External Supplier Control Obligations

Pianificazione del ripristino

Versione 11.0 ottobre 2021

1. Definizioni:

"Crisi"	Indica un evento di disturbo o un problema reputazionale per cui sono necessari una risposta che vada oltre la struttura e/o le risorse normalmente utilizzate per le attività operative ordinarie e interventi esecutivi per il processo decisionale e il coordinamento.
"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"	Processo o pianificazione del ripristino dei servizi e dei processi aziendali, insieme alle dipendenze sottostanti
"Evento di disturbo"	Una serie di effetti dell'incidente, indipendente dalla causa, che i Fornitori hanno scelto di mitigare attraverso l'implementazione di funzionalità e la pianificazione del ripristino e della resilienza
"Recovery Time Objective"	Indica il tempo che intercorre fra un guasto o un'interruzione imprevista dei servizi e la ripresa delle operazioni.

2. 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 e il livello di pianificazione necessario per garantire l'erogazione dei servizi entro i livelli di servizio concordati e i Recovery Time Objective corrispondenti. Le categorie degli Eventi di disturbo devono includere come minimo: ▪ Perdita di edifici in più sedi, che impedisce di supportare le operazioni aziendali. ▪ Scenario di perdita dei dati, compresi gli eventi informatici e il potenziale impatto sull'erogazione dei servizi a Barclays. Perdita di risorse dei colleghi, che può influire sulla fornitura dei livelli di servizio concordati. ▪ Indisponibilità dei servizi dovuti a Barclays a causa di potenziali eventi informatici o di altro tipo e dei relativi effetti sull'erogazione dei servizi a Barclays. ▪ Ripristino singolo e simultaneo di servizi tecnologici (come la perdita del data center).	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
	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. 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 essenziali per l'erogazione del servizio a Barclays, al fine di garantire che siano altrettanto resilienti per il Fornitore stesso. Tali dipendenze devono essere riviste ogni 12 mesi e sottoposte agli interventi di manutenzione necessari. Le dipendenze da considerare includono: ▪ Perdita di tutti i dati e le tecnologie ▪ Indisponibilità di servizi erogati dai subappaltatori rilevanti (quelli critici per l'erogazione del servizio a Barclays) ▪ Perdita di forza lavoro (perdita di edifici e/o di personale, tenendo conto della mancanza di strategie di ripristino delle aree di lavoro o per il lavoro a domicilio) Questi aspetti devono essere verificati e convalidati tramite il Piano di ripristino aziendale, al fine di dimostrare che i servizi soddisfano i requisiti della Categoria di resilienza stabiliti da Barclays per garantire che siano ugualmente resilienti e presentino i livelli di servizio richiesti.	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 del servizio fornito a Barclays. Come minimo, è necessario considerare quanto segue:	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

Titolo del controllo	Descrizione del controllo	Perché è importante
	▪ 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 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).	concordati e che i servizi soddisfino i requisiti di resilienza stabiliti da Barclays.
4. Test integrati	Su richiesta di Barclays, 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 carenze reali o i servizi non abbiano subito modifiche sostanziali.	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. Procedura di gestione di Incidenti e Crisi	Il Fornitore deve adottare una procedura documentata per la gestione di Incidenti e Crisi, che comprenda il processo di escalation di Incidenti/Crisi a Barclays. Dopo l'esito positivo delle attività di test e la convalida svolte dal Fornitore ogni 12 mesi, le procedure per la gestione di Incidenti e Crisi devono essere approvate. La procedura deve definire le attività minime e i risultati richiesti per la gestione e il trattamento di Incidenti/Crisi lungo l'intero ciclo di vita, dall'inizio alla chiusura. Il Fornitore è tenuto a nominare: (i) Una persona responsabile di approvare la procedura, confermando che è idonea allo scopo.	Il Fornitore deve esporre chiaramente le procedure per la gestione dei servizi in caso di Incidente o Crisi. Il Fornitore e Barclays devono avere una visione comune della procedura di escalation per gli scenari di Incidente e Crisi. Le attività di test e convalida hanno lo scopo di garantire che la persona o il team incaricato possieda le competenze, le conoscenze e un'organizzazione adeguate per gestire gli Incidenti e le Crisi, se e quando necessario.

