EBA/GL/2021/05

2 luglio 2021

Progetto di orientamenti

sulla governance interna

1. Conformità e obblighi di notifica

Status giuridico dei presenti orientamenti

1. I presenti orientamenti sono emanati in applicazione dell'articolo 16 del regolamento (UE) n. 1093/2010 ([1]). Conformemente all'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti e gli istituti finanziari, compresi gli enti, compiono ogni sforzo per conformarsi agli orientamenti.

2. Gli orientamenti definiscono la posizione 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 un particolare settore. Le autorità competenti di cui all'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010 sono tenute a conformarsi a detti orientamenti integrandoli opportunamente nelle rispettive prassi di vigilanza (ad es. modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti sono diretti principalmente agli enti.

Obblighi di notifica

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti devono comunicare all'ABE entro il (05.12.2021) se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna notifica da parte delle autorità competenti, queste sono ritenute dall'ABE non conformi. Le notifiche dovrebbero essere inviate trasmettendo il modulo disponibile sul sito web dell'ABE all'indirizzo compliance@eba.europa.eu con il riferimento «EBA/GL/2021/05» da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti. Ogni eventuale variazione dello status di conformità deve essere altresì comunicata all'ABE.

4. Le notifiche sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010.

([1]) 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 (GU L 331 del 15.12.2010, pag. 12).

2. Oggetto, ambito di applicazione e definizioni

Oggetto

5. I presenti orientamenti specificano ulteriormente i dispositivi, i processi e i meccanismi di governance interna che gli enti soggetti alla direttiva 2013/36/UE ([2]) e le imprese di investimento soggette al titolo VII di tale direttiva in applicazione dell'articolo 1, paragrafi 2 e 5, del regolamento (UE) 2019/2033 dovrebbero attuare in conformità dell'articolo 74, paragrafo 1, della direttiva 2013/36/UE, al fine di garantire una loro gestione efficace e prudente.

Destinatari

I presenti orientamenti sono rivolti alle autorità competenti di cui all'articolo 4, paragrafo 2, punto i), del regolamento (UE) n. 1093/2010 e agli istituti finanziari di cui all'articolo 4, paragrafo 1, del medesimo regolamento che siano enti ai fini dell'applicazione della direttiva 2013/36/UE secondo la definizione di cui all'articolo 3, paragrafo 1, punto 3), della suddetta direttiva, anche in considerazione dell'articolo 3, paragrafo 3, della medesima direttiva, o imprese di investimento soggette al titolo VII della direttiva 2013/36/UE in applicazione dell'articolo 1, paragrafi 2 e 5, del regolamento (UE) 2019/2033 («enti»).

Ambito di applicazione

6. I presenti orientamenti si applicano in relazione ai dispositivi di governance degli enti, fra cui la loro struttura organizzativa e le rispettive linee di responsabilità, i processi volti a individuare, gestire, monitorare e segnalare tutti i rischi ([3]) ai quali sono o potrebbero essere esposti nonché il quadro di controllo interno.

7. Gli orientamenti intendono includere tutte le strutture esistenti dei consigli e non ne sostengono nessuna in particolare. Gli orientamenti non interferiscono con la ripartizione generale delle competenze, in conformità del diritto societario nazionale. Di conseguenza, dovrebbero applicarsi indipendentemente dalle strutture amministrative impiegate (struttura monistica e/o dualistica e/o strutture di altra natura) negli Stati membri. L'organo di gestione, di cui all'articolo 3, paragrafo 1, punti 7 e 8, della direttiva 2013/36/UE, è da intendersi come avente funzioni di gestione (esecutive) e di supervisione strategica (non esecutive) ([4]).

([2]) Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).
([3]) Ogni riferimento ai rischi nei presenti orientamenti include i rischi legati al riciclaggio e al finanziamento del terrorismo.
([4]) Cfr. anche il considerando 56 della direttiva 2013/36/UE.

