Autorità bancaria europea

ABE BS 2011 116 definitivo

27 settembre 2011

Orientamenti ABE sull'organizzazione interna (GL 44)

Londra, 27 settembre 2011

Orientamenti ABE sull'organizzazione interna

Oggetto degli orientamenti

1. Il presente documento contiene orientamenti emanati ai sensi dell'articolo 16 del regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione ("regolamento ABE"). Conformemente all'articolo 16, paragrafo 3, del regolamento ABE, le autorità competenti e gli operatori dei mercati finanziari compiono ogni sforzo per conformarsi agli orientamenti.

2. Gli orientamenti presentano il parere dell'ABE in merito alle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione in una particolare area. L'ABE si attende pertanto che tutte le autorità competenti e gli operatori dei mercati finanziari si conformino agli orientamenti loro rivolti, salvo contrario avviso. Le autorità competenti sono tenute a conformarsi agli orientamenti che si applicano ad esse mediante il loro inserimento nelle rispettive prassi di vigilanza (ad esempio modificando il proprio quadro giuridico o le proprie norme di vigilanza e/o le procedure di orientamento o vigilanza), anche quando particolari orientamenti contenuti nel documento si rivolgono in primo luogo agli enti creditizi e alle imprese di investimento (di seguito "enti").

Obblighi di notifica

3. Le autorità competenti sono tenute a notificare all'ABE entro il 28 novembre 2012 se sono conformi o se intendono conformarsi agli orientamenti in questione, in alternativa sono tenute a indicare le ragioni della mancata conformità. Le notifiche devono essere inviate da persone autorizzate a segnalare all'ABE la conformità per conto delle autorità competenti all'indirizzo compliance@eba.europa.eu.

4. La notifica delle autorità competenti di cui al precedente paragrafo è pubblicata sul sito web dell'ABE, ai sensi dell'articolo 16 del regolamento ABE.

Nel testo degli orientamenti vengono fornite note esplicative su specifici aspetti, che offrono esempi oppure illustrano le motivazioni alla base di una disposizione. Laddove presenti, le note esplicative appaiono in una casella di testo incorniciata.

Indice

Titolo I - Oggetto, ambito di applicazione e definizioni

1. Oggetto

Gli orientamenti hanno lo scopo di armonizzare le aspettative della vigilanza e di promuovere la corretta attuazione dei dispositivi di governo in linea con l'articolo 22 e l'allegato V della direttiva 2006/48/CE e il diritto societario nazionale dei vari paesi.

2. Ambito e livello di applicazione

1. Le autorità competenti devono richiedere agli enti di conformarsi alle disposizioni contenute nei presenti orientamenti in materia di organizzazione interna.
2. Le autorità competenti esaminano l'applicazione dei presenti orientamenti nell'ambito del proprio processo di revisione e valutazione prudenziale.

Nota esplicativa
Il CEBS e l'ABE hanno emanato orientamenti sul processo di revisione prudenziale, disponibili sul sito web dell'ABE.

3. I presenti orientamenti si applicano agli enti a livello individuale e alle capogruppo e controllate a livello consolidato o subconsolidato, salvo contrario avviso.
4. A tutte le disposizioni contenute negli orientamenti si applica il principio di proporzionalità stabilito nella direttiva 2006/48/CE e nella direttiva 2006/49/CE (modificate). Un ente è in grado di dimostrare in quale modo il proprio modello di governo, che tiene conto della natura, della portata e della complessità delle attività svolte, è conforme agli obiettivi fissati dagli orientamenti.

3. Definizioni

1. Nei presenti orientamenti, per "organo gestorio" di un ente si intende: l'organo direttivo (o gli organi direttivi) con funzione di supervisione strategica e di gestione, che costituisce la massima autorità decisionale ed è responsabile della determinazione degli indirizzi strategici, degli obiettivi aziendali e della direzione generale dell'ente. L'organo gestorio deve essere composto dalle persone che dirigono effettivamente le attività dell'ente.
2. Nei presenti orientamenti, per "enti" si intendono gli enti creditizi e le imprese di investimento ai sensi della direttiva 2006/48/CE e della direttiva 2006/49/CE.

Titolo II – Requisiti relativi alla organizzazione interna degli enti

A. Struttura e organizzazione aziendali

4. Quadro organizzativo

1. L'organo gestorio di un ente deve assicurare una struttura aziendale trasparente e idonea a tale ente. La struttura deve promuovere e attestare la gestione efficace e prudente dell'ente sia a livello individuale sia consolidato. I flussi informativi e l'allocazione delle responsabilità e dei poteri devono essere chiari, adeguatamente definiti, coerenti e attuati.
2. L'organo gestorio deve garantire che la struttura dell'ente e, ove applicabile, le strutture del gruppo siano trasparenti e chiare sia al personale dell'ente, sia alle competenti autorità di vigilanza.
3. L'organo gestorio deve valutare in quale modo i vari elementi della struttura aziendale si integrano e interagiscono tra loro. La struttura non deve impedire all'organo gestorio di monitorare e gestire efficacemente i rischi che l'ente o il gruppo assume.
4. L'organo gestorio deve valutare l'impatto che modifiche alla struttura del gruppo possono avere sulla solidità di esso, e provvedere rapidamente agli adeguamenti necessari.

> Nota esplicativa
>
> Le modifiche possono derivare, ad esempio, dalla costituzione di nuove controllate, da fusioni e acquisizioni, dalla vendita o dalla liquidazione di parti del gruppo, o possono essere dovute a fattori esterni.

5. Sistema dei controlli (checks and balances) nei gruppi

1. Nella struttura di un gruppo, l'organo gestorio della capogruppo di un ente è responsabile dell'adeguata organizzazione interna del gruppo e deve garantire che vi sia un sistema di governo adatto alla struttura, alle attività e ai rischi del gruppo e delle sue componenti.
2. A livello di entità giuridica, l'organo gestorio di una filiazione regolamentata di un gruppo deve conformarsi ai medesimi principi e politiche di organizzazione interna della capogruppo, salvo ove diversamente disposto da norme di legge, disposizioni di vigilanza e in base al principio di proporzionalità. Ne consegue che l'organo gestorio di una filiazione regolamentata deve, nell'ambito delle proprie responsabilità in materia di organizzazione interna, fissare le proprie politiche, e valutare tutte le decisioni o le prassi adottate a livello consolidato al fine di garantire che esse non comportino per la filiazione regolamentata una violazione delle norme di legge o delle disposizioni di vigilanza applicabili o della disciplina prudenziale. L'organo gestorio della filiazione regolamentata deve anche garantire che tali decisioni e prassi non siano di ostacolo:

a. alla sana e prudente gestione della filiazione;

b. alla solidità finanziaria della filiazione; o

c. agli interessi legali degli azionisti della filiazione.

3. Gli organi gestori della capogruppo e delle sue controllate devono applicare quanto riportato nei seguenti paragrafi e tenerne conto nel considerare gli effetti della dimensione del gruppo sulla propria organizzazione interna.
4. Nello svolgimento dei propri compiti di organizzazione interna, l'organo gestorio della capogruppo di un ente deve essere consapevole di tutti i rischi rilevanti e degli aspetti di rilievo che possono influire sul gruppo, sulla capogruppo stessa e sulle filiazioni. L'organo gestorio deve pertanto esercitare un adeguato controllo sulle filiazioni, rispettando le indipendenti responsabilità legali e di governo degli organi gestori delle controllate regolamentate.
5. Per svolgere i propri compiti in materia di organizzazione interna, l'organo gestorio di un ente capogruppo deve:

   a. istituire un assetto di governo che contribuisca a garantire un'efficace attività di controllo delle filiazioni e tenga conto della natura, delle dimensioni e della complessità dei diversi rischi cui il gruppo e le controllate sono esposti;

   b. approvare una politica aziendale di governo a livello consolidato per le controllate, che includa l'impegno a rispettare tutti i requisiti stabiliti in materia di organizzazione e governo;

   c. garantire che, per ogni controllata, siano disponibili risorse sufficienti al rispetto degli standard in materia di organizzazione e governo a livello consolidato e individuale;

   d. disporre di mezzi idonei a verificare che ogni controllata sia conforme a tutti i requisiti stabiliti in materia di organizzazione interna; e

   e. garantire che i flussi informativi all'interno di un gruppo siano chiari e trasparenti, soprattutto nei casi in cui le linee di business non corrispondono alla struttura giuridica del gruppo.

6. Una controllata regolamentata dovrebbe considerare come elemento di forte organizzazione e governo quello di disporre di un numero sufficiente di membri indipendenti nell'organo gestorio. Per membri indipendenti dell'organo gestorio si intendono i consiglieri non esecutivi che sono indipendenti dalla controllata e dal rispettivo gruppo, nonché dal socio di controllo.

6. Conoscenza della propria struttura

1. L'organo gestorio deve conoscere e comprendere a pieno la struttura operativa dell'ente (c.d. Know-your-structure) e garantire che esso sia in linea con la gestione sociale approvata e con il profilo di rischio dell'ente.

Nota esplicativa

È fondamentale che l'organo gestorio conosca e comprenda a pieno la struttura operativa dell'ente. Qualora all'ente facciano capo molte entità giuridiche all'interno del gruppo, il loro numero e, in modo particolare, le interconnessioni e operazioni tra loro possono costituire un problema per la definizione dell'organizzazione interna dell'ente e per la gestione e il controllo dei rischi del gruppo nel suo complesso, la qual cosa rappresenta di per sé un rischio.

2. L'organo gestorio deve guidare e comprendere la struttura dell'ente, la sua evoluzione e i suoi limiti, e deve garantire che la struttura sia giustificata e non abbia un grado di complessità eccessiva o inopportuna. L'organo gestorio è anche responsabile dell'approvazione di sani indirizzi strategici e politiche aziendali per lo stabilimento di nuove strutture. Analogamente, l'organo gestorio deve riconoscere i rischi derivanti dalla complessità strutturale dell'entità giuridica e garantire che l'ente sia in grado di fornire in maniera tempestiva informazioni riguardanti la tipologia, l'organigramma, gli assetti proprietari e le attività di ogni entità giuridica.
3. L'organo gestorio di un ente capogruppo deve comprendere non solo l'organizzazione societaria del gruppo, ma anche gli obiettivi delle diverse entità che lo compongono, e i legami e i rapporti tra loro esistenti. Ciò include la comprensione dei rischi operativi specifici del gruppo, delle esposizioni intragruppo e di come il funding, il profilo patrimoniale e quello di rischio potrebbero esserne influenzati in condizioni normali e avverse.
4. L'organo gestorio di un ente capogruppo deve garantire che le varie entità del gruppo (compreso lo stesso ente) ricevano informazioni sufficienti a consentire loro di avere una chiara percezione degli obiettivi e dei rischi generali del gruppo. Tutti i flussi informativi tra le entità che sono significativi e rilevano per il funzionamento operativo del gruppo dovrebbero essere documentati e tempestivamente accessibili, su richiesta, all'organo gestorio, alle funzioni di controllo e alle autorità di vigilanza, se del caso.
5. L'organo gestorio di un ente capogruppo deve assicurarsi di essere informato sui rischi derivanti dalla struttura del gruppo. Ciò include:
   a. informazioni sui principali fattori di rischio, e
   b. relazioni periodiche per la valutazione della struttura complessiva dell'ente e del grado di conformità delle attività delle singole entità rispetto agli indirizzi strategici approvati.

