Empoli, 2 novembre 2012

Spett.le
Banca d'Italia
Nomativa e Politica di Vigilanza - Roma

Con le osservazioni che seguono Cabel, quale network di servizi in outsourcing per banche e altri intermediari finanziari, si propone di partecipare alla procedura pubblica di consultazione delle Disposizioni di vigilanza prudenziale per le banche sul Sistema dei controlli interni, sistema informativo e continuità operativa emanate da codesta Banca d'Italia.
In particolare le note che qui si formulano attengono al Titolo V, Capitoli 8 e 9.
La scrivente tiene, in primo luogo, a rappresentare il proprio apprezzamento per una normativa che mira a conferire organicità alla tematica del governo del rischio informatico, profilo che richiede la massima consapevolezza da parte dei vari "stakeholders" .
Dalla lettura del documento si ricava la determinazione di far emergere meglio quanto resta sottinteso nella normativa finora in vigore in termini di best practices, nel tempo consolidatesi in standard internazionali (e connesse certificazioni) volte ad assicurare il rispetto di procedure ormai ampiamente diffuse. Del resto anche la funzione informatica delle Banche Centrali Europee nel loro interagire con quella della BCE seguono tali standard (Cobit, Iso, Isea, etc), quale linguaggio comune e tali riferimenti sono citati nelle fonti della normativa.
Una prima osservazione - da intendere peraltro come richiesta di chiarimento - attiene alla misura in cui la normativa sulla continuità operativa riguardi o meno i cosiddetti outsourcers informatici, considerato che a pag 63 i destinatari della disciplina in tema di continuità operativa indicati nel testo con il nome collettivo di "intermediari", sono individuati in:
- banche e i gruppi bancari;
- sistemi di pagamento e relativi fornitori di servizi tecnologici; le controparti centrali, le società di gestione accentrata di strumenti finanziari, i gestori di sistemi di riscontro e rettifica giornaliera e società che forniscono servizi di compensazione e liquidazione su strumenti finanziari; i mercati regolamentati all'ingrosso su titoli di Stato, i sistemi multilaterali all'ingrosso su titoli di Stato e i sistemi multilaterali di scambio di depositi in euro. [1]
Sembrerebbe trattarsi di funzioni sistemiche connesse pressoché esclusivamente con i servizi i pagamento, il che porterebbe ad escludere, almeno in via diretta, quali destinatari gli outsourcers come fornitori di servizi di facility management, application management e BPO, cui, per buona parte del sistema bancario italiano, e' affidata la gestione della funzione informatica a cominciare dalla continuità operativa. È corretta questa interpretazione?
Ancorché la rispondenza dei sistemi informatici resti affidata alla responsabilità delle banche, e ove sia ovviamente di interesse per la Vigilanza, ci permettiamo di sollevare la questione se non debba essere richiamata l'esigenza da parte di ogni full provider di una configurazione minima del proprio sistema informatico che protegga dal rischio di

[1] * Sembrerebbe opportuno prevedere che le misure prese dai soggetti sistemici citati si debbano anche raccordare tra di loro e con quelle delle autorità di controllo, per decidere il da farsi in casi di emergenza, quali la chiusura dei mercati, come e' successo di recente in USA per l'uragano Sandy ove lo Stock Exchange e' stato chiuso per due giorni per decisione congiunta del Mercato e delle Autorità.

interruzione dell'operatività, e ciò nella considerazione dei rapporti di interdipendenza che oramai legano sempre più strettamente gli intermediari bancari, anche di dimensione ridotta, con rischi di propagazione delle disfunzioni da interruzione di servizio.
Un livello di fault tolerance e/o di resilienza adeguati vengono dalle best practices collegati con l'esistenza di un doppio sito elaborativo e di un terzo di disaster recovery, con la ridondanza delle connessioni, distribuite tra carrier diversi e/o strumenti tecnologici distinti (linee telefoniche, ponti radio, fibre ottiche, etc.). Non dovrebbero i full outsourcer assicurare almeno questo minimo? È normativamente praticabile la fissazione di un livello minimo, in termini di continuità operativa, cui uniformare le prestazioni degli outsourcer informatici, anche per il tramite delle banche, dato che l'offerta dei servizi in discorso appare al momento abbastanza disomogenea?
Sarebbe normativamente ipotizzabile la prescrizione di almeno una certificazione internazionale, quale evidenza di terza parte circa il rispetto delle best practices da parte dell'outsourcer in materia di processi produttivi?
La seconda questione riguarda i controlli che le banche clienti dovrebbero poter esercitare sull'outsourcer. Sembra di capire che possa essere prevista anche nelle banche che esternalizzano una figura di responsabile del controllo sull'outsourcer, come avviene in caso di esternalizzazione della funzione di compliance (pag49).
Anche se concordiamo in linea di principio con questa linea, corre l'obbligo di far presente che sarebbe una figura difficile da creare e da tenere costantemente aggiornata con gli sviluppi tecnologici (e i rischi sottostanti) dell'industria nel suo complesso. Appare complessa anche la possibilità di prevedere normativamente l' obbligo a carico delle banche di tenere una struttura attiva per poter eventualmente riassorbire (insourcing) le funzioni esternalizzate, stanti gli investimenti sia materiali sia immateriali che dovrebbero essere effettuati per questo scopo, in costanza di contratto di outsourcing delle funzioni ICT (pag. IV, prima alinea, Relazione illustrativa).
In luogo di questa previsione, potrebbe essere prevista un contrattualistica con diritti e doveri precisi in capo al fornitore, nella fissazione dei livelli di servizio e degli altri obblighi contrattuali, dando maggiore enfasi normativa alla formulazione delle regole da prevedere nel contratto di fornitura, oltre a una chiara possibilità di uscita che salvaguardi tanto gli interessi delle banche quanto quelli dell'outsourcer che deve poter contare su una durata adeguata del contratto di fornitura (non inferiore a tre anni, ma più opportunamente quinquennale) per la programmazione dei propri investimenti. Nel contempo vanno evitate situazioni di captivity, ad esempio con penali all'uscita alla fine del contratto.
Potrebbe essere inserito anche l'obbligo per l'outsourcer di istituire, nella propri struttura, appositi comitati tecnici o simili, ai quali consentire la partecipazione dei clienti per condividere le scelte tecnologiche e per raccoglierne sistematicamente le esigenze. Il comitato avrebbe anche funzioni di controllo sul processo di adeguamento delle applicazioni, soprattuto ove scaturiscano da modificazioni normative di vigilanza o di legge, per la maggiore consapevolezza circa la conformità delle applicazioni ai dettati prescrittivi.
Si sottopone alla valutazione di codesto Organo di Vigilanza pure l'opportunità di dettagliare meglio la "continuità operativa" anche come qualità di scrittura del software, quale componente strategica per la stabilità dei servizi di "application management"; andrebbe a nostro avviso precisato meglio anche il concetto dei "prolungati disservizi" (pag. 55).
Si resta a disposizione per eventuali chiarimenti in ordine a quanto esposto.
Si ringrazia per l'attenzione e si inviano distinti saluti.

L'Amministratore Delegato
D. Corsini