8. I termini «organo di amministrazione nella sua funzione di gestione» e «organo di amministrazione nella sua funzione di supervisione strategica» sono utilizzati nei presenti orientamenti senza riferimento a una struttura di governance specifica e i riferimenti alla funzione di gestione (esecutiva) o di supervisione strategica (non esecutiva) dovrebbero essere intesi in relazione agli organi o ai membri dell'organo di amministrazione responsabili di tale funzione, in conformità del diritto nazionale. Nell'attuare i presenti orientamenti, le autorità competenti dovrebbero prendere in considerazione il rispettivo diritto societario nazionale e specificare, laddove necessario, a quale organo o membro dell'organo di gestione dovrebbero applicarsi tali funzioni.

9. Negli Stati membri in cui l'organo di gestione delega, parzialmente o totalmente, le funzioni esecutive a una persona o a un organo esecutivo interno (ad es. un amministratore delegato, un team di gestione o un comitato esecutivo), le persone che esercitano dette funzioni esecutive sulla base di tale delega dovrebbero essere considerate parte della funzione di gestione dell'organo di gestione. Ai fini dei presenti orientamenti, qualunque riferimento all'organo di gestione nella sua funzione di gestione dovrebbe includere anche i membri dell'organo esecutivo o l'amministratore delegato, come definiti nei presenti orientamenti, anche se non sono stati proposti o nominati quali membri formali dell'organo o degli organi di gestione dell'ente a norma del diritto nazionale.

10. Negli Stati membri nei quali alcune responsabilità sono esercitate direttamente dagli azionisti, dai membri o dai proprietari dell'ente anziché dall'organo di gestione, gli enti dovrebbero garantire che tali responsabilità e le relative decisioni siano in linea, nei limiti del possibile, con gli orientamenti applicabili all'organo di gestione.

11. Le definizioni di amministratore delegato, direttore finanziario e personale che riveste ruoli chiave di cui ai presenti orientamenti hanno uno scopo puramente pratico e non intendono imporre una nomina per tali incarichi né creare tali posizioni, salvo se previsto dal diritto dell'Unione o nazionale in materia.

12. Gli enti dovrebbero attenersi ai presenti orientamenti e le autorità competenti dovrebbero garantirne il rispetto da parte degli enti su base individuale, subconsolidata e consolidata, in conformità del livello di applicazione stabilito all'articolo 109 della direttiva 2013/36/UE.

Definizioni

13. Salvo indicazione contraria, i termini utilizzati e definiti nella direttiva 2013/36/UE e nel regolamento (UE) n. 575/2013 hanno il medesimo significato nei presenti orientamenti. In aggiunta, ai fini dei presenti orientamenti, si applicano le definizioni riportate di seguito.

Amministratore delegato	la persona responsabile della gestione e dell'orientamento delle attività complessive di un ente.

Azionista	una persona che detiene le azioni di un ente o, a seconda della forma giuridica dell'ente, altri proprietari o membri dell'ente.
Capacità di rischio	il livello massimo di rischio che un ente è in grado di assumere, considerando la sua base di capitale e gestione dei rischi nonché le sue capacità di controllo e i suoi vincoli normativi.
Consolidamento prudenziale	l'applicazione delle norme prudenziali, di cui alla direttiva 2013/36/UE e al regolamento (UE) n. 575/2013, su base consolidata o subconsolidata, in conformità della parte 1, titolo II, capo 2, del regolamento (UE) n. 575/2013 ([5]).
Cultura del rischio	le norme, gli atteggiamenti e i comportamenti di un ente rispetto alla consapevolezza del rischio, all'assunzione e alla gestione del rischio, nonché i controlli che determinano le decisioni in merito ai rischi. La cultura del rischio influenza le decisioni dei dirigenti e dei dipendenti durante le attività quotidiane e si ripercuote sui rischi che essi assumono.
Direttore finanziario	la persona responsabile a livello generale della gestione di tutte le attività seguenti: gestione delle risorse finanziarie, pianificazione finanziaria e rendicontazione finanziaria.
Divario retributivo di genere	la differenza tra la remunerazione oraria lorda media di uomini e donne espressa come percentuale della remunerazione oraria lorda media degli uomini.
Ente consolidante	un ente tenuto a rispettare i requisiti prudenziali sulla base della situazione consolidata, in conformità della parte 1, titolo II, capo 2, del regolamento (UE) n. 575/2013.
Enti quotati	gli enti i cui strumenti finanziari sono ammessi alla negoziazione su un mercato regolamentato o su un sistema multilaterale di negoziazione, come definiti all'articolo 4, paragrafi 21 e 22, della direttiva 2014/65/UE, in uno o più Stati membri ([6]).
Enti significativi	gli enti di cui all'articolo 131 della direttiva 2013/36/UE [enti a rilevanza sistemica a livello globale (G-SII) e altri enti a rilevanza sistemica (O-SII)] e, a seconda dei casi, altri enti determinati dall'autorità competente o dal diritto nazionale, sulla base di una valutazione delle dimensioni e dell'organizzazione interna degli enti e della natura, ampiezza e complessità delle loro attività.
Incarico di amministratore	una posizione in qualità di membro dell'organo di gestione di un ente o di un'altra entità giuridica.