7. Attività non standard o non trasparenti

1. Qualora un ente operi mediante società veicolo o strutture correlate o in giurisdizioni che ostacolano la trasparenza o non rispettano gli standard bancari internazionali, l'organo gestorio è tenuto a comprendere gli obiettivi e la struttura di tali entità, nonché i rischi specifici associati ad esse. L'organo

gestorio deve accettare tali attività solo dopo essersi accertato che i rischi sono gestiti in maniera adeguata.

Nota esplicativa

Oltre a tale principio, le autorità competenti possono anche applicare i "Principi fondamentali per un'efficace vigilanza bancaria", elaborati dal Comitato di Basilea per la vigilanza bancaria, quando valutano attività aziendali in giurisdizioni non del tutto trasparenti o che non rispettano gli standard bancari internazionali.

L'ente può avere motivi legittimi per operare in talune giurisdizioni (o con entità o controparti che operano in tali giurisdizioni) o per istituire particolari strutture (ad esempio società veicolo o trust societari). Tuttavia, operare in giurisdizioni non del tutto trasparenti o che non rispettano gli standard bancari internazionali (ad esempio in ambito di vigilanza prudenziale, fisco, contrasto al fenomeno del riciclaggio di denaro e lotta al finanziamento del terrorismo), o operare mediante strutture complesse o non trasparenti può esporre a specifici rischi legali, reputazionali e finanziari. Tali strutture possono anche ostacolare la capacità dell'organo gestorio di condurre un adeguato controllo delle attività e interferire con l'esercizio di un'efficace vigilanza bancaria. Pertanto, esse devono essere approvate e mantenute solo se ne sono stati definiti e compresi gli obiettivi, se ne è stato garantito un controllo efficace e se tutti i rischi specifici associati, che tali strutture potrebbero comportare, possono essere adeguatamente gestiti.

Ne consegue che l'organo gestorio deve prestare particolare attenzione a tutte queste situazioni che possono complicare la comprensione della struttura del gruppo.

2. L'organo gestorio deve istituire, mantenere e riesaminare, su base continuativa, indirizzi strategici, politiche aziendali e procedure idonei a disciplinare i meccanismi per l'approvazione e il mantenimento di tali strutture e attività, al fine di garantire che esse siano coerenti con i loro obiettivi.
3. L'organo gestorio deve garantire che siano intraprese opportune misure per evitare o mitigare i rischi di tali attività. Ciò include che:

    a. l'ente disponga di politiche aziendali e procedure adeguate e di processi documentati (ad esempio i limiti operativi applicabili, i requisiti informativi) per la valutazione, l'approvazione e la gestione dei rischi di tali attività, avendo presenti le conseguenze per la struttura operativa del gruppo;

    b. le informazioni riguardanti tali attività e i relativi rischi siano accessibili alla direzione generale e ai revisori (audit) dell'ente e siano portate a conoscenza dell'organo gestorio e delle autorità di vigilanza;

c. l'ente valuti periodicamente il persistere della effettiva necessità di svolgere attività che ostacolano la trasparenza.

4. Le stesse misure devono essere adottate quando un ente svolge attività non standard o non trasparenti per la clientela.

Nota esplicativa
Le attività non standard o non trasparenti per la clientela (ad esempio aiutare i clienti a costituire società veicolo in giurisdizioni off-shore; istituire strutture complesse ed effettuare operazioni finanziarie per loro conto o fornire servizi fiduciari) comportano problemi per l'organizzazione interna e possono esporre a considerevoli rischi operativi e reputazionali. Devono pertanto essere utilizzate le stesse misure di gestione dei rischi che sono adottate per le attività aziendali proprie dell'ente.

5. Tutte le strutture e le attività menzionate devono essere sottoposte a regolari revisioni da parte della revisione interna ed esterna.

B. Organo gestorio

B.1 Doveri e responsabilità dell'organo gestorio

8. Responsabilità dell'organo gestorio

1. L'organo gestorio è complessivamente responsabile dell'ente e definisce gli indirizzi strategici di esso. Le responsabilità dell'organo gestorio sono chiaramente definite in un documento scritto e approvate.

Nota esplicativa
Il corretto esercizio delle responsabilità dell'organo gestorio è la base per la sana e prudente gestione dell'ente. Le responsabilità documentate devono inoltre essere in linea con il diritto societario nazionale.

2. Tra le principali responsabilità dell'organo gestorio dovrebbero essere incluse le funzioni di indirizzo e supervisione riguardanti:

   a. la gestione sociale dell'ente nell'ambito del quadro giuridico e normativo applicabile, tenuto conto degli obiettivi finanziari di lungo periodo e della solvibilità dell'ente;

   b. gli indirizzi strategici e le politiche generali dell'ente per il governo dei rischi, compresi la tolleranza al rischio/appetito per il rischio e l'assetto per la gestione dei rischi dell'ente;

   c. l'ammontare, il tipo e la distribuzione di capitale interno e fondi propri adeguati a fronteggiare i rischi dell'ente;

d. una struttura organizzativa solida e trasparente dotata di efficaci canali di comunicazione e di reporting;

e. una politica per la nomina e la successione di coloro che rivestono ruoli chiave all'interno dell'ente;

f. uno schema di remunerazione in linea con gli indirizzi strategici di governo dei rischi dell'ente;

g. i principi di governo societario e i valori di impresa dell'ente, anche mediante un codice etico o un documento equivalente; e

h. un sistema dei controlli interni adeguato ed efficace, che includa funzioni di controllo dei rischi, di conformità alle norme e di revisione interna (internal audit) e ne garantisca il corretto funzionamento, e un adeguato sistema per la rendicontazione finanziaria e la contabilità.

3. L'organo gestorio dovrebbe anche riesaminare periodicamente e adeguare le politiche aziendali e gli indirizzi strategici. L'organo gestorio ha il compito di garantire una comunicazione adeguata con le autorità di vigilanza e altre parti interessate.

9. Valutazione dell'organizzazione interna

1. L'organo gestorio monitora e valuta periodicamente l'efficacia dell'organizzazione interna dell'ente.
2. Con cadenza almeno annuale deve essere svolta una revisione dell'assetto organizzativo interno e della sua attuazione, ponendo particolare attenzione a tutti i cambiamenti dovuti a fattori interni ed esterni che influiscono sull'ente.

10. Funzioni di gestione e di supervisione strategica dell'organo gestorio

1. Deve esservi un'efficace interazione tra le funzioni di gestione e di supervisione strategica dell'organo gestorio dell'ente.

Nota esplicativa

Di norma negli Stati membri si utilizza uno dei seguenti due **modelli di governo**: quello monistico o quello dualistico. In entrambi i modelli, l'organo con funzione di gestione e l'organo con funzione di supervisione strategica svolgono il proprio ruolo nella gestione dell'ente, direttamente o tramite la costituzione di comitati.

La funzione di gestione propone gli indirizzi per la direzione dell'ente, garantisce la corretta attuazione degli indirizzi strategici e ha la responsabilità della gestione corrente dell'ente.

La funzione di supervisione strategica vigila sulla funzione di gestione e le fornisce consulenza. Il suo ruolo di supervisione consiste nel fornire un

contributo costruttivo quando si definiscono gli indirizzi strategici di un ente, nel monitorare le prestazioni della funzione di gestione e la realizzazione degli obiettivi concordati, e nel garantire l'integrità delle informazioni finanziarie e efficaci sistemi di gestione del rischio e controlli interni.

Per realizzare un buon assetto di governo, le funzioni di gestione e di supervisione strategica di un ente devono interagire in maniera efficace così da consentire l'attuazione degli indirizzi strategici concordati per l'ente e soprattutto gestire i rischi cui l'ente è esposto. Le differenze rilevanti nei quadri legislativi e regolamentari dei vari paesi non devono ostacolare l'efficace interazione tra queste due funzioni, indipendentemente dal fatto che siano esercitate dallo stesso organo o da organi diversi.

2. L'organo gestorio con funzione di supervisione strategica deve:

   a. essere pronto a, e in grado di mettere alla prova e rivedere in maniera critica e costruttiva le proposte, i chiarimenti e le informazioni forniti dai membri dell'organo gestorio con funzione di gestione;

   b. vigilare che gli indirizzi strategici, la tolleranza al rischio/appetito per il rischio e le politiche aziendali dell'ente siano attuate in maniera coerente e che gli standard di prestazione si mantengano in linea con gli obiettivi finanziari di lungo periodo e la solvibilità dell'ente; e

   c. vigilare sul livello delle prestazioni dei membri dell'organo gestorio con funzione di gestione rispetto a tali standard.

3. L'organo gestorio con funzione di gestione deve coordinare la gestione corrente dell'ente con gli indirizzi strategici di governo dei rischi definiti dall'organo gestorio con funzione di supervisione strategica, e discutere regolarmente con quest'ultimo l'attuazione di tali indirizzi strategici.

4. Ogni funzione deve fornire all'altra informazioni sufficienti. L'organo gestorio con funzione di gestione deve informare con regolarità e in modo esauriente, tempestivamente se necessario, l'organo gestorio con funzione di supervisione strategica in merito agli elementi rilevanti per la valutazione di una determinata situazione, per la gestione dell'ente e per il mantenimento della sua solidità finanziaria.

B.2 Composizione e funzionamento dell'organo gestorio

11. Composizione, nomina e successione dell'organo gestorio

1. L'organo gestorio deve avere un numero adeguato di membri e una composizione appropriata. L'organo gestorio deve disporre di politiche aziendali per la selezione e il monitoraggio dei propri membri, e per la programmazione della loro successione.

2. Un ente deve fissare le dimensioni e la composizione del proprio organo gestorio tenendo conto delle dimensioni e della complessità dell'ente e della natura e dell'ambito delle sue attività. La selezione dei membri dell'organo gestorio deve garantire una sufficiente competenza collettiva.
3. L'organo gestorio deve individuare e selezionare candidati qualificati e dotati di esperienza, e garantire un'adeguata programmazione della successione per l'organo gestorio, prestando la dovuta attenzione a ogni altro requisito giuridico in merito alla composizione, la nomina o la successione.
4. L'organo gestorio deve garantire che un ente disponga di politiche aziendali per la selezione di nuovi membri e la rinomina dei membri esistenti. Tali politiche aziendali dovrebbero includere la descrizione delle competenze e delle abilità necessarie per garantire una professionalità sufficiente.
5. I membri dell'organo gestorio dovrebbero essere nominati per un periodo appropriato. Le candidature per la rinomina dovrebbero essere basate sul profilo cui si fa riferimento sopra e dovrebbero essere presentate soltanto dopo aver attentamente valutato la prestazione offerta da tale membro durante l'ultimo mandato.
6. Quando l'organo gestorio definisce un piano di successione per i propri membri, esso deve considerare la data di scadenza del contratto o mandato di ogni membro al fine di evitare, ove possibile, che troppi membri debbano essere sostituiti contemporaneamente.