Titolo del controllo	Descrizione del controllo	Perché è importante
	(ii) Un referente principale e uno secondario (in caso di assenza del referente principale) per ciascun ruolo di Crisi.	
6. Relazione a posteriori sull'Incidente o la Crisi	Successivamente all'interruzione del servizio, entro quattro settimane di calendario dal ripristino dei normali livelli operativi del servizio, è necessario inviare a Barclays una Relazione a posteriori sull'Incidente o la Crisi. La relazione deve comprendere, come minimo, una valutazione degli aspetti seguenti: ▪ La causa principale dell'incidente o della crisi ▪ Le misure correttive adottate e gli eventuali interventi di miglioramento continuo per evitare che il problema si ripresenti ▪ Qualsiasi effetto sui clienti Barclays noti al Fornitore	La Relazione a posteriori sull'Incidente o la Crisi è necessaria per garantire a Barclays che i problemi sono stati individuati/risolti e che le lezioni sono state apprese in modo tempestivo.
7. 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 di Barclays con Categoria di Resilienza 0-3 e dei corrispondenti RTO (Recovery Time Objectives) ed RPO (Recovery Point Objective). I piani devono essere rivisti almeno una volta ogni 12 mesi, per verificarne l'accuratezza. ☐ 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 per molto tempo nell'ambiente ripristinato e che funzioni nella modalità operativa ordinaria, al fine di dimostrare che tutti i componenti funzionino in modo efficace ed efficiente. Di fatto di tratta di un'azione coordinata (PCO, Production Crossover).	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.
8. Piani di Ripristino e Integrità dei Dati	Il Fornitore deve disporre di uno o più Piani di ripristino e Integrità dei Dati (DIRP) per ogni sistema/servizio tecnologico necessario a supportare l'erogazione di servizi Barclays con Categoria di Resilienza 0-1. I piani devono essere rivisti almeno una volta ogni 12 mesi, per verificarne l'accuratezza.	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
9. Data Centre Diversity	Il Fornitore deve garantire la resilienza di ogni sistema/servizio tecnologico necessario a supportare la resilienza dell'erogazione dei servizi con Categoria di Resilienza 0-3 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.	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.
10. Convalida dei piani SRP	Il Fornitore deve testare e convalidare i Piani di ripristino de Sistemi (SRP) al fine di dimostrare che i sistemi/servizi tecnologici possono essere ripristinare in modo da soddisfare i requisiti della Categoria di Resilienza 0-3 previsti da Barclays. Per ogni sistema/servizio tecnologico necessario a supportare l'erogazione dei servizi con Categoria di Resilienza 0-1, progettato 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 le attività operative ordinarie, per un periodo di tempo sufficiente a dimostrarne la capacità e la piena funzionalità di integrazione (PCO, Production Crossover). 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 di piani SRP e PCO deve essere eseguita almeno due volte all'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 ogni 24 mesi. Se un test non raggiunge i requisiti minimi di ripristino per la Categoria di Resilienza applicabile, il Fornitore deve comunicarlo immediatamente a Barclays e fornire un piano di correzione dettagliato (che comprenda le misure da adottare e le relative date di completamento). Il fornitore deve informare Barclays prima di eseguire la PCO.	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
11. Convalida dei piani DIRP	Il Fornitore deve testare e convalidare i Piani di ripristino e Integrità dei Dati (DIRP) per ogni sistema/servizio tecnologico necessario a supportare l'erogazione dei servizi con Categoria di Resilienza 0-1 a Barclays, al fine di dimostrare l'integrità dei dati durante il ripristino. La convalida deve essere eseguita almeno ogni 12 mesi. Qualora uno dei piani non presenti i requisiti di ripristino minimi 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).	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.
12. Piani di ricostruzione/repaving di piattaforme e applicazioni	Per supportare il ripristino da eventi di disturbo, come un exploit informatico, il Fornitore deve disporre di una piattaforma e di un piano di ricostruzione/repaving delle applicazioni per ogni servizio/sistema tecnologico necessario al fine di supportare l'erogazione dei servizi con Categoria di Resilienza 0-1 a Barclays, che deve essere rivisto, approvato e testato almeno una volta 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 servizi tecnologici e i contratti di supporto devono prevedere piani di ripristino appropriati per un evento che rischia di compromettere la sicurezza informatica o l'integrità dei dati.

3. 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 raggiungono il Recovery Time Objective (RTO) specificato di seguito per la Categoria di Resilienza applicabile stabilita da Barclays:

		ERMF - Risk Impact Assessment	Exceptional Impact	High Impact	Moderate Impact	Low Impact	Insignificant Impact
		Resilience Category	0	1	2	3	4
		Resilience Type	Continuous	Highly Resilient	Resilient	Recover	Suspend / Backup Only
Disruption Event	Application	RTO for Application Recovery (non-data events)	Up to 1 hour	Up to 4 hours	Up to 12 hours	up to 24 hours	No planned recovery
		RPO	Up to 5 minutes	Up to 15 mins	Up to 30 mins	Up to 24 hours	No planned recovery