([5]) Cfr. anche le norme tecniche di regolamentazione in materia di consolidamento prudenziale, disponibili all'indirizzo: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf

([6]) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).

Personale	tutti i dipendenti di un ente e delle sue filiazioni nell'ambito del suo consolidamento, fra cui le filiazioni non soggette alla direttiva 2013/36/UE e tutti i membri dell'organo di gestione nella sua funzione di gestione e nella sua funzione di supervisione strategica.
Personale che riveste ruoli chiave	le persone che hanno un'influenza significativa sulla direzione dell'ente, ma che non sono membri dell'organo di amministrazione e non ricoprono il ruolo di amministratore delegato. Queste includono i responsabili delle funzioni di controllo interno e il direttore finanziario, se non sono membri dell'organo di gestione, e altro personale che riveste ruoli chiave, laddove individuati dagli enti secondo un approccio basato sul rischio. L'altro personale che riveste ruoli chiave potrebbe includere i responsabili di linee di business significative, di succursali dello Spazio economico europeo/Associazione europea di libero scambio, di filiazioni di paesi terzi e di altre funzioni interne.
Propensione al rischio	il livello aggregato e i tipi di rischio che un ente è disposto ad assumere in funzione della sua capacità di rischio, in linea con il suo modello di business, per conseguire gli obiettivi strategici che si è prefissato.
Responsabili delle funzioni di controllo interno	le persone al livello gerarchico più elevato incaricate di gestire in modo efficace l'operatività quotidiana delle funzioni indipendenti di gestione dei rischi, di conformità e di audit interno.

3. Attuazione

Data di applicazione

14. I presenti orientamenti aggiornati si applicano a partire dal 31 dicembre 2021.

Abrogazione

15. Gli orientamenti dell'ABE sulla governance interna (EBA/GL/2017/11) del 26 settembre 2017 sono abrogati con effetto dal 31 dicembre 2021.

4. Orientamenti

Titolo I. Proporzionalità

16. Il principio di proporzionalità sancito dall'articolo 74, paragrafo 2, della direttiva 2013/36/UE mira a garantire che i dispositivi di governance interna siano coerenti con il profilo di rischio individuale e il modello di business dell'ente, in modo che gli obiettivi di disposizioni e obblighi normativi siano raggiunti in modo efficace.

17. Nello sviluppo e nell'attuazione di dispositivi di governance interna, gli enti dovrebbero tener conto delle loro dimensioni e della loro organizzazione interna, nonché della natura, dell'ampiezza e della complessità delle loro attività. Gli enti significativi dovrebbero mettere in atto dispositivi di governance più sofisticati, mentre enti piccoli e meno complessi possono attuare dispositivi di governance più semplici. Gli enti dovrebbero tuttavia notare che le dimensioni o la rilevanza sistemica di un ente potrebbero, di per sé, non essere indicative della misura in cui tale ente è esposto ai rischi.