12. Commitment, indipendenza e gestione dei conflitti di interesse nell'organo gestorio

1. I membri dell'organo gestorio dovrebbero impegnarsi attivamente nelle attività dell'ente e dovrebbero essere in grado di adottare decisioni e valutazioni proprie che siano fondate, obiettive e indipendenti.
2. La selezione dei membri dell'organo gestorio dovrebbe assicurare che al suo interno siano garantite professionalità e indipendenza sufficienti. Un ente dovrebbe garantire che i membri dell'organo gestorio possano impegnare tempo e sforzi sufficienti ad adempiere le loro responsabilità in maniera efficace.
3. I membri dell'organo gestorio devono avere solo un numero limitato di mandati o di altre attività professionali che richiedono molto tempo. I membri devono inoltre informare l'ente delle loro attività professionali secondarie (ad esempio i mandati in altre imprese). Poiché il presidente ha maggiori responsabilità e doveri, ci si deve aspettare che esso dedichi a tale incarico un tempo maggiore.
4. L'impegno minimo in termini di tempo previsto per tutti i membri dell'organo gestorio dovrebbe essere indicato in un documento scritto. Quando i membri dell'organo gestorio valutano la nomina di un nuovo membro o sono informati di un nuovo mandato da parte di un membro esistente, essi dovrebbero assicurarsi su come tale soggetto intende impiegare tempo sufficiente per adempiere le proprie responsabilità nei confronti dell'ente. Si dovrebbe dare

un'informativa sulla frequenza di partecipazione dei membri dell'organo gestorio con funzione di supervisione strategica. Un ente dovrebbe anche valutare l'opportunità di dare un'informativa sulle assenze prolungate dei membri dell'organo gestorio con funzione di gestione.

5. I membri dell'organo gestorio dovrebbero poter agire in maniera obiettiva, critica e indipendente. Tra le misure intese a rafforzare la capacità di valutazione obiettiva e indipendente si dovrebbe includere l'assunzione dei membri da un numero di candidati sufficientemente ampio e la presenza di un numero sufficiente di membri non esecutivi.

Nota esplicativa
Qualora l'organo gestorio con funzione di supervisione strategica sia formalmente separato dall'organo gestorio con funzione di gestione, devono essere comunque garantite l'obiettività e l'indipendenza dell'organo gestorio con funzione di supervisione strategica mediante una selezione appropriata di membri indipendenti.

6. L'organo gestorio deve avere una politica aziendale scritta per la gestione dei conflitti di interesse che potrebbero insorgere con i suoi membri. Tale politica dovrebbe specificare:

   a. il dovere dei membri di evitare conflitti di interesse che non siano stati comunicati all'organo gestorio e approvati da esso, oppure di garantire che i conflitti siano affrontati in maniera adeguata;

   b. il processo di verifica o di approvazione cui i membri devono sottoporsi prima di intraprendere determinate attività (come ad esempio far parte di un altro organo gestorio) per garantire che il nuovo incarico non comporti un conflitto di interesse;

   c. il dovere dei membri di informare l'ente di ogni situazione che possa provocare, o che ha già provocato, un conflitto di interesse;

   d. la responsabilità dei membri di astenersi dal partecipare a processi decisionali o a votazioni in qualsiasi ambito in cui possa esservi per i membri un conflitto di interesse, oppure quando l'obiettività o la capacità dei membri di assolvere correttamente ai propri doveri nei confronti dell'ente possano essere altrimenti compromesse;

   e. procedure adeguate per le operazioni con parti correlate da effettuare alle condizioni di mercato (on an arm's length basis); e

   f. le modalità in cui l'organo gestorio tratterebbe eventuali casi di non conformità alla politica aziendale.

13. Requisiti dell'organo gestorio

1. I membri dell'organo gestorio devono essere e restare idonei sotto il profilo della professionalità, anche mediante un'adeguata formazione, per le posizioni che rivestono. Essi devono avere una piena comprensione degli assetti di governo dell'ente e del proprio ruolo in essi.
2. I membri dell'organo gestorio, individualmente e collettivamente, dovrebbero possedere le necessarie competenze, esperienze, capacità, conoscenze e qualità personali, tra le quali professionalità e integrità personale, per svolgere correttamente i propri compiti.
3. I membri dell'organo gestorio dovrebbero avere una comprensione aggiornata delle attività aziendali, a un livello commisurato alle proprie responsabilità. Ciò include una conoscenza adeguata dei settori dei quali essi non sono direttamente responsabili, ma sui quali sono chiamati a rispondere collettivamente.
4. I membri dell'organo gestorio dovrebbero avere collettivamente una piena comprensione della natura delle attività aziendali e dei rischi a esse associati, e avere competenze ed esperienze adeguate e appropriate per ciascuna delle attività materiali che l'ente intende svolgere al fine di porre in essere efficaci assetti organizzativi e di controllo.
5. Un ente dovrebbe disporre di un solido processo per garantire che i membri dell'organo gestorio siano, individualmente e collettivamente, in possesso di requisiti sufficienti.
6. I membri dell'organo gestorio dovrebbero acquisire, mantenere e accrescere le proprie conoscenze e competenze al fine di adempiere le proprie responsabilità. Gli enti dovrebbero garantire che i membri abbiano accesso a programmi di formazione personalizzati che tengano conto delle divergenze tra il profilo di conoscenze richiesto dall'ente e le effettive conoscenze dei membri. Tra gli ambiti che dovrebbero essere oggetto di formazione presso l'ente vi sono gli strumenti e i modelli di gestione dei rischi, i nuovi sviluppi, le modifiche nell'organizzazione, i prodotti complessi, i nuovi prodotti o mercati e le fusioni. La formazione dovrebbe riguardare anche i settori di attività per i quali i membri non sono direttamente responsabili. L'organo gestorio dovrebbe dedicare alla formazione tempo e risorse finanziarie e di altro tipo sufficienti.

14. Funzionamento organizzativo dell'organo gestorio

1. L'organo gestorio dovrebbe definire prassi e procedure organizzative adeguate per la propria organizzazione e il proprio funzionamento, e disporre dei mezzi necessari a garantire che le prassi siano applicate e periodicamente riviste a scopo di miglioramento.

Nota esplicativa
Solide prassi e procedure organizzative per l'organo gestorio inviano importanti segnali all'interno e all'esterno su politiche aziendali e obiettivi degli assetti di

governo dell'ente. Le prassi e le procedure includono la frequenza, i processi di lavoro e i verbali delle riunioni, il ruolo del presidente e l'uso dei comitati.

2. L'organo gestorio dovrebbe riunirsi periodicamente al fine di adempiere le proprie responsabilità in modo adeguato ed efficace. I membri dell'organo gestorio devono dedicare tempo sufficiente alla preparazione delle riunioni. La preparazione delle riunioni comprende la fissazione di un ordine del giorno. I verbali delle riunioni dovrebbero riportare i punti iscritti all'ordine del giorno e indicare chiaramente le decisioni adottate e le azioni concordate. Le prassi e le procedure, unitamente ai diritti, le responsabilità e le attività principali dell'organo gestorio, dovrebbero essere documentate e periodicamente riesaminate dall'organo gestorio.

Valutazione del funzionamento dell'organo gestorio

3. L'organo gestorio dovrebbe valutare regolarmente l'efficacia e l'efficienza singola e collettiva delle proprie attività, delle prassi e delle procedure organizzative e del funzionamento dei comitati. Per effettuare la valutazione è possibile il ricorso a mediatori esterni.

Ruolo del presidente dell'organo gestorio

4. Il presidente dovrebbe garantire che le decisioni dell'organo gestorio siano adottate sulla base di informazioni fondate e adeguate. Il presidente dovrebbe incoraggiare e promuovere discussioni aperte e critiche e garantire che pareri dissenzienti possano essere espressi e discussi nel processo decisionale.

Nota esplicativa

Il presidente dell'organo gestorio svolge un ruolo fondamentale nel corretto funzionamento dell'organo gestorio. Il presidente dirige l'organo gestorio ed è responsabile del suo efficace funzionamento complessivo.

5. In un sistema monistico, il presidente dell'organo gestorio e l'amministratore delegato dell'ente non dovrebbe essere la stessa persona. Qualora il presidente dell'organo gestorio sia anche amministratore delegato, l'ente dovrebbe adottare misure per ridurre al minimo le potenziali implicazioni negative sul sistema dei controlli (checks and balances).

Nota esplicativa

Il sistema dei controlli (checks and balances) potrebbe prevedere, ad esempio, la presenza di un membro indipendente di alto livello nell'organo gestorio con funzione di supervisione strategica o in una posizione simile.

Comitati specializzati dell'organo gestorio

6. L'organo gestorio con funzione di supervisione strategica dovrebbe valutare, tenendo conto delle dimensioni e della complessità dell'ente, l'opportunità di stabilire comitati specializzati costituiti da membri dell'organo gestorio (altri soggetti possono essere invitati a partecipare perché la propria specifica competenza o consulenza rileva nell'ambito di una particolare questione). I comitati specializzati possono includere un comitato per il controllo interno (audit committee), un comitato per i rischi (risk committee), un comitato per la remunerazione, un comitato per le nomine o per le risorse umane e/o un comitato per l'organizzazione interna, l'etica o il controllo di conformità.

> Nota esplicativa
>
> La delega assegnata a tali comitati non esime in alcun modo l'organo gestorio con funzione di supervisione strategica dall'adempimento dei propri doveri e delle proprie responsabilità a livello collettivo. Tuttavia i comitati possono assistere l'organo gestorio in specifici ambiti, favorendo la definizione e l'attuazione di prassi e di decisioni di buona organizzazione interna.

7. Un comitato specializzato dovrebbe disporre di una combinazione ottimale di conoscenze, competenze ed esperienze che, nell'insieme, consentano di comprendere a fondo e di valutare in modo obiettivo le questioni rilevanti e di proporre nuove idee in merito. Esso dovrebbe avere un numero sufficiente di membri indipendenti. Ogni comitato dovrebbe avere un mandato documentato (che comprenda anche lo scopo) dall'organo gestorio con funzione di supervisione strategica e procedure di lavoro consolidate. Occasionalmente la carica di presidente può essere svolta a rotazione dai membri.

> Nota esplicativa
>
> La rotazione della carica di presidente tra i membri contribuisce a evitare un'inappropriata concentrazione di potere e a promuovere nuove prospettive.

8. I presidenti dei rispettivi comitati dovrebbero riferire regolarmente all'organo gestorio. I comitati specializzati devono interagire tra loro, in modo opportuno, al fine di garantire la coerenza ed evitare carenze. A tal fine è possibile fare ricorso alla partecipazione reciproca (cross-participation): il presidente o un membro di un comitato specializzato può essere anche membro di un altro comitato specializzato.

Comitato per il controllo interno

9. Un comitato per il controllo interno (o suo equivalente) dovrebbe, inter alia, verificare l'efficacia del sistema di controlli interni, di revisione interna e di gestione dei rischi dell'impresa, vigilare sui revisori esterni dell'ente, raccomandare, per l'approvazione da parte dell'organo gestorio, la nomina, il

compenso e la revoca dei revisori esterni, rivedere e approvare l'ambito e la frequenza della revisione interna, rivedere le relazioni della revisione interna e controllare che l'organo gestorio con funzione di gestione adotti tempestivamente le necessarie misure correttive per fronteggiare carenze nei controlli, non conformità alle norme, ai regolamenti e alle politiche aziendali e altri problemi individuati dai revisori interni. Il comitato per il controllo interno dovrebbe inoltre vigilare sull'istituzione di politiche contabili da parte dell'ente.

Nota esplicativa
Cfr. anche l'articolo 41 della direttiva 2006/43/CE relativa alle revisioni legali dei conti annuali e dei conti consolidati.

