Prof. Ranieri Razzante
Presidente

Spettabile
BANCA D'ITALIA
Servizio Normativa e Politiche di Vigilanza prudenziale
Via Milano, 53
npv@pec.bancaditalia.it

Roma, 31 ottobre 2012

OGGETTO: consultazione pubblica sulle disposizioni di vigilanza prudenziale per le banche, il sistema dei controlli interni, sistema informativo e continuità operativa.

Spettabile Autorità di Vigilanza,

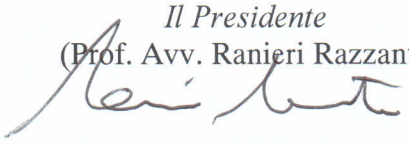
AIRA manifesta vivo apprezzamento per l'iniziativa volta a sottoporre in consultazione il documento recante le disposizioni di vigilanza prudenziale per le banche, le disposizioni sul sistema dei controlli interni, il sistema informativo e la continuità operativa e ringrazia per l'opportunità offerta di partecipare al confronto.

Preliminarmente ai rilievi di merito sulle emanande disposizioni di vigilanza, la scrivente Associazione esprime un giudizio positivo sulle finalità perseguite dal provvedimento.

Rimettiamo in allegato le nostre osservazioni, frutto del supporto dei soci.

Onorati di poter condividere con codesto Istituto le nostre riflessioni su un intervento normativo di indubbia rilevanza, restiamo a completa disposizione per fornire i chiarimenti che dovessero essere necessari e porgiamo i migliori saluti.

Il Presidente
(Prof. Avv. Ranieri Razzante)



Titolo V – Capitolo 7 – Sezione I – Paragrafo 3

Definizioni, pag. 3

Lettera e) *"Funzioni aziendali di controllo: la funzione di conformità alle norme (compliance), la funzione di controllo dei rischi (risk management function) e la funzione di revisione interna (internal audit)".*

Sebbene il documento in consultazione sarà inserito nella Circolare n. 263 del 27 dicembre 2006, recante *"Nuove disposizioni di vigilanza prudenziale per le banche"*, in sostituzione della parte riguardante *"La gestione e il controllo dei rischi. Ruolo degli organi aziendali"*, pare opportuno richiamare l'attenzione sul **mancato ed esplicito riferimento alla "Funzione antiriciclaggio" tra le "funzioni aziendali di controllo".**

La Funzione Antiriciclaggio è, infatti, istituita nell'ambito del Sistema dei Controlli Interni della Banca, coordinato nelle sue componenti attraverso idonei flussi informativi.
Nell'ambito del progetto di adeguamento al Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, emanato da Banca d'Italia il 10/03/2011 ai sensi dell'art. 7, comma 2, del D.lgs. 231/07, la succitata Funzione sovrintende all'obbligo di prevenzione e gestione del rischio di riciclaggio, che assume rilievo - come rischio di natura legale e reputazionale - anche sotto il profilo del rispetto della regolamentazione prudenziale. Quest'ultima, a sua volta, impone di fronteggiare i rischi con un idoneo assetto organizzativo e un'adeguata dotazione patrimoniale.

*****

Titolo V – Capitolo 7 – Sezione I – Paragrafo 6

Principi generali, pag. 4

"Il sistema dei controlli interni è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il conseguimento delle seguenti finalità:

- *verifica dell'attuazione delle strategie e delle politiche aziendali;*
- *contenimento del rischio entro il limite massimo accettato ("tolleranza al rischio" o "appetito per il rischio");*
- *salvaguardia del valore delle attività e protezione delle perdite;*
- *efficacia ed efficienza dei processi aziendali;*
- *affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;*
- ***prevenzione del rischio che la banca sia coinvolta, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse con il riciclaggio, l'usura ed il finanziamento al terrorismo);***
- *conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne".*

Nel riportato paragrafo riguardante i principi generali che permeano il sistema dei controlli interni si fa esplicito riferimento alla prevenzione del rischio che la banca sia coinvolta, anche involontariamente, in attività illecite, con particolare riferimento a quelle connesse con il riciclaggio, l'usura ed il finanziamento al terrorismo.

Alla Funzione antiriciclaggio sono assegnate attività complesse ed eterogenee che impattano trasversalmente sul funzionigramma aziendale e qualificabili come: attività di natura legale, attività con valenza organizzativa, attività di natura operativa, attività di controllo, attività formativa.

Appare dunque indispensabile considerare il ruolo della Funzione antiriciclaggio nell'ambito del provvedimento posto in consultazione. Quanto detto dovrebbe indurre a riportare un esplicito riferimento alla succitata Funzione tra quelle aziendali di controllo, stante la sua centralità nel sistema dei controlli interni.

*****

Titolo V – Capitolo 7 – Sezione II – Paragrafo 4

Organo con funzione di controllo, pag. 13

"(...) L'organo con funzione di controllo svolge altresì le funzioni dell'organismo di vigilanza - previsto ai sensi della legge n. 231/2001, in materia di responsabilità amministrativa degli enti - che vigila sul funzionamento e l'osservanza dei modelli di organizzazione e di gestione di cui si dota la banca per prevenire i reati rilevanti ai fini della medesima legge. Ove vi siano particolari e motivate esigenze, le banche possono affidare tali funzioni a un organismo appositamente istituito".

Si osserva come si dovrebbe lasciare la possibilità agli intermediari finanziari di scegliere di munirsi di un apposito Organismo di Vigilanza ex D.lgs. 231/2001 o di attribuire le funzioni di questo all'Organo di controllo, a prescindere da particolari e motivate esigenze. Ciò sulla base del fatto che l'attività svolta dall'Organismo di Vigilanza richiede competenze peculiari non sempre riscontrabili nei membri degli organi di controllo.

*****

Titolo V – Capitolo 7 – Sezione III – Paragrafi 1, 2 e 3

Istituzione delle funzioni aziendali di controllo. Programmazione e rendicontazione dell'attività di controllo. Requisiti specifici delle funzioni aziendali di controllo, pagg. 15 - 22

Si ritiene necessario l'inserimento nei paragrafi suddetti della Funzione antiriciclaggio fra le funzioni aziendali di controllo. Il *"Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, ai sensi dell'art. 7, comma 2, del decreto legislativo 21 novembre 2007, n. 231"*, pubblicato dalla Banca d'Italia in data 10 marzo 2011, infatti, impone agli intermediari finanziari di dotarsi di una funzione specificatamente deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo.

Anche la Funzione antiriciclaggio, difatti, organizzata in coerenza con il principio di proporzionalità, deve essere indipendente e dotata di risorse qualitativamente e quantitativamente adeguate ai compiti da svolgere. I Responsabili della Funzione antiriciclaggio devono essere in possesso di adeguati requisiti di indipendenza, autorevolezza e professionalità. Questi devono rientrare a tutti gli effetti nel novero dei responsabili di funzioni aziendali di controllo e le persone incaricate della Funzione non devono avere responsabilità dirette di aree operative né essere gerarchicamente dipendenti da soggetti responsabili di dette aree.

*****

Titolo V – Capitolo 7 – Sezione IV – Paragrafo 1

Principi generali e requisiti particolari, pagg. 23 – 26

Si suggerisce di menzionare la Funzione antiriciclaggio anche all'interno del presente paragrafo. Secondo quanto stabilito dal Provvedimento di Banca d'Italia del 10 marzo 2011 (capitolo secondo, sezione I, paragrafo 4, pag. 18), lo svolgimento della Funzione antiriciclaggio può essere affidato a soggetti esterni dotati di idonei requisiti in termini di professionalità, autorevolezza e indipendenza. L'esternalizzazione deve essere formalizzata in un accordo che definisca almeno: la compiuta indicazione degli obiettivi da perseguire; la frequenza minima dei flussi informativi nei confronti del referente interno e degli organi di vertice e di controllo aziendali; gli obblighi di riservatezza; la possibilità di rivedere le condizioni del servizio al verificarsi di modifiche normative o nell'operatività e nell'organizzazione dell'impresa esternalizzante; la possibilità per le Autorità di Vigilanza e la UIF di accedere alle informazioni utili per l'attività di supervisione e controllo; l'obbligo di nominare un responsabile interno con il compito di monitorare le modalità di svolgimento del servizio da parte dell'outsourcer.