18. Ai fini dell'applicazione del principio di proporzionalità e allo scopo di garantire un'adeguata attuazione degli obblighi normativi e dei presenti orientamenti, enti e autorità competenti dovrebbero tener conto di tutti i seguenti aspetti:

    a. le dimensioni, in termini di totale di bilancio dell'ente e delle sue filiazioni rientranti nell'ambito del consolidamento prudenziale;

    b. la presenza geografica dell'ente e il volume delle proprie attività in ogni paese;

    c. la forma giuridica dell'ente, incluso se l'ente fa parte di un gruppo e, in tal caso, la valutazione della proporzionalità relativa al gruppo;

    d. se l'ente è quotato in borsa;

    e. se l'ente è autorizzato a utilizzare modelli interni per la misurazione dei requisiti patrimoniali (ad es. l'approccio basato sui rating interni);

    f. il tipo di attività e di servizi autorizzati prestati dall'ente (ad es. cfr. l'allegato 1 della direttiva 2013/36/UE e l'allegato 1 della direttiva 2014/65/UE);

    g. il modello di business e la strategia di base; la natura e la complessità delle attività nonché la struttura organizzativa dell'ente;

h. la strategia in materia di rischio, la propensione al rischio e l'effettivo profilo di rischio dell'ente, tenendo in considerazione anche il risultato delle valutazioni del capitale e della liquidità nello SREP;

i. gli assetti proprietari e la struttura di finanziamento dell'ente;

j. il tipo di clienti (ad es. clientela al dettaglio, società, istituzioni, piccole imprese, enti pubblici) e la complessità dei prodotti o dei contratti;

k. le funzioni esternalizzate e i canali di distribuzione;

l. i sistemi informatici disponibili, inclusi i sistemi di continuità e le funzioni esternalizzate in quest'area;

m. se l'ente rientra nella definizione di ente piccolo e non complesso o di grande ente di cui all'articolo 4, paragrafo 1, punti 145) e 146), del regolamento (UE) n. 575/2013.

Titolo II. Ruolo e composizione dell'organo di gestione e dei relativi comitati

1 Ruolo e responsabilità dell'organo di gestione

19. Conformemente all'articolo 88, paragrafo 1, della direttiva 2013/36/UE, l'organo di gestione deve avere la definitiva e generale responsabilità dell'ente e definisce, sorveglia e risponde dell'attuazione dei dispositivi di governance all'interno dell'ente che garantiscono una gestione efficace e prudente dello stesso.

20. I compiti dell'organo di gestione dovrebbero essere definiti con chiarezza, operando una distinzione tra i compiti della funzione di gestione (esecutiva) e quelli della funzione di supervisione strategica (non esecutiva). Le responsabilità e i compiti dell'organo di gestione dovrebbero essere descritti in un documento scritto e debitamente approvati dall'organo di gestione stesso. Tutti i membri dell'organo di gestione dovrebbero essere pienamente consapevoli della sua struttura e delle sue responsabilità nonché della suddivisione dei compiti tra le diverse funzioni dell'organo di gestione e dei suoi comitati.

21. L'organo di gestione nella sua funzione di supervisione strategica dovrebbe interagire in modo efficace con l'organo di gestione nella sua funzione di gestione. Ciascuna funzione dovrebbe fornire all'altra informazioni sufficienti per permettere a entrambe di svolgere i rispettivi ruoli. Al fine di conseguire un sistema appropriato di equilibrio dei poteri, il processo decisionale dell'organo di gestione non dovrebbe essere dominato da un singolo membro o da un gruppo ristretto dei suoi membri.

22. Le responsabilità dell'organo di gestione dovrebbero includere la definizione, l'approvazione e la sorveglianza dell'attuazione di quanto segue:

a. la strategia aziendale complessiva e le politiche chiave dell'ente nell'ambito del quadro giuridico e regolamentare applicabile, tenendo conto degli interessi finanziari e della solvibilità di lungo periodo dell'ente;

b. la strategia globale in materia di rischi, la propensione al rischio e il quadro di gestione dei rischi dell'ente nonché le misure per garantire che l'organo di gestione dedichi tempo sufficiente al rischio e alle questioni legate alla gestione del rischio;

c. un quadro adeguato ed efficace di governance interna e di controllo interno, come definito nel titolo V, che:

    i. includa una chiara struttura organizzativa e una gestione dei rischi interna indipendente ed efficiente, funzioni di conformità e audit che dispongano di autorità, peso e risorse nella misura sufficiente per svolgere le loro funzioni,

    ii. assicuri il rispetto degli obblighi normativi applicabili nel contesto della prevenzione del riciclaggio e del finanziamento del terrorismo;

d. gli importi, i tipi e la distribuzione sia di capitale interno che di capitale regolamentare al fine coprire adeguatamente i rischi dell'ente;

e. gli obiettivi per la gