore deve essere in grado di dimostrare di aver considerato, testato e convalidato diversi fattori di gravità.	
2. Requisiti della 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 riviste ogni 12 mesi e sottoposte agli interventi di manutenzione necessari. Le dipendenze da considerare includono: ▪ Tecnologia e dati (forniti internamente e da subappaltatori). ▪ Subappaltatori importanti (quelli che svolgono un ruolo critico per l'erogazione 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.
3. Convalida dei Requisiti di pianificazione del ripristino	Il Fornitore deve prevedere Piani di ripristino aziendali per gli Eventi di disturbo concordati. I Piani di ripristino aziendali 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	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.

Titolo del controllo	Descrizione del controllo	Perché è importante
	I piani di ripristino devono essere testati e convalidati ogni 12 mesi 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 e presentare un piano correttivo dettagliato (che includa le misure da adottare e le relative date di completamento).	
4. Test integrati	Categoria di resilienza 0-1 - Su richiesta di Barclays, in una data concordata reciprocamente, il Fornitore deve partecipare a un test integrato con lo scopo di convalidare la resilienza/continuità collettiva, sia di Barclays che del Fornitore stesso. 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.	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 per gestire le gli eventi di disturbo e ridurre al minimo gli effetti sui clienti di Barclays e sul sistema finanziario in generale.
5. Piani di Ripristino dei Sistemi	Il Fornitore deve disporre di Piani di ripristino dei sistemi (SRP, System Recovery Plan) per ogni sistema/servizio tecnologico necessario a supportare l'erogazione di servizi a Barclays, con gli RTO (Recovery Time Objective) ed RPO (Recovery Point Objective) corrispondenti. I piani devono essere rivisti almeno una volta ogni 12 mesi, per verificarne l'accuratezza.	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. Piani di Ripristino dei dati	Categoria di resilienza 0-1 - Il Fornitore deve disporre di uno o più Piani di ripristino dei dati per ciascun sistema/servizio tecnologico necessario al fine di garantire la fornitura dei servizi a Barclays. I piani devono essere rivisti almeno una volta ogni 12 mesi, 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 ci troviamo di 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
7. Data Centre Diversity	Il Fornitore deve garantire la resilienza di ogni sistema/servizio tecnologico necessario a garantire l'erogazione dei servizi a Barclays nei vari data center e che la distanza 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 servizio deve essere disponibile in aree di disponibilità diverse al fine di mitigare un'eventuale interruzione AZ. I servizi con Categoria di resilienza 0-1 devono essere resilienti in tutte le Aree cloud.	I data center dovrebbero disporre di fonti di alimentazione, collegamenti di rete e altri componenti alternativi e trovarsi a una distanza sufficiente a ridurre il rischio che vengano colpiti contemporaneamente da un singolo evento.
8. Convalida del Piano di ripristino dei sistemi	Il Fornitore deve testare e convalidare i Piani di ripristino dei sistemi per dimostrare che i sistemi e i servizi tecnologici possono essere ripristinati e rispettare gli RTO (Recovery Time Objective) ed RPO (Recovery Point Objective) definiti dalla matrice di criticità della resilienza. Per ogni sistema o servizio tecnologico necessario a garantire la fornitura dei servizi con Categoria di Resilienza 0-1, progettati con una configurazione attiva/passiva come misura di resilienza, l'ambiente passivo deve essere attivato seguendo il Piano di ripristino dei sistemi documentato e utilizzato come ambiente di produzione per le attività operative ordinarie, per un periodo di tempo sufficiente a dimostrarne la capacità e la piena funzionalità di integrazione (PCO, Production Crossover). Per i servizi progettati come attivi/attivi, la convalida deve dimostrare il funzionamento continuo in caso di perdita di un ambiente attivo (scenario con risorse di elaborazione ridotte). I requisiti relativi alla frequenza di convalida devono essere supportati dalla Categoria di Resilienza associata, vale a dire: - Categoria di Resilienza 0: la convalida dei piani SRP deve essere eseguita almeno quattro volte l'anno tramite PCO. - Categoria di Resilienza 1: La convalida dei piani SRP e PCO deve essere eseguita almeno due volte l'anno tramite PCO. - Categoria di Resilienza 2: La convalida dei piani SRP deve essere eseguita almeno ogni 12 mesi. - Categoria di Resilienza 3: La convalida dei piani SRP deve essere eseguita almeno ogni 24 mesi.	I sistemi tecnologici distribuiti da terzi possono influire sul percorso dei clienti Barclays. È fondamentale accertarsi che i terzi che supportano le operazioni commerciali di Barclays adottino piani di resilienza adeguati e testati. È inoltre essenziale che Barclays disponga delle autorizzazioni necessarie per adottare misure di governance appropriate nella gestione dei propri Fornitori. L'azione coordinata (PCO, Production Crossover) è un metodo per dimostrare che l'istanza passiva di un sistema configurato attivo-passivo funzioni come previsto e possieda la capacità richiesta per le attività operative ordinarie. La PCO può essere inoltre utilizzata per dimostrare il funzionamento regolare di qualsiasi dipendenza dai sistemi a monte o a valle.

Titolo del controllo	Descrizione del controllo	Perché è importante
	Qualora uno dei test non dimostri i requisiti di ripristino minimi della Categoria di resilienza applicabile, il Fornitore deve comunicarlo immediatamente a Barclays e presentare un piano correttivo dettagliato (che includa le misure da adottare e le relative date di completamento).	
9. Convalida del Piano di ripristino dei dati	Categoria di resilienza 0-1 - Il Fornitore deve testare e convalidare i Piani di ripristino dei dati per ciascun sistema/servizio tecnologico necessario a garantire la fornitura di servizi a Barclays e dimostrare che il processo di ripristino è in grado di recuperare i dati in uno stato operativo. La convalida deve essere eseguita almeno ogni 12 mesi. Qualora uno dei piani non presenti i requisiti di ripristino minimi della Categoria di Resilienza applicabile, il Fornitore deve comunicarlo immediatamente a Barclays e presentare un piano correttivo dettagliato (che includa le misure da adottare e le relative date di completamento).	I dati sono un elemento critico che può subire vari tipi di effetti negativi. È necessario mettere in pratica il piano documentato in modo da ripristinare, recuperare o ricreare i dati al fine di confermarne l'accuratezza e la fattibilità.
10. Piani di ricostruzione di piattaforme e applicazioni	Categoria di resilienza 0-1 - Il Fornitore deve implementare un Piano di ricostruzione della piattaforma e delle applicazioni per ogni servizio/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. 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 Qualora uno dei piani non presenti i requisiti di ripristino minimi della Categoria di Resilienza applicabile, il Fornitore deve comunicarlo immediatamente a Barclays e	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.

Titolo del controllo	Descrizione del controllo	Perché è importante
	presentare un piano correttivo dettagliato (che includa le misure da adottare e le relative date di completamento).	