

BANCA D'ITALIA

Terms of Reference (ToR) per la continuità operativa

I Tor servono a facilitare la valutazione di conformità alle “Linee guida per la continuità di servizio delle infrastrutture qualificate dei sistemi di pagamento” emanate a novembre 2004. I ToR devono essere letti congiuntamente alle Linee guida che rimangono il documento di riferimento ufficiale e contengono maggiori informazioni e dettagli.

N.	Domande	Spiegazione
Ruolo dei vertici aziendali		
1	Sono stati coinvolti direttamente i massimi organi amministrativi e di controllo? In particolare, i vertici aziendali hanno formulato le politiche in tema di continuità operativa e approvato i relativi piani di sviluppo e di gestione?	
2	Il vertice aziendale si è assicurato, sulla base di adeguate analisi, che i due siti - primario e alternativo - abbiano profili di rischio differenti e ha sottoposto ad attenta valutazione il rischio residuo di blocco contemporaneo degli stessi?	
Contenuti del piano.		
3	Sono chiaramente definite le attività vitali e critiche?	
4	Sono valutati gli scenari di rischio con le connesse analisi d'impatto?	
5	Sono assegnate le risorse necessarie per la realizzazione del piano?	
6	Sono valutate le soluzioni individuate riguardo alla localizzazione dei siti alternativi?	
7	Sono definite misure di estrema emergenza per fronteggiare l'eventualità di un blocco contemporaneo dei centri primario e alternativo?	

N.	Domande	Spiegazione
8	Sono approntate specifiche misure atte a contenere i rischi - come quelli di natura informatica – rivenienti da eventuali attacchi per i quali la stessa disponibilità di un sito alternativo non costituisce presidio efficace?	
9	Sono definite le priorità di ripartenza delle attività vitali e critiche?	
10	É individuata la persona o la struttura incaricata di dichiarare lo stato di emergenza e chiaramente fissata la struttura di comando preposta alla gestione della crisi con le relative responsabilità?	
11	Sono definite le attività necessarie per il rispetto degli obiettivi di ripristino e ripartenza?	
12	Il sito primario e quello secondario si avvalgono di personale diverso? In caso contrario, è definita la procedura di riallocazione del personale?	
13	Sono individuate le attività correlate alla erogazione dei servizi vitali e critici, con l'indicazione dei relativi collegamenti, interni ed esterni, in termini di condizionamenti operativi, logici e temporali?	
14	Sono indicate le misure e le cautele che le controparti devono adottare per prevenire malfunzionamenti nell'operatività reciproca e ricadute di natura sistemica?	
15	Sono individuati meccanismi e accorgimenti di natura logistica in grado di diversificare le fonti di approvvigionamento dei servizi essenziali per il funzionamento delle infrastrutture?	

N.	Domande	Spiegazione
16	Sono stabilite la frequenza e l'ampiezza delle verifiche periodiche (almeno una volta l'anno), coordinate a livello di sistema o di gruppi di operatori?	
17	Sono previsti adeguati meccanismi per la valutazione degli interventi gestionali e dei risultati delle verifiche, con particolare riferimento agli effetti di natura sistemica, nonché per la promozione dei necessari interventi correttivi?	
18	Sono definite le modalità di gestione e controllo del piano?	
Obiettivi del piano.		
19	La ripartenza e il ripristino delle attività vitali sono assicurate entro le due ore dalla dichiarazione dello stato di crisi?	
20	La perdita di dati è tendenzialmente limitata all'ultima transazione inviata da ciascuna controparte?	
21	Sono definiti appositi raccordi procedurali con le controparti per il ripristino manuale delle transazioni perse, adottando gli accorgimenti necessari a minimizzare il rischio di elaborazioni duplicate o errate?	
22	La ripartenza dei servizi critici è assicurata entro un tempo relativamente breve – tendenzialmente dell'ordine di una settimana - dall'evento catastrofico?	
23	Sono valutate e predefinite le modalità operative per supplire all'eventuale degrado, allungando gli orari di operatività o limitando i volumi delle transazioni immesse dai partecipanti al sistema?	

N.	Domande	Spiegazione
24	<p>La ripartenza e il ripristino delle attività vitali sono comunque assicurati entro breve tempo dal verificarsi dell'incidente, anche in caso di catastrofe (blocco dei servizi essenziali ovvero gravi danni o serio pericolo sul lato umano)?</p> <p>L'eventuale perdita di dati è comunque contenuta indicativamente entro le quattro ore precedenti la dichiarazione dello stato di crisi, anche in caso di catastrofe?</p> <p>Sono predisposti adeguati meccanismi procedurali, atti a consentire la tempestiva ripresa delle transazioni perse e a minimizzare il rischio di elaborazioni duplicate o errate, anche in uno scenario di catastrofe?</p>	
Verifica del piano.		
25	Il piano è documentato in maniera efficace e chiara?	
26	È prevista la sua diffusione all'interno dell'azienda attraverso un'adeguata attività di formazione e addestramento?	
27	E' definito un processo per la rilevazione delle carenze e delle anomalie del piano, che preveda la valutazione dei massimi organi amministrativi e controllo nei casi di maggiore criticità?	
28	Le verifiche globali dei piani di emergenza simulano condizioni operative e volumi di attività realistici, effettuando il controllo delle funzionalità e delle prestazioni in situazioni di crisi e verificando la capacità dell'organizzazione di attuare nei tempi previsti le misure definite nel piano?	
29	Il collaudo integrato coinvolge anche i clienti/utenti e le controparti rilevanti, verificando anche l'adeguatezza della struttura dei collegamenti con i fornitori di servizi essenziali?	

N.	Domande	Spiegazione
30	I risultati delle verifiche sono adeguatamente documentati, portati all'attenzione dell'alta direzione e inviati, per le parti di competenza, alle unità operative coinvolte e alla funzione di auditing?	
Controlli interni.		
31	Sono previsti adeguati meccanismi e procedure di controllo da parte della funzione di revisione interna e/o di soggetti terzi indipendenti?	
32	Il consiglio di amministrazione ha valutato attentamente le possibilità di applicazione di standard di sicurezza riconosciuti a livello nazionale e/o internazionale, nonché l'assoggettamento del piano stesso a valutazione da parte di terze parti ovvero a certificazione eseguita da laboratori di valutazione accreditati presso enti a ciò delegati, ove ciò fosse possibile in base agli standard di sicurezza prescelti?	
Comunicazioni alla Banca d'Italia.		
33	Sono rappresentate alla Banca d'Italia le principali iniziative assunte in materia e, comunque, ogni circostanza o fatto che riduce il grado di affidabilità del sistema nel suo insieme o di parti rilevanti dello stesso?	
34	Sono immediatamente segnalate le anomalie aventi ricadute significative sul livello di servizio offerto e i relativi interventi correttivi?	
35	I piani di continuità sono stati approntati e comunicati alla Banca d'Italia?	