10. Il presidente del comitato dovrebbe essere indipendente. Se il presidente è un ex membro dell'organo con funzione di gestione dell'ente, dovrebbe trascorrere un intervallo di tempo adeguato prima che egli possa assumere la posizione di presidente di un comitato.
11. Nel complesso i membri del comitato per il controllo interno dovrebbero essere in possesso di rilevanti esperienze pratiche e recenti nel settore dei mercati finanziari o dovrebbero avere maturato, nello svolgimento di precedenti attività lavorative, un'esperienza professionale sufficiente direttamente collegata alle attività dei mercati finanziari. In ogni caso, il presidente del comitato per il controllo interno dovrebbe avere acquisito conoscenze ed esperienze specialistiche in materia di applicazione dei principi contabili e dei processi dei controlli interni.

Comitato per i rischi

12. Un comitato per i rischi (o suo equivalente) dovrebbe offrire consulenza e assistenza all'organo gestorio in materia di tolleranza al rischio/appetito per il rischio attuali e prospettici, e sui connessi indirizzi strategici dell'ente. Esso è inoltre responsabile di controllare l'attuazione degli indirizzi strategici. Affinché la sua azione risulti più efficace, il comitato per i rischi dovrebbe comunicare regolarmente con la funzione di controllo dei rischi e il responsabile dei rischi (Chief Risk Officer) dell'ente e, se del caso, dovrebbe potersi avvalere della consulenza di esperti esterni, soprattutto in relazione a prospettate operazioni strategiche quali fusioni e acquisizioni.

B.3 Principi di buona condotta (business conduct)

15. Valori aziendali e codice etico

1. L'organo gestorio dovrebbe definire e promuovere standard etici e professionali di alto livello.

Nota esplicativa

Quando la reputazione di un ente viene messa in discussione, la perdita di fiducia può essere difficile da recuperare e può avere ripercussioni in tutto il mercato.

L'attuazione di standard appropriati (ad esempio un codice etico), che mirano a garantire un comportamento responsabile e professionale da parte di tutto l'ente, dovrebbe contribuire a ridurre i rischi ai quali l'ente è esposto. In particolare, il rischio operativo e quello reputazionale verranno ridotti se tali standard sono attuati in maniera rigorosa e se è loro assegnata una priorità elevata.

2. L'organo gestorio dovrebbe avere chiare politiche aziendali per delineare le modalità con le quali tali standard dovrebbero essere rispettati.
3. Dovrebbe essere effettuata costantemente la verifica dell'attuazione degli standard e del grado di conformità ad essi. I risultati di tali verifiche dovrebbero essere regolarmente comunicati all'organo gestorio.

16. Conflitti di interesse all'interno dell'ente

1. L'organo gestorio dovrebbe stabilire, attuare e mantenere politiche aziendali efficaci per l'identificazione dei conflitti di interesse esistenti e di quelli potenziali. I conflitti di interesse di cui l'organo gestorio è stato informato e che sono stati approvati da esso devono essere gestiti in maniera adeguata.
2. Una politica aziendale scritta dovrebbe identificare le relazioni, i servizi, le attività o le operazioni di un ente nell'ambito dei quali possono emergere conflitti di interesse e fissare le modalità di gestione di tali conflitti. Tale politica aziendale dovrebbe coprire le relazioni e le operazioni tra i vari clienti di un ente e tra l' ente e:
   a. la clientela (definita dal modello commerciale e/o in relazione ai vari servizi e attività forniti dall'ente);
   b. gli azionisti;
   c. i membri dell'organo gestorio;
   d. il personale (staff);
   e. i principali fornitori o partner commerciali; e
   f. altre parti correlate (ad esempio la capogruppo o le controllate).
3. La capogruppo dovrebbe considerare e bilanciare gli interessi di tutte le sue controllate, e tenere conto della misura in cui tali interessi contribuiscono nel lungo periodo agli obiettivi e agli interessi comuni del gruppo nel suo complesso.

4. La politica aziendale sui conflitti di interesse dovrebbe fissare le misure da adottare al fine di prevenire o gestire i conflitti di interesse. Le procedure e le misure in essa previste potrebbero includere:

   a. un'adeguata separazione dei compiti, ad esempio affidando a persone diverse le attività in conflitto nei processi riguardanti operazioni o servizi, o attribuendo a persone diverse i compiti di controllo e di informativa per le attività in conflitto;

   b. l'introduzione di barriere allo scambio di informazioni, quali ad esempio la separazione fisica di alcuni dipartimenti; e

   c. misure volte a evitare che soggetti che svolgono determinate attività anche al di fuori dell'ente esercitino un'influenza inopportuna all'interno dell'ente in relazione a tali attività.

17. Procedure di allerta interna

1. L'organo gestorio dovrebbe istituire adeguate procedure di allerta interna per la segnalazione da parte del personale di eventuali disfunzioni dell'assetto organizzativo.
2. Un ente dovrebbe adottare adeguate procedure di allerta interna utilizzabili dal personale per richiamare l'attenzione su problemi legittimi e rilevanti che riguardano aspetti legati all'organizzazione interna. Tali procedure dovrebbero garantire la riservatezza del personale che segnala tali disfunzioni. Al fine di evitare conflitti di interesse, si dovrebbero poter segnalare queste fattispecie di problemi al di fuori delle tradizionali linee di reporting [ad esempio attraverso la funzione di conformità alle norme o la funzione di revisione interna o mediante una procedura interna di segnalazione delle irregolarità (c.d. procedura *whistleblower*)]. Le procedure di allerta dovrebbero essere accessibili a tutto il personale dell'ente. Le informazioni fornite dal personale attraverso la procedura di allerta, se rilevanti, dovrebbero essere rese disponibili all'organo gestorio.

Nota esplicativa
In alcuni Stati membri, in aggiunta alle procedure di allerta interne di un ente, può esistere la possibilità per il personale di informare l'autorità di vigilanza su problemi di questo genere.

B.4 Politiche di esternalizzazione delle funzioni aziendali (outsourcing) e per la remunerazione

18. Esternalizzazione di funzioni aziendali (outsourcing)

1. L'organo gestorio approva e rivede regolarmente la politica di esternalizzazione delle funzioni aziendali di un ente.

> Nota esplicativa
>
> Il presente orientamento si limita a trattare la politica aziendale di esternalizzazione; gli aspetti di dettaglio in materia di esternalizzazione sono trattati negli Orientamenti del CEBS in materia di esternalizzazione delle funzioni aziendali (CEBS Guidelines on outsourcing), disponibili sul sito web dell'ABE.
>
> Gli enti devono conformarsi a entrambi gli orientamenti. In caso di discordanza tra i due documenti, dovrebbero prevalere gli orientamenti del CEBS in materia di esternalizzazione, in quanto più specifici. Qualora invece un argomento non sia trattato negli orientamenti del CEBS in materia di esternalizzazione, si dovrebbe applicare il principio generale indicato nei presenti orientamenti.

2. La politica aziendale di esternalizzazione dovrebbe valutare l'impatto dell'esternalizzazione sulle attività di un ente e sui rischi ai quali l'ente è esposto (come ad esempio il rischio operativo, reputazionale e di concentrazione). La politica aziendale dovrebbe stabilire i flussi informativi e le modalità di controllo che devono essere garantiti per tutta la durata del contratto di esternalizzazione (ivi compresi la redazione di uno studio di fattibilità per l'esternalizzazione, la sottoscrizione di un contratto di esternalizzazione, l'attuazione del contratto fino alla sua scadenza, i piani di emergenza e le strategie di uscita). La politica aziendale deve essere rivista e aggiornata regolarmente, e le eventuali modifiche necessarie devono essere attuate tempestivamente.
3. Un ente resta pienamente responsabile di tutti i servizi e le attività esternalizzati, nonché delle decisioni gestionali da essi derivanti. Ne consegue che la politica aziendale di esternalizzazione dovrebbe definire chiaramente che l'esternalizzazione non solleva l'ente dai propri obblighi regolamentari e dalle proprie responsabilità verso i clienti.
4. La politica aziendale dovrebbe indicare che il ricorso all'esternalizzazione non deve ostacolare un'efficace vigilanza on-site o off-site dell'ente e non deve essere in contrasto con le regole di vigilanza su servizi e attività. La politica aziendale dovrebbe anche coprire il ricorso all'esternalizzazione interna (ad esempio quella fornita da un'entità giuridica distinta ma all'interno del gruppo dell'ente) e ogni circostanza specifica del gruppo da tenere in considerazione.

19. Assetto organizzativo della politica aziendale di remunerazione

1. Il controllo finale sulla politica aziendale di remunerazione dovrebbe spettare all'organo gestorio dell'ente.

Nota esplicativa

I presenti orientamenti forniscono il quadro *generale* applicabile all'assetto organizzativo della politica aziendale di remunerazione. Aspetti *specifici* in materia di remunerazione sono stati trattati negli orientamenti del CEBS di dicembre 2010 sulla remunerazione (CEBS Guidelines on Remuneration). Gli enti devono conformarsi a entrambi gli orientamenti.

2. L'organo gestorio con funzione di supervisione strategica deve salvaguardare, approvare e supervisionare i principi della politica aziendale generale per la remunerazione. Le procedure utilizzate dall'ente per fissare i criteri di remunerazione devono essere chiare, adeguatamente documentate e trasparenti nell'ambito dell'ente.
3. In aggiunta alla responsabilità generale dell'organo gestorio per la politica aziendale di remunerazione nel suo complesso e per la sua revisione, è richiesto un coinvolgimento adeguato delle funzioni aziendali di controllo. I membri dell'organo gestorio, i membri del comitato per la remunerazione e altro personale coinvolto nella definizione e nell'attuazione della politica aziendale di remunerazione devono essere in possesso di competenze attinenti e avere la capacità di effettuare una valutazione indipendente dell'adeguatezza della politica aziendale di remunerazione, che includa anche le implicazioni da essa derivanti per la gestione del rischio.
4. La politica aziendale di remunerazione dovrebbe anche mirare a prevenire i conflitti di interesse. L'organo gestorio con funzione di gestione non dovrebbe fissare i criteri per la propria remunerazione; al fine di evitare ciò, esso potrebbe considerare, ad esempio, la possibilità di avvalersi di un comitato indipendente per la remunerazione. Un'unità operativa non dovrebbe poter determinare i criteri di remunerazione delle proprie funzioni di controllo.
5. L'organo gestorio dovrebbe controllare l'applicazione della politica aziendale di remunerazione al fine di assicurare che essa funzioni come previsto. L'attuazione della politica aziendale di remunerazione dovrebbe anche essere sottoposta a una verifica centrale e indipendente.

C. Gestione del rischio

20. Cultura dei rischi

1. Un ente dovrebbe sviluppare una cultura dei rischi integrata a tutti i livelli e estesa a tutto l'ente, basata sulla piena comprensione dei rischi che esso deve fronteggiare e delle modalità di gestione di tali rischi, in considerazione della propria tolleranza al rischio/appetito per il rischio.

Nota esplicativa

Poiché le attività di un ente comportano l'assunzione di rischi, è fondamentale che vi sia una gestione adeguata di essi. La diffusione di una cultura dei rischi solida e coerente a tutti i livelli dell'ente è un elemento fondamentale per un'efficace gestione dei rischi.