*****

Titolo V – Capitolo 7 – Sezione IV – Paragrafo 2

Esternalizzazione del trattamento del contante, pag. 26

Si sottolinea l'importanza della menzione della Funzione antiriciclaggio fra le funzioni aziendali di controllo atte al monitoraggio e alla valutazione delle procedure seguite per l'allacciamento e la gestione dei rapporti di esternalizzazione del trattamento del contante. Ciò in ragione dei rischi di riciclaggio sottesi all'attività di trattamento del contante.

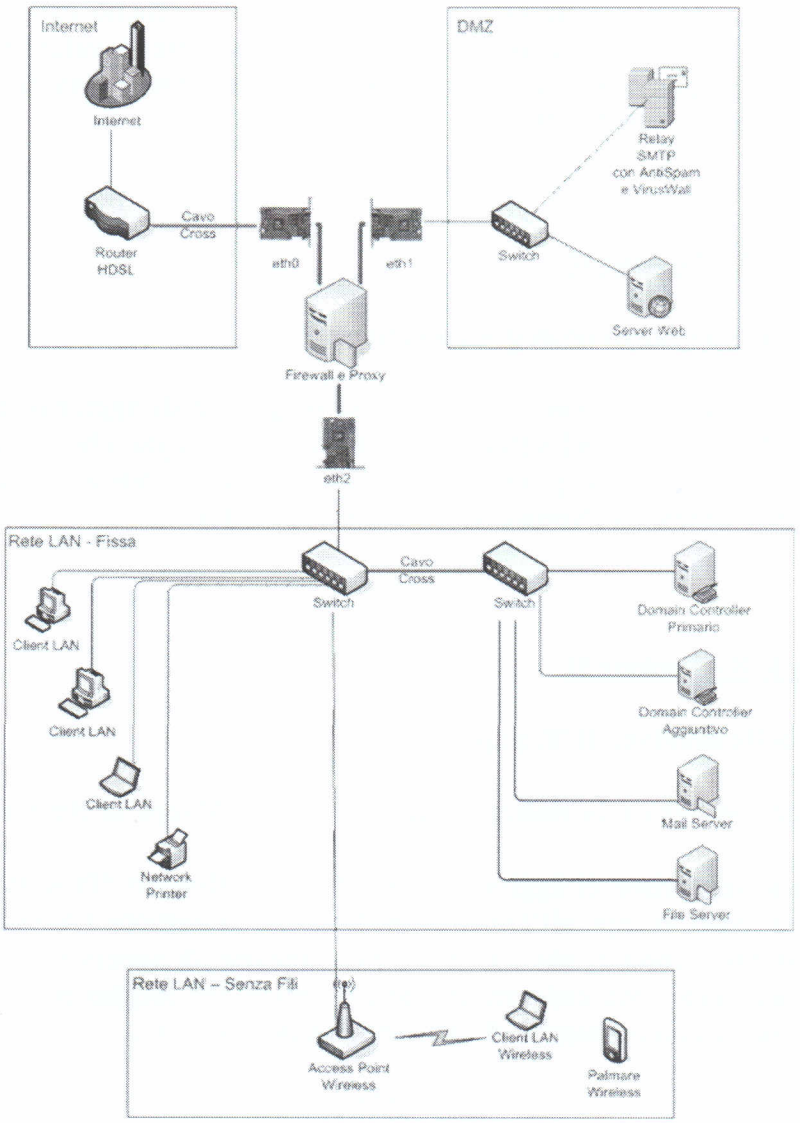
In ogni caso si ritiene opportuno suggerire l'esplicitazione, con elenco tassativo, delle attività esternalizzabili.