2. Un ente dovrebbe sviluppare la propria cultura dei rischi attraverso politiche aziendali, esempi, informazione e formazione al personale per sensibilizzare i dipendenti in merito alle responsabilità in materia di rischi.
3. Ogni membro della struttura organizzativa dovrebbe essere pienamente consapevole delle proprie responsabilità in relazione alla gestione del rischio. La gestione del rischio non dovrebbe essere confinata agli specialisti in materia di rischi o alle funzioni di controllo. Le unità operative, sotto la supervisione dell'organo gestorio, dovrebbero essere principalmente responsabili della gestione dei rischi su base giornaliera, in considerazione della tolleranza al rischio/appetito per il rischio dell'ente e in linea con le sue politiche aziendali, le procedure e i controlli.
4. Un ente dovrebbe avere un sistema globale di gestione del rischio che si estenda a tutte le unità operative, di supporto e di controllo, che riconosca pienamente la sostanza economica delle esposizioni al rischio e che ricomprenda tutti i rischi rilevanti (ad esempio quelli finanziari e non finanziari, nel bilancio e fuori bilancio, se contingenti o contrattuali, oppure no). Il suo ambito non dovrebbe limitarsi ai rischi di credito, di mercato, di liquidità e operativi, ma dovrebbe anche includere i rischi di concentrazione, reputazionali, di conformità alle norme e strategici.
5. La gestione dei rischi dovrebbe consentire all'ente di prendere decisioni informate. Tali decisioni dovrebbero basarsi sulle informazioni derivanti dall'identificazione, dalla misurazione o dalla valutazione e dal monitoraggio dei rischi. I rischi dovrebbero essere valutati mediante approccio bottom-up e top-down, in tutti i processi gestionali e le linee di business, utilizzando una terminologia coerente e metodologie compatibili all'interno dell'ente e del gruppo.
6. Il sistema di gestione del rischio deve essere sottoposto a revisione indipendente interna o esterna, e riesaminato regolarmente in rapporto alla tolleranza al rischio/appetito per il rischio dell'ente, tenendo in considerazione le informazioni provenienti dalla funzione di controllo dei rischi e, se del caso, dal comitato per i rischi. Tra i fattori da considerare vi sono inoltre sviluppi esterni e interni, tra cui la crescita delle attività di bilancio e del volume dei ricavi, l'aumentata complessità delle attività dell'ente, del profilo di rischio e della struttura operativa, l'espansione geografica, le fusioni e le acquisizioni e l'introduzione di nuovi prodotti o di nuove linee di business.

21. Allineamento della remunerazione al profilo di rischio

1. La politica aziendale e le prassi di remunerazione di un ente dovrebbero essere coerenti con il suo profilo di rischio e promuovere una sana ed efficace gestione dei rischi.

Nota esplicativa
I presenti orientamenti forniscono i principi generali applicabili all'allineamento della politica aziendale di remunerazione al profilo di rischio dell'ente. Gli aspetti *specifici* della politica aziendale di remunerazione sono trattati negli orientamenti del CEBS di dicembre 2010 in materia di remunerazione (CEBS Guidelines on Remuneration). Gli enti devono conformarsi ad entrambi gli orientamenti.

2. La politica aziendale di remunerazione complessiva di un ente dovrebbe essere in linea con i valori, la strategia commerciale, la tolleranza al rischio/appetito per il rischio e gli interessi di lungo periodo dell'ente. Essa non dovrebbe incoraggiare l'eccessiva assunzione di rischi. La remunerazione variabile garantita o i pagamenti per la cessazione anticipata del rapporto di lavoro che vanno a ricompensare gli insuccessi non sono coerenti con una sana gestione del rischio o con il principio della ricompensa per i risultati ottenuti (pay-for-performance) e, di norma, dovrebbero essere vietati.
3. Per il personale la cui attività professionale ha un impatto significativo sul profilo di rischio dell'ente (ad esempio i membri dell'organo gestorio, l'alta dirigenza, i soggetti che assumono i rischi (risk taker) nelle unità operative, il personale responsabile dei controlli interni e i dipendenti che ricevono una remunerazione totale che li colloca nella stessa fascia retributiva degli alti dirigenti e dei risk taker), la politica aziendale di remunerazione dovrebbe stabilire disposizioni specifiche per garantire che la remunerazione di tale personale sia in linea con una sana ed efficace gestione del rischio.
4. Il personale con funzioni di controllo dovrebbe essere adeguatamente remunerato in base agli obiettivi e alle prestazioni e non in relazione alle prestazioni delle unità operative da esso controllate.
5. Qualora la remunerazione sia legata alle prestazioni, essa dovrebbe basarsi su una combinazione di prestazioni individuali e collettive. Quando si definiscono le prestazioni individuali, andrebbero presi in considerazione fattori diversi dalle prestazioni finanziarie. La misurazione delle prestazioni per la corresponsione di premi dovrebbe includere gli adeguamenti per tutti i tipi di rischi e per il costo del capitale e della liquidità.
6. Il rapporto tra retribuzione di base e premi dovrebbe essere proporzionato. Un premio significativo non dovrebbe essere corrisposto soltanto in forma di bonus up-front (cioè liquidato nell'anno stesso di assegnazione), ma dovrebbe includere una componente differita aggiustata per il rischio e flessibile. La tempistica per la corresponsione dei premi dovrebbe tenere conto delle prestazioni corrette per i rischi (risk performance).

22. Il sistema di gestione dei rischi

1. Il sistema di gestione dei rischi di un ente dovrebbe includere politiche aziendali, procedure, limiti operativi e controlli che consentano di individuare, misurare o valutare, monitorare, attenuare e segnalare in maniera adeguata, tempestiva e continua, i rischi derivanti dalle attività dell'ente sia a livello di linea di business sia di ente nel suo complesso.
2. Il sistema di gestione dei rischi di un ente dovrebbe fornire orientamenti specifici sull'attuazione degli indirizzi strategici dell'ente. Tali orientamenti dovrebbero, se del caso, stabilire e mantenere limiti operativi interni coerenti con il livello di rischio accettato (tolleranza al rischio/appetito per il rischio dell'ente) e commisurati al sano funzionamento, alla solidità finanziaria e agli obiettivi strategici dell'ente. Il profilo di rischio di un ente (ossia l'aggregato delle proprie esposizioni ai rischi effettivi e potenziali) dovrebbe essere mantenuto all'interno di tali limiti operativi. Il sistema di gestione del rischio dovrebbe garantire che le violazioni dei limiti operativi siano trattate con la massima priorità e fronteggiate con procedure adeguate.
3. Nell'identificazione e misurazione dei rischi l'ente dovrebbe sviluppare strumenti retrospettivi e prospettici per integrare il lavoro sulle esposizioni correnti. Gli strumenti dovrebbero consentire l'aggregazione delle esposizioni ai rischi attraverso tutte le linee di business e facilitare l'identificazione di concentrazioni dei rischi.
4. Gli strumenti prospettici (quali ad esempio analisi di scenario e stress test) dovrebbero individuare le potenziali esposizioni ai rischi in diverse circostanze avverse; gli strumenti retrospettivi dovrebbero consentire di rivedere il profilo di rischio corrente rispetto alla tolleranza al rischio/appetito per il rischio dell'ente e al relativo sistema di gestione dei rischi, e fornire contributi per eventuali adeguamenti.

Nota esplicativa
Gli orientamenti in materia di stress test sono disponibili sul sito web dell'ABE.

5. La responsabilità finale della valutazione dei rischi spetta unicamente all'ente, che dovrebbe pertanto valutare criticamente i propri rischi e non dovrebbe fare affidamento esclusivamente a valutazioni esterne.

Nota esplicativa
A titolo esemplificativo, un ente dovrebbe validare un modello di rischio acquistato e adeguarlo alle proprie caratteristiche individuali per garantire che i rischi siano identificati e analizzati in modo accurato e completo.

Le valutazioni esterne dei rischi (inclusi i rating esterni o i modelli acquistati da fornitori esterni) possono aiutare a fornire una stima più completa dei rischi. Gli enti dovrebbero essere consapevoli dell'ambito di tali valutazioni.

6. Le decisioni che determinano il livello di rischio assunto non dovrebbero basarsi soltanto su informazioni quantitative o sulle risultanze dei modelli, ma dovrebbero anche tener conto delle limitazioni pratiche e teoriche delle misure e dei modelli, applicando un metodo qualitativo (che preveda il parere di esperti e un'analisi critica). Dovrebbero essere esplicitamente esaminati le tendenze e i dati rilevanti del contesto macroeconomico al fine di individuare il loro possibile impatto sulle esposizioni e i portafogli. Tali valutazioni dovrebbero essere formalmente integrati nelle decisioni in materia di rischi rilevanti.

Nota esplicativa

Gli enti dovrebbero tenere conto che le risultanze delle valutazioni quantitative prospettiche e degli stress test dipendono in larga misura dalle limitazioni e dalle ipotesi dei modelli (fra cui l'impatto e la durata dello shock e i rischi alla base). A titolo esemplificativo, il fatto che i modelli mostrino rendimenti sul capitale economico molto elevati potrebbe derivare da una debolezza nei modelli (ad esempio l'esclusione di alcuni rischi rilevanti) piuttosto che da una migliore strategia o esecuzione dell'ente.

7. Un sistema di reportistica regolare e trasparente dovrebbe essere stabilito in modo che l'organo gestorio e tutte le unità rilevanti di un ente ricevano le informazioni in maniera tempestiva, precisa, sintetica, comprensibile e sostanziale, e possano condividere le informazioni rilevanti in materia di identificazione, misurazione o valutazione, e monitoraggio dei rischi. Il sistema di reportistica dovrebbe essere adeguatamente definito, documentato e approvato dall'organo gestorio.
8. Se istituito, il comitato per i rischi dovrebbe ricevere regolarmente relazioni formali e comunicazioni informali, a seconda dei casi, dalla funzione di controllo dei rischi e dal responsabile dei rischi (Chief Risk Officer).

Nota esplicativa

Un'efficace sistema di comunicazione delle informazioni sui rischi è fondamentale per l'intero processo di gestione dei rischi, facilita il processo di revisione e quello decisionale e contribuisce a evitare l'adozione di decisioni che potrebbero involontariamente aumentare il rischio. Un'efficace reportistica dei rischi implica la considerazione e la comunicazione degli obiettivi strategici in materia di rischi e dei dati rilevanti sui rischi (ad esempio le esposizioni e i principali indicatori di rischio, Key risk indicators) sia trasversalmente all'interno dell'ente sia verticalmente nei processi gestionali.

23. Nuovi prodotti

1. Gli enti dovrebbero disporre di una documentata politica aziendale per l'approvazione di nuovi prodotti (New Product Approval Policy, NPAP), approvata dall'organo gestorio, che affronta lo sviluppo di nuovi mercati, prodotti e servizi e le modifiche rilevanti a prodotti e servizi esistenti.
2. La politica aziendale di approvazione di nuovi prodotti di un ente dovrebbe tenere conto di ogni elemento che deve essere considerato prima di decidere di entrare in nuovi mercati, trattare nuovi prodotti, avviare un nuovo servizio o apportare modifiche rilevanti a prodotti o servizi esistenti. La politica aziendale di approvazione di nuovi prodotti dovrebbe inoltre includere la definizione di "nuovo prodotto/mercato/attività" che deve essere utilizzata nell'organizzazione e dalle funzioni interne coinvolte nel processo decisionale.
3. La politica aziendale di approvazione di nuovi prodotti dovrebbe indicare i principali profili che devono essere trattati prima di adottare una decisione. Tali profili dovrebbero includere la conformità alle norme, i modelli di pricing, gli impatti su rischiosità, adeguatezza patrimoniale e redditività, la disponibilità di risorse adeguate per le attività di "front-office", "back-office" e "middle-office" e adeguati strumenti interni e competenze per la comprensione e il monitoraggio dei rischi associati. La decisione di avviare una nuova attività dovrebbe indicare chiaramente l'unità operativa e le persone che ne sono responsabili. Nessuna nuova attività dovrebbe essere avviata fino a quando non siano disponibili risorse adeguate per comprendere e gestire i rischi a essa associati.
4. La funzione di controllo dei rischi dovrebbe essere coinvolta nell'approvazione di nuovi prodotti o delle modifiche rilevanti ai prodotti esistenti. Il suo apporto dovrebbe includere una valutazione completa e oggettiva dei rischi derivanti da nuove attività in diverse ipotesi di scenario, delle potenziali carenze nel sistema di gestione dei rischi e i controlli interni dell'ente, e della capacità dell'ente di gestire efficacemente tutti i nuovi rischi. La funzione di controllo dei rischi dovrebbe anche avere una chiara visione d'insieme del processo di introduzione (roll-out) di nuovi prodotti (o delle modifiche rilevanti apportate ai prodotti esistenti) nei diversi portafogli e linee di business, e il potere di richiedere che le modifiche ai prodotti esistenti siano sottoposte al processo formale previsto nella politica aziendale per l'approvazione di nuovi prodotti (formal NPAP process).

D. Controlli interni

24. Il sistema dei controlli interni

1. Un ente dovrebbe sviluppare e mantenere un robusto e completo sistema di controlli interni, che includa specifiche funzioni di controllo indipendenti adeguatamente legittimate a svolgere il loro compito.

2. Il sistema dei controlli interni di un ente dovrebbe garantire operazioni efficaci ed efficienti, un controllo adeguato dei rischi, una condotta prudente, l'attendibilità della reportistica delle informazioni finanziarie e non finanziarie, sia all'interno sia verso l'esterno, e la conformità alle leggi, ai regolamenti, ai requisiti di vigilanza prudenziali, e alle regolamentazioni e alle decisioni interne dell'ente. Il sistema dei controlli interni dovrebbe riguardare l'intera organizzazione, comprese le attività di tutte le linee di business, le unità di supporto e di controllo. Il sistema dei controlli interni dovrebbe essere adeguato per le attività dell'ente, con robuste procedure amministrative e contabili.
3. Nello sviluppo del proprio sistema dei controlli interni, l'ente dovrebbe garantire che vi siano un processo decisionale chiaro, trasparente e documentato e una chiara attribuzione delle responsabilità e dei poteri per assicurare la conformità alle norme e alle decisioni interne. Al fine di attuare un efficace sistema dei controlli interni in tutti i settori di operatività dell'ente, le unità operative e di supporto dovrebbero in primo luogo istituire e mantenere adeguate politiche aziendali e procedure per i controlli interni.
4. Un adeguato sistema dei controlli interni richiede inoltre che funzioni di controllo indipendenti effettuino una verifica della conformità a tali politiche e procedure. Le funzioni di controllo dovrebbero includere una funzione di Controllo dei Rischi (Risk Management), una funzione di Conformità alle norme (Compliance) e una funzione di Revisione Interna (Internal Audit).
5. Le funzioni di controllo dovrebbero essere stabilite a un adeguato livello gerarchico e dovrebbero riferire direttamente all'organo gestorio. Esse dovrebbero essere indipendenti dalle unità operative e di supporto che sono oggetto di revisione e controllo, e indipendenti l'una dall'altra dal punto di vista organizzativo (in quanto svolgono funzioni diverse). Tuttavia, negli enti di minore complessità o dimensione, i compiti della funzione di Controllo dei Rischi e della funzione di Conformità alle norme potrebbero essere integrate. Le funzioni di controllo del gruppo dovrebbero supervisionare le funzioni di controllo delle filiazioni.
6. Al fine di garantire l'indipendenza della funzione di controllo devono essere soddisfatte le seguenti condizioni:

    a. il personale adibito alla funzione di controllo non svolge compiti che ricadono nell'ambito delle attività che la funzione di controllo deve verificare e controllare;

    b. la funzione di controllo è separata dal punto di vista organizzativo dalle attività che deve verificare e controllare;

    c. il responsabile della funzione di controllo è subordinato ad una persona che non è responsabile della gestione delle attività che la funzione di controllo verifica e controlla. Di norma, il responsabile della funzione di controllo dovrebbe riferire direttamente all'organo gestorio e ai comitati rilevanti, e dovrebbe partecipare regolarmente alle loro riunioni; e

d. la remunerazione del personale adibito alla funzione di controllo non dovrebbe essere legata alle prestazioni delle attività che la funzione di controllo verifica e controlla, né diversamente in modo tale da comprometterne l'obiettività.

7. Le funzioni di controllo dovrebbero disporre di un numero adeguato di risorse qualificate (sia a livello di capogruppo sia di controllate nei gruppi). Il personale dovrebbe mantenere le proprie qualifiche su base continuativa e dovrebbe ricevere una formazione adeguata. Il personale dovrebbe anche avere a disposizione sistemi di dati e di supporto adeguati, con accesso alle informazioni interne e esterne necessarie per adempiere le proprie responsabilità.
8. Le funzioni di controllo dovrebbero sottoporre regolarmente all'organo gestorio relazioni formali sulle principali carenze individuate. Tali relazioni dovrebbero includere approfondimenti successivi (follow-up) sulla rimozione di quanto precedentemente rilevato e, per ogni nuova carenza rilevante individuata, i rischi rilevanti che ne derivano, la valutazione d'impatto e raccomandazioni. L'organo gestorio dovrebbe intervenire sulle risultanze delle funzioni di controllo in modo tempestivo ed efficace e richiedere misure correttive adeguate.

25. Funzione di Controllo dei Rischi (Risk Control Function, RCF)

1. Un ente dovrebbe istituire una funzione di controllo dei rischi onnicomprensiva e indipendente.
2. La funzione di controllo dei rischi dovrebbe garantire che tutti i principali rischi cui l'ente è esposto siano individuati e adeguatamente gestiti dalle pertinenti unità dell'ente, e che un quadro complessivo di tutti i rischi rilevanti sia sottoposto all'organo gestorio. La funzione di controllo dei rischi dovrebbe fornire rilevanti e indipendenti informazioni, analisi e pareri di specialisti sull'esposizione ai rischi, e consulenza su proposte e decisioni in materia di rischi adottate dall'organo gestorio e dalle unità operative o di supporto con riferimento alla coerenza di tali proposte e decisioni con la tolleranza al rischio/appetito per il rischio dell'ente. La funzione di controllo dei rischi potrebbe raccomandare l'apporto di miglioramenti al sistema di gestione dei rischi e opzioni per porre rimedio a violazioni delle politiche aziendali, delle procedure e dei limiti operativi in materia di rischi.
3. La funzione di controllo dei rischi dovrebbe essere un elemento centrale nell'organizzazione dell'ente, strutturata in modo tale da consentire l'attuazione delle politiche aziendali in materia di rischi e controllare il sistema di gestione dei rischi. Gli enti di maggiori dimensioni e complessità e articolazione possono prevedere la costituzione di funzioni di controllo dei rischi dedicate per ciascuna linea di business. Tuttavia, nell'ente dovrebbe essere presente una funzione di controllo dei rischi centrale (che includa, nel caso della capogruppo di un gruppo e ove opportuno, una funzione di controllo dei rischi di gruppo) al fine di fornire una visione d'insieme su tutti i rischi.

4. La funzione di controllo dei rischi dovrebbe essere indipendente dalle unità operative e di supporto che assumono i rischi sui quali essa vigila, ma non dovrebbe essere isolata da tali unità. La funzione di controllo dei rischi dovrebbe disporre di conoscenze sufficienti in materia di tecniche e procedure di gestione dei rischi, di mercati e di prodotti. L'interazione tra il contesto operativo e la funzione di controllo dei rischi dovrebbe promuovere la piena consapevolezza della gestione dei rischi in tutto il personale dell'ente.

26. Il ruolo della funzione di controllo dei rischi

1. La funzione di controllo dei rischi dovrebbe essere attivamente coinvolta sin dalla fase iniziale nell'elaborazione degli indirizzi strategici sui rischi e in tutte le decisioni che riguardano la gestione dei rischi rilevanti di un ente. La funzione di controllo dei rischi dovrebbe svolgere un ruolo fondamentale nel garantire che l'ente disponga di efficaci processi di gestione dei rischi.

Il ruolo della funzione di controllo dei rischi in materia di indirizzi strategici e decisioni

2. La funzione di controllo dei rischi dovrebbe fornire all'organo gestorio tutte le informazioni rilevanti relative ai rischi (ad esempio attraverso analisi tecniche sull'esposizione ai rischi) al fine di consentire a tale organo di fissare il livello di tolleranza al rischio/appetito per il rischio dell'ente.
3. La funzione di controllo dei rischi dovrebbe anche valutare gli indirizzi strategici in materia di rischi, compresi gli obiettivi proposti dalle unità operative, e fornire consulenza all'organo gestorio prima dell'adozione di una decisione. Gli obiettivi delle unità operative, che includono il livello di rischiosità dei crediti e l'indice di redditività del capitale proprio (Return on Equity, ROE), dovrebbero essere ragionevoli e coerenti.
4. La funzione di controllo dei rischi dovrebbe condividere con tutte le unità operative la responsabilità per l'attuazione degli indirizzi strategici e della politica aziendale dell'ente in materia di rischi. Da un lato, le unità operative dovrebbero applicare i rilevanti limiti operativi, dall'altro, la funzione di controllo dei rischi dovrebbe garantire che i limiti operativi siano in linea con il livello generale di propensione al rischio/appetito per il rischio dell'ente, e monitorare su base continuativa che l'ente non assuma rischi eccessivi.
5. Il coinvolgimento della funzione di controllo dei rischi nei processi decisionali dovrebbe garantire che i rischi siano tenuti in adeguata considerazione. Tuttavia, la responsabilità delle decisioni adottate dovrebbe restare in capo alle unità operative e di supporto e, in ultima analisi, all'organo gestorio.

Il ruolo della funzione di controllo dei rischi nelle operazioni con parti correlate

6. La funzione di controllo dei rischi dovrebbe garantire che le operazioni con parti correlate siano oggetto di verifica e che i rischi, effettivi o potenziali, che esse comportano per l'ente siano individuati e adeguatamente valutati.

Il ruolo della funzione di controllo dei rischi nella complessità della struttura giuridica

7. La funzione di controllo dei rischi dovrebbe adoperarsi per individuare i rischi rilevanti derivanti dalla complessità della struttura giuridica di un ente.

Nota esplicativa

Tra i rischi potrebbero essere ricompresi la mancanza di trasparenza nella gestione, i rischi operativi derivanti da complesse e interconnesse strutture di funding, esposizioni infragruppo, impossibilità di escutere garanzie reali e rischio di controparte.

Il ruolo della funzione di controllo dei rischi nelle modifiche rilevanti

8. La funzione di controllo dei rischi dovrebbe valutare le modalità in cui i rischi rilevanti individuati possono influire sulla capacità dell'ente o del gruppo di gestire il proprio profilo di rischio e di reperire funding e capitale in condizioni normali e in circostanze avverse.
9. Prima dell'adozione di decisioni riguardanti modifiche rilevanti o operazioni eccezionali, la funzione di controllo dei rischi dovrebbe essere coinvolta nella valutazione dell'impatto di tali modifiche e operazioni eccezionali sulla rischiosità complessiva dell'ente e del gruppo.