*****

Titolo V – Capitolo 8 – Sezione I

Premessa, fonti normative, destinatari della disciplina, definizioni, pag. 44 – 46

Si ritiene preliminarmente indispensabile, per una corretta valutazione della situazione ICT, prevedere la realizzazione di un Progetto/Mappa di Rete per l'infrastruttura esistente, o in fase di realizzazione, all'interno dell'intermediario.
Il Progetto/Mappa di Rete, come da esempio allegato, mette in luce:



- Schema logico della rete: schema che mostra le eventuali suddivisioni della rete in subnets, dispositivi connessi con la descrizione dei servizi, e l'assegnazione degli indirizzi IP.

- Schema fisico della rete: schema che mostra come sono impostate le effettive connessioni di rete tra i dispositivi. Mostra inoltre i dettagli dei dispositivi di rete (numero di porte e la loro velocità, collegamenti di rete, MAC Address, marca e modello, eventuali parametri di accesso).

- Servers e Workstations: questa analisi produce documentazioni dettagliate di tutti i server e le postazioni connesse alla rete. La documentazione comprenderà un dettaglio delle

componenti hardware e software installate sui PC e la configurazione di rete del PC. La documentazione dovrà riportare anche il numero di licenza per il software installato, il numero di versione dello stesso e la data dell'ultimo aggiornamento che lo riguarda.

- Servizi Server: questa analisi esamina i servizi installati sui server e ne produce una documentazione. La documentazione comprenderà la configurazione dei servizi attivi.

Il progetto di Rete è indispensabile per valutare correttamente i punti strategici di collegamento e di vulnerabilità dell'infrastruttura ICT. Esso ha anche la funzione di permettere un più rapido e corretto inventario degli strumenti Hardware e Software, con la conseguente necessaria aggiornata conoscenza degli elementi obsoleti o in fase di obsolescenza. Ricordiamo inoltre che l'inventario delle componenti di un sistema ICT è indispensabile per una corretta valutazione delle misure minime ed idonee per l'adeguamento agli standard dettati dalla normativa in materia di Privacy e Sicurezza dei Dati personali e sensibili (D.lgs. 196/2003).

*****

Titolo V – Capitolo 8 – Sezione II

Compiti dell'organo con funzione di gestione, pag. 49

"(...) pone in atto opportune azioni correttive", si suggerisce di aggiungere la locuzione *"e preventive"*, utilizzando il metodo del sistema di gestione della qualità, che prevede l'adozione di misure correttive, atte a correggere un problema, ed azioni preventive, atte a correggere le cause che generano un determinato problema (Normativa UNI EN ISO 9000).

*****

Titolo V – Capitolo 8 – Sezione II

Organizzazione della funzione ICT, pag. 49

Si ritiene opportuno assegnare la realizzazione del Progetto/Mappa di Rete all'Organizzazione della Funzione ICT.

Di conseguenza si suggerisce di aggiungere la "Mappa di Rete" o "Progetto di Rete" (di cui sopra) fra i documenti posti in capo all'Organo con funzione di gestione (Allegato A, pag. 61 del documento). Si suggerisce, inoltre, che l'Organo con funzione di supervisione strategica venga informato circa il documento, con cadenza annuale, in modo che meglio possa *"promuovere gli strumenti, emanare linee guida in materia di approvvigionamento (...)"*.

*****

Titolo V – Capitolo 8 – Sezione III

La gestione del rischio informatico, pag. 51

Fra gli avvenimenti da documentare, previsti per la gestione del rischio informatico, si suggerisce di introdurre quelli relativi agli incidenti per la sicurezza; quindi l'introduzione di un registro che dovrebbe contemplare: data, ora, utente che rileva il problema, descrizione, categoria (segnalazione antivirus, anomalia, perdita di un dato, presenza di phishing in posta elettronica, ecc.). Un registro di siffatta specie risulta infatti indispensabile per verificare punti deboli del sistema o ricorrenza di determinati avvenimenti.

Il registro, compilato di volta in volta, dovrebbe poi essere presentato, almeno con cadenza annuale, all'Organo con funzione di gestione per la verifica degli incidenti.