Nota esplicativa

Tra le modifiche rilevanti o le operazioni eccezionali potrebbero essere inclusi le fusioni e le acquisizioni, lo stabilimento o la dismissione di filiazioni o società veicolo (SPV), i nuovi prodotti, le modifiche ai sistemi, alla gestione dei rischi o alle relative procedure, e le modifiche all'assetto organizzativo dell'ente.

Cfr. gli Orientamenti congiunti emanati nel 2008 dai tre ex Comitati di III livello delle autorità europee di vigilanza finanziaria (CEBS, CESR e CEIOPS) in materia di valutazione prudenziale delle acquisizioni e degli aumenti delle partecipazioni in società del settore finanziario (Joint Guidelines on the Prudential Assessment of Acquisitions and Increases in Holdings in the Financial Sector), pubblicati sul sito web dell'ABE. La funzione di controllo dei rischi dovrebbe essere attivamente coinvolta sin dalla fase iniziale nell'individuazione dei rischi rilevanti in relazione a cambiamenti nella struttura del gruppo, fusioni e acquisizioni comprese [ciò include le possibili conseguenze di un mancato adempimento degli obblighi di adeguata verifica (Due Diligence) che non

consenta di individuare i rischi a seguito di fusioni], e dovrebbe riferire le proprie risultanze direttamente all'organo gestorio.

Il ruolo della funzione di controllo dei rischi nei sistemi di misurazione e valutazione dei rischi

10. La funzione di controllo dei rischi dovrebbe garantire che per i sistemi interni di misurazione e valutazione dei rischi dell'ente sia analizzato un appropriato numero di scenari e siano utilizzate ipotesi sufficientemente conservative sulle dipendenze e sulle correlazioni. Dovrebbero essere incluse le valutazioni qualitative a livello aziendale (anche con il contributo di un esperto) sul rapporto tra rischiosità e redditività dell'ente e il contesto operativo esterno.

Il ruolo della funzione di controllo dei rischi nel monitoraggio dei rischi

11. La funzione di controllo dei rischi dovrebbe garantire che tutti i rischi individuati possano essere effettivamente monitorati dalle unità operative. La funzione di controllo dei rischi dovrebbe monitorare regolarmente il profilo di rischio attuale dell'ente e valutarlo rispetto agli obiettivi strategici e alla tolleranza al rischio/propensione per il rischio dell'ente al fine di consentire all'organo gestorio di adottare decisioni nell'esercizio della funzione di gestione e di verificarle nell'esercizio della funzione di supervisione strategica.
12. La funzione di controllo dei rischi dovrebbe analizzare gli andamenti e riconoscere i nuovi rischi o quelli emergenti che derivano dal mutare delle circostanze e delle condizioni. Esso dovrebbe anche esaminare con regolarità i risultati effettivi in materia di rischi raffrontandoli con le stime precedenti (test retrospettivi ovvero back testing) al fine di valutare e migliorare l'accuratezza e l'efficacia del processo di gestione dei rischi.
13. La funzione di controllo dei rischi di gruppo dovrebbe monitorare i rischi assunti dalle controllate. Le incoerenze rispetto agli indirizzi strategici di gruppo approvati dovrebbero essere segnalate al pertinente organo gestorio.

Il ruolo della funzione di controllo dei rischi con riferimento alle esposizioni non autorizzate

14. La funzione di controllo dei rischi dovrebbe essere adeguatamente coinvolta in tutte le modifiche agli indirizzi strategici dell'ente, alla tolleranza al rischio/propensione per il rischio e ai limiti operativi approvati.
15. La funzione di controllo dei rischi dovrebbe valutare in maniera indipendente ogni abuso o violazione (incluse le relative motivazioni e un'analisi giuridica ed economica del costo effettivo di eliminazione, riduzione o copertura dell'esposizione rispetto al potenziale costo del suo mantenimento). La funzione di controllo dei rischi dovrebbe informare le unità operative interessate e raccomandare l'adozione di possibili misure.

Nota esplicativa

Gli abusi o le violazioni agli indirizzi strategici, alla tolleranza al rischio/appetito per il rischio o ai limiti operativi possono derivare da nuove operazioni, da modifiche nelle condizioni del mercato o da un'evoluzione degli indirizzi strategici, delle politiche aziendali o delle procedure dell'ente, nel caso in cui i limiti operativi o la tolleranza al rischio/appetito per il rischio non siano stati conseguentemente modificati.

16. La funzione di controllo dei rischi svolge un ruolo fondamentale nel garantire che una decisione sia adottata al livello appropriato su propria raccomandazione, che le rilevanti unità operative si conformino ad essa e che di tale decisione siano opportunamente informati l'organo gestorio, il comitato dei rischi e l'unità operativa o di supporto.
17. L'ente dovrebbe intraprendere misure adeguate contro comportamenti fraudolenti interni ed esterni e le violazioni della disciplina (ad esempio violazione delle procedure interne o dei limiti operativi).

Nota esplicativa

Ai fini dei presenti orientamenti, il termine "frode" (fraude) comprende le frodi interne e quelle esterne di cui all'allegato X, parte 5, della direttiva 2006/48/CE. Sono ricomprese in questo ambito le perdite dovute a frode, appropriazione indebita o inosservanza di leggi, regolamenti o politiche aziendali (ad esclusione dei casi di diversità/discriminazione) in cui sia coinvolto almeno un soggetto interno all'ente (frode interna), e le perdite derivanti da frode, appropriazione indebita o inosservanza delle leggi da parte di terzi (frode esterna).

27. Responsabile dei rischi

1. Un ente dovrebbe nominare un responsabile dei rischi (Chief Risk Officer, CRO), al quale è affidata la responsabilità esclusiva della funzione di controllo dei rischi e del monitoraggio del sistema di gestione dei rischi dell'ente all'interno di tutta la struttura organizzativa.
2. Il responsabile dei rischi (o una posizione equivalente) ha il compito di fornire informazioni esaurienti e accessibili sui rischi, consentendo all'organo gestorio di comprendere in pieno il profilo di rischio complessivo dell'ente. Ciò si applica anche al responsabile dei rischi della capogruppo con riferimento all'intero gruppo.
3. Il responsabile dei rischi dovrebbe disporre di competenze, esperienza operativa, indipendenza e anzianità di servizio sufficienti per intervenire sulle decisioni che influiscono sull'esposizione al rischio di un ente. Un ente dovrebbe valutare la possibilità di concedere il diritto di veto al responsabile dei rischi. Il responsabile dei rischi e l'organo gestorio o i relativi comitati dovrebbero essere

in grado di comunicare direttamente tra loro in relazione alle principali questioni in materia di rischi, compresi gli sviluppi nell'operatività che potrebbero essere non coerenti con la tolleranza al rischio/propensione per il rischio e gli indirizzi strategici dell'ente.

4. Se un ente intende concedere al responsabile dei rischi il diritto di veto sulle decisioni, le proprie politiche aziendali in materia di rischi dovrebbero specificare le circostanze nelle quali il responsabile dei rischi può esercitare tale diritto e la natura delle proposte di decisione (ad esempio una decisione in materia di credito o di investimento, o la fissazione di un limite operativo). Le politiche aziendali dovrebbero descrivere le procedure di appello o per riportare le questioni ai livelli più elevati (escalation), e le modalità di informazione dell'organo gestorio.
5. Quando le caratteristiche dell'ente, in particolare le dimensioni, l'organizzazione e la natura delle attività, non sono tali da giustificare l'attribuzione del ruolo di responsabile dei rischi a un soggetto appositamente nominato, la funzione potrebbe essere svolta da un altro dipendente dell'ente di alto grado, a condizione che non si creino conflitti di interesse.
6. L'ente dovrebbe porre in essere processi documentati per l'assegnazione della posizione di responsabile dei rischi e per la revoca di tale incarico. L'organo gestorio con funzione di supervisione strategica dovrebbe dare la sua preventiva approvazione alla sostituzione del responsabile dei rischi. In generale, la notizia della destituzione o della nomina di un responsabile dei rischi dovrebbe essere divulgata, e l'autorità di vigilanza deve essere informata sui motivi che hanno portato a tale destituzione/nomina.

28. Funzione di Conformità alle Norme (Compliance Function)

1. Un ente dovrebbe istituire una funzione di conformità alle norme per gestire il rischio di non conformità.
2. Un ente dovrebbe approvare e attuare una politica aziendale di conformità alle norme che deve essere resa nota a tutto il personale.

> Nota esplicativa
>
> Il rischio di non conformità (definito come il rischio effettivo o potenziale di perdite finanziarie e patrimoniali derivanti da violazioni o non conformità a leggi, norme, regolamenti, accordi, pratiche aziendali stabilite o standard etici) può comportare sanzioni, danni e/o l'annullamento di contratti e può danneggiare la reputazione di un ente.

3. Un ente dovrebbe istituire una funzione di conformità alle norme permanente ed efficace, e nominare un soggetto responsabile di tale funzione per tutto l'ente e il gruppo (il responsabile della conformità, Compliance Officer o Chief of Compliance). Negli enti di minore dimensione e complessità tale funzione può essere esercitata unitamente con le funzioni di controllo o di supporto, o assistita da esse (ad esempio per le risorse umane, l'ufficio legale, ecc.).

4. La funzione di conformità alle norme dovrebbe garantire il rispetto della politica aziendale in materia di conformità, e riferire all'organo gestorio e - se del caso - alla funzione di controllo dei rischi in merito alla gestione del rischio di non conformità da parte dell'ente. Le risultanze dell'attività della funzione di conformità alle norme dovrebbero essere tenute in considerazione dall'organo gestorio e dalla funzione di controllo dei rischi nell'ambito del processo decisionale.
5. La funzione di conformità alle norme dovrebbe fornire consulenza all'organo gestorio sulle leggi, le norme, i regolamenti e gli standard che l'ente è tenuto ad osservare, e dovrebbe valutare il possibile impatto di ogni modifica al contesto normativo e regolamentare sulle attività dell'ente.
6. La funzione di conformità alle norme dovrebbe anche verificare che i nuovi prodotti e le nuove procedure siano conformi al vigente contesto legislativo e a tutte le modifiche nella legislazione, nei regolamenti e nei requisiti prudenziali che siano di imminente emanazione e di cui si abbia notizia.

Nota esplicativa

Particolare attenzione dovrebbe essere prestata nei casi in cui l'ente svolga determinati servizi o metta in piedi strutture per conto della clientela (ad esempio agendo come consulente per la creazione di una società o di un'impresa collettiva (partnership), fornendo servizi fiduciari o sviluppando complesse operazioni finanziarie strutturate per la clientela) che possono sollevare particolari problemi di natura prudenziale e di organizzazione interna.