*****

Titolo V – Capitolo 8 – Sezione IV

Policy di sicurezza, pag. 52

Si ritiene opportuno integrare la frase: *"i principi generali sull'utilizzo e la gestione dei sistemi informatici da parte dei diversi profili aziendali"* con *"Tali principi dovranno prevedere l'assegnazione di profili di autorizzazione per i sistemi informatici, profili attribuiti nel rispetto di quelli aziendali, da documentare e rivedere periodicamente, almeno annualmente, per verifica della sussistenza degli stessi"*. Questo nel rispetto di quanto previsto dal punto 13 dell'Allegato B del D.lgs. 196/2003.

La documentazione circa l'attribuzione dei profili e la verifica della sussistenza, con cadenza almeno annuale, dovrebbe rientrare fra i documenti previsti a pag. 51.

*****

Titolo V – Capitolo 8 – Sezione IV

La sicurezza dei dati e il controllo degli accessi, pagg. 52 - 53

La regolamentazione dell'accesso logico ai sistemi deve assicurare al titolare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato tale da rendere indispensabile e indifferibile intervenire per necessità di operatività e di sicurezza del sistema; ciò ai sensi di quanto disposto dal punto 10 dell'Allegato B al D.lgs. 196/2003. Essendo al giorno d'oggi possibili tecniche di accesso al sistema tramite azzeramento della password dell'incaricato, ovvero attraverso la custodia delle password da parte del custode delle password, è necessario che la procedura sia descritta in questo contesto.

Si suggerisce di modificare il terzo punto dell'elenco (pag. 53 del documento) come segue: *" - la procedura di autenticazione per l'accesso alle applicazioni e ai sistemi informatici; in particolare,* ***anche in tempi diversi per quanto riguarda nello specifico il codice di identificazione,*** *devono essere garantite l'univoca associazione a ciascun utente delle proprie credenziali di accesso (...)"*.

Questo nel rispetto di quanto previsto dal punto 6 dall'Allegato B del D.lgs. 196/2003.

Sempre con riferimento al medesimo punto, si dovrebbe ricordare la necessità di disattivare (e non cancellare, in quanto serve avere memoria delle credenziali per non associarle ad altri utenti, nemmeno in tempi diversi) le credenziali di autenticazione non utilizzate per almeno sei mesi, a meno di quelle preventivamente autorizzate per soli scopi di gestione tecnica. Questo nel rispetto di quanto previsto dal punto 7 dell'Allegato B del D.lgs. 196/2003.

Ancora, allo stesso punto, in ossequio a quanto previsto dal punto 5 dell'Allegato B del D.lgs. 196/2003, si suggerisce di rimarcare la circostanza che la password debba essere modificata autonomamente dall'utente al primo accesso e, in seguito, regolarmente. Ciò poiché, nelle verifiche, emerge come questa operazione di rado venga eseguita in modo corretto.

*****

Titolo V – Capitolo 8 – Sezione IV

La gestione dei cambiamenti, pag. 54

Riguardo la gestione dei cambiamenti, si suggerisce di aggiungere un punto in elenco: *"La procedura completa di collaudo ed attività di messa in produzione per gli aggiornamenti annuali/semestrali dei programmi per elaboratori"*. Aggiornamento previsto per legge nel rispetto di quanto previsto dal punto 17 dell'Allegato B del D.lgs. 196/2003.

*****

Titolo V – Capitolo 8 – Sezione IV

La gestione degli incidenti di sicurezza, pag. 55

Si rimarca la necessità di una registrazione sintetica di tutti gli incidenti di sicurezza, che dovrebbe contemplare: data, ora, utente che rileva il problema, descrizione, categoria (segnalazione antivirus, anomalia, perdita di un dato, presenza di phishing in posta elettronica, ecc.). Questo come materiale in ingresso alla valutazione dei rischi informatici.

*****

Titolo V – Capitolo 8 – Sezione VI

Indicazioni particolari, pag. 59

Con riferimento al Cloud Computing:

- esiste un quarto tipo di tipologia di implementazione che è il Cloud Ibrido:
  Il cloud Ibrido è una combinazione del modello pubblico e di quello privato, ovvero è un modello in cui l'utente utilizza risorse sia del suo cloud privato che di un cloud pubblico. Il cloud Ibrido può essere utilizzato con successo in vari casi.