29. Funzione di Revisione Interna (Internal Audit Function)

1. La funzione di revisione interna dovrebbe valutare se la qualità del sistema dei controlli interni di un ente è efficace ed efficiente.
2. La funzione di revisione interna dovrebbe avere accesso senza alcuna restrizione ai documenti e alle informazioni rilevanti in tutte le unità operative e di controllo.
3. La funzione di revisione interna dovrebbe valutare la conformità di tutte le attività e le unità dell'ente (comprese la funzione di controllo dei rischi e la funzione di conformità alle norme) alle politiche aziendali e alle procedure dell'ente. Pertanto la funzione di revisione interna non dovrebbe essere combinata con altre funzioni. La funzione di revisione interna dovrebbe anche valutare se le politiche aziendali e le procedure esistenti siano adeguate e conformi ai requisiti giuridici e regolamentari.
4. La funzione di revisione interna dovrebbe verificare, in particolare, l'integrità dei processi che garantiscono l'affidabilità dei metodi e delle tecniche, delle ipotesi e delle sorgenti di informazioni utilizzati dall'ente nei modelli interni (ad esempio, la modellazione dei rischi e la misurazione contabile). La funzione di revisione interna dovrebbe anche valutare la qualità e l'uso di strumenti qualitativi di identificazione e valutazione dei rischi. Tuttavia, al fine di

rafforzare la propria indipendenza, la funzione di revisione interna non dovrebbe essere direttamente coinvolta nella definizione o nella selezione dei modelli o di altri strumenti di gestione del rischio.

5. L'organo gestorio dovrebbe incoraggiare i revisori interni ad aderire agli standard professionali nazionali e internazionali. L'attività di revisione interna dovrebbe essere eseguita sulla base di un piano di revisione (audit plan) e a dettagliati programmi di revisione (audit programs) che seguano un approccio basato sul rischio (risk-based approccio). Il piano di revisione dovrebbe essere approvato dal comitato per il controllo interno e/o dall'organo gestorio.

Nota esplicativa
Un esempio di standard professionali cui si fa riferimento nel testo potrebbero essere gli standard stabiliti dall'Institute of Internal Auditors.

6. La funzione di revisione interna dovrebbe riferire direttamente all'organo gestorio e/o al comitato per il controllo interno (se del caso) le sue risultanze e le proposte per miglioramenti rilevanti ai controlli interni. Tutte le raccomandazioni in materia di controlli interni dovrebbero essere sottoposte a una procedura formale di follow-up da parte dei rispettivi livelli della dirigenza al fine di garantire e riferire in merito alla loro attuazione.

E. Sistemi informativi e continuità operativa

30. Sistema informativo e comunicazione

1. Un ente dovrebbe disporre di sistemi informativi e di comunicazione efficaci e affidabili che coprano tutte le loro attività significative.

Nota esplicativa
Il processo decisionale della direzione potrebbe essere negativamente influenzato da informazioni non attendibili o fuorvianti fornite da sistemi non adeguatamente progettati e controllati. Una componente fondamentale delle attività di un ente è quindi quella di istituire e gestire sistemi informativi e di comunicazione che coprano il novero complessivo delle attività dell'ente. Le informazioni sono di norma fornite attraverso mezzi elettronici e non elettronici. Un ente dovrebbe essere particolarmente consapevole dei requisiti organizzativi e in materia di controlli interni relativi al trattamento delle informazioni in formato elettronico, e della necessità di avere una lista di controllo (audit trail) adeguata. Ciò si applica anche nei casi in cui il sistema informativo sia stato esternalizzato ad un fornitore di servizi IT (IT service provider).

2. I sistemi informativi, compresi quelli che conservano e utilizzano i dati in formato elettronico, dovrebbero essere sicuri, monitorati in maniera

indipendente e sostenuti da adeguati piani di emergenza (contingency arrangements). Quando un ente istituisce i sistemi informativi, esso dovrebbe conformarsi agli standard IT generalmente accettati.

31. Gestione della continuità operativa

1. Un ente dovrebbe avere un'efficace gestione della continuità operativa al fine di assicurare la propria capacità di operare su base continuativa e limitare le perdite in caso di grave interruzione dell'operatività.

Nota esplicativa
L'operatività di un ente dipende da diversi processi critici (ad esempio i sistemi informativi, i sistemi di comunicazione, gli edifici). Lo scopo della gestione della continuità operativa è minimizzare le rilevanti ricadute operative, finanziarie, giuridiche, reputazionali, ecc., derivanti da incidenti o catastrofi o da un blocco prolungato che colpiscono tali processi, e dalla conseguente interruzione delle procedure operative ordinarie dell'ente. Altre misure di gestione del rischio potrebbero essere: ridurre la probabilità che tali incidenti si verifichino, o trasferirne gli effetti finanziari a terzi (ad esempio mediante la stipula di un'assicurazione).

2. Al fine di stabilire un'efficace gestione della continuità operativa, un ente dovrebbe attentamente analizzare la propria esposizione a gravi interruzioni delle attività e valutare (dal punto di vista quantitativo e qualitativo) le possibili ripercussioni di tali eventi, ricorrendo ad analisi interne e/o esterne dei dati e degli scenari. L'analisi dovrebbe riguardare tutte le unità operative e di supporto e la funzione di controllo dei rischi, e dovrebbe tenere conto della loro interdipendenza. Dovrebbero inoltre essere attivamente coinvolte: una specifica funzione di continuità operativa indipendente, la funzione di controllo dei rischi o la funzione di gestione dei rischi operativi. I risultati dell'analisi dovrebbero contribuire a definire le priorità e gli obiettivi di recovery dell'ente.

Nota esplicativa
Riguardo alla funzione di gestione dei rischi operativi, cfr. anche l'allegato X, parte 3, paragrafo 4, della direttiva 2006/48/CE, che prevede l'istituzione di tale funzione indipendente per gli enti che utilizzano metodi avanzati di misurazione (AMA); i compiti di tale funzione sono descritti ai paragrafi 615-620 degli orientamenti ABE in materia di validazione pubblicati nel 2006 (EBA Guidelines on Validation), disponibili sul sito web dell'ABE.

3. Sulla base dell'analisi di cui sopra, un ente dovrebbe dotarsi di:

    a. piani di emergenza e di continuità operativa (contingency and business continuity plans) al fine di garantire che l'ente reagisca in maniera

adeguata alle emergenze e sia in grado di mantenere le attività operative critiche in caso di interruzione delle proprie procedure operative ordinarie;

b. piani di recovery (recovery plans) per i processi critici per consentire all'ente di ripristinare le procedure operative ordinarie in un intervallo di tempo appropriato. Tutti i rischi residuali derivanti da possibili interruzioni dell'attività dovrebbero essere coerenti con la tolleranza al rischio/propensione per il rischio dell'ente.

4. I piani di emergenza, di continuità operativa e di recovery dovrebbero essere documentati e attentamente attuati. La relativa documentazione dovrebbe essere disponibile all'interno delle unità operative e di supporto e della funzione di controllo dei rischi, e dovrebbe essere archiviata in sistemi fisicamente separati e prontamente accessibili in caso di emergenza. Il personale dovrebbe ricevere adeguata formazione al riguardo. I piani dovrebbero essere regolarmente testati e aggiornati. Eventuali problemi o carenze che si verifichino nel corso dei controlli dovrebbero essere documentati e analizzati, e i piani dovrebbero essere rivisti di conseguenza.

F. Trasparenza

32. Obblighi informativi

1. Gli indirizzi strategici e le politiche aziendali dovrebbero essere comunicati a tutto il personale rilevante all'interno dell'ente.
2. Il personale di un ente dovrebbe comprendere le politiche aziendali e le procedure che attengono ai propri compiti e responsabilità, e attenersi ad esse.
3. Di conseguenza, l'organo gestorio dovrebbe informare e aggiornare in maniera chiara e coerente il personale rilevante sugli indirizzi strategici e le politiche aziendali dell'ente, almeno al livello necessario per svolgere i propri compiti particolari. Allo scopo possono essere utilizzati orientamenti scritti, manuali o altri mezzi.

33. Trasparenza dell'organizzazione interna

1. L'organizzazione interna di un ente dovrebbe essere trasparente. Un ente dovrebbe presentare la propria posizione attuale e le prospettive future in modo chiaro, bilanciato, accurato e tempestivo.

Nota esplicativa
L'obiettivo della trasparenza nell'ambito dell'organizzazione interna è quello di fornire a tutti coloro che detengono un interesse nei confronti dell'ente (compresi gli azionisti, i dipendenti, i clienti e, in generale, il pubblico) le informazioni chiave per consentire a costoro di valutare l'efficacia dell'organo gestorio a dirigere l'ente.

In base all'articolo 72 della direttiva 2006/48/CE e all'articolo 2 della direttiva 2006/49/CE, gli enti creditizi imprese madri nell'UE e gli enti creditizi controllati da una società di partecipazione finanziaria madre nell'UE dovrebbero pubblicare informazioni complete e sostanziali che descrivano la propria organizzazione interna a livello consolidato. È buona prassi che ogni ente comunichi in maniera proporzionale informazioni sulla propria organizzazione interna su base individuale.

2. L'ente dovrebbe pubblicare almeno quanto segue:

   a. le proprie strutture e politiche aziendali in materia di assetti organizzativi, inclusi gli obiettivi, la struttura organizzativa, i meccanismi di organizzazione interna, la struttura e l'organizzazione dell'organo gestorio, compresa la frequenza delle partecipazioni, e il sistema degli incentivi e della remunerazione dell'ente;

   b. la natura, la portata, lo scopo e la sostanza economica delle operazioni con le parti associate e correlate, se hanno un impatto rilevante sull'ente;

   c. il modo in cui viene stabilita la propria strategia operativa e in materia di rischi (compreso il coinvolgimento dell'organo gestorio) e i fattori di rischio prevedibili;

   d. i comitati istituiti e i rispettivi mandati e composizioni;

   e. il sistema dei controlli interni e le modalità in cui le funzioni di controllo sono organizzare, i compiti principali che esse svolgono, il modo in cui le loro prestazioni sono monitorate dall'organo gestorio e le modifiche rilevanti pianificate per tali funzioni;

   f. le informazioni rilevanti riguardo i propri risultati finanziari e operativi.

3. Le informazioni sulla posizione attuale dell'ente dovrebbero essere conformi ai requisiti normativi in materia di disclosure. Le informazioni dovrebbero essere chiare, accurate, pertinenti, tempestive e accessibili.
4. Nei casi in cui un alto grado di accuratezza potrebbe comportare ritarderebbe ritardi nella pubblicazione di informazioni sensibili al fattore tempo, l'ente dovrebbe individuare il giusto bilanciamento tra tempestività e precisione, tenendo presente l'obbligo di fornire un quadro veritiero e corretto della propria situazione e di dover fornire una spiegazione soddisfacente per eventuali ritardi. Tale spiegazione non dovrebbe essere utilizzata per ritardare i regolari obblighi di reporting.

Titolo III – Disposizioni finali e attuazione

34. Abrogazione

Con l'adozione e la pubblicazione dei presenti orientamenti sull'organizzazione interna, vengono abrogati i seguenti orientamenti: la sezione 2.1, dal titolo

"Guidelines on Internal Governance", degli orientamenti del CEBS sull'applicazione del processo di revisione prudenziale (CEBS Guidelines on the Application of the Supervisory Review Process del 25 gennaio 2006); i principi di alto livello per le politiche aziendali di remunerazione (High Level Principles for Remuneration Policies del 20 aprile 2009) e i principi di alto livello per la gestione del rischio (High Level Principles for Risk Management del 16 febbraio 2010).

35. Data di applicazione

Le autorità competenti dovrebbero attuare gli orientamenti sull'organizzazione interna integrandoli nelle rispettive procedure di vigilanza entro il 31 marzo 2012. Dopo tale data, le autorità competenti sono tenute a garantire che gli enti si conformino effettivamente a tali orientamenti.