- Per quanto riguarda la sicurezza ICT, lo stesso D.lgs. 196/2003, prevede, ad esempio, il backup dei dati, ossia una forma di ridondanza dell'informazione, come misura minima di sicurezza da osservare. Aggiungiamo ciò che lo stesso Garante per la Privacy ha ribadito nella recente *"Scheda di documentazione cloud computing: indicazioni per l'utilizzo consapevole dei servizi"* e cioè che: *"nel caso in cui i dati trattati non siano i propri, come avviene per aziende e pubbliche amministrazioni che raccolgono e detengono informazioni di terzi, l'adozione di servizi che non offrono adeguate garanzie di riservatezza e di continuità operativa può avere rilevanti ripercussioni nel patrimonio informativo dei soggetti cui i dati si riferiscono. In tal senso, il titolare del trattamento dei dati a fronte del contenimento di costi dovrà comunque provvedere al salvataggio (backup) dei dati allocati nel cloud, ad esempio creandone una copia locale (eventualmente sotto forma di archivio compresso), allo scopo di gestire gli eventuali rischi insiti nell'acquisizione di servizi che, pur con i vantaggi dell'economicità, potrebbero tuttavia non offrire sufficienti garanzie di affidabilità e di disponibilità."*. In aggiunta a questo, si ricorda come i D.lgs. 82/2005 e 235/2010 contengano prescrizioni orientate al mantenimento di continuità operativa e al disaster recovery con forme di ridondanza dei dati.

- **Potenziali rischi per la sicurezza.** Si ricorda inizialmente come alcuni rischi per la sicurezza del cloud siano comuni anche ad altre tipologie di gestione in outsourcing, mentre altri siano

propri di questa specifica modalità di fornitura. Tra i principali rischi che si devono affrontare si possono rimarcare:

1. *Perdita di governance*: poiché il cliente intermediario necessariamente cede al fornitore il controllo di una serie di aspetti che interessano le difese di sicurezza. Egli potrebbe perdere il controllo su dove effettivamente risiedano i suoi dati all'interno di un Cloud Provider.

2. *Problemi nella migrazione*: l'immaturità o l'assenza di strumenti, considerati standard e formati da template di esportazione/importazione dati, rende difficile migrare da un fornitore ad un altro.

3. *Errore nell'isolamento*: per ottenere i vantaggi nelle economie di scala, il cloud provider mette in comune le risorse tra più clienti e poi ne consente l'accesso per la sola parte di specifica competenza (isolamento). Esiste quindi la possibilità che a seguito di un attacco, o per un errore, tale separazione venga meno compromettendo la riservatezza e l'accountability.

4. *Controllo del servizio*: dal punto di vista dell'organizzazione e del controllo può capitare che il fornitore non possa fornire evidenza della propria compliance o non permetta audit da parte del cliente.

5. *Protezione dei dati*: potrebbe essere difficile per il cliente intermediario controllare che i dati siano utilizzati legalmente e quale sia la loro reale collocazione nella struttura.

6. *Distruzione dei dati e supporti*: quando venisse fatta una richiesta di cancellare una risorsa, essa potrebbe essere rimossa ma non effettivamente distrutta e resa irrecuperabile. Quando venisse richiesto di cancellare definitivamente dei dati, backup o di distruggere i supporti fisici si potrebbe scoprire che questi contengono anche le informazioni relative ad altri utenti intermediari, in ragione dell'Isolamento descritto prima.

7. *Conoscenza dell'organizzazione*: problemi derivanti da mancato controllo degli amministratori di sistema in seno ad un'organizzazione che fornisce servizi Cloud. Controllo previsto dalle delibere del Garante della Privacy sugli amministratori di sistema (Provvedimento del Garante del 27 novembre 2008, relativo a *"misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*, pubblicato sulla G.U. n. 300 del 24 dicembre 2008; e Provvedimento del Garante del 12 febbraio 2009, pubblicato sulla G.U. n. 45 del 24 febbraio 2009, con il quale sono stati unificati e contestualmente prorogati i termini per l'adempimento delle prescrizioni contenute nel citato provvedimento del 27 novembre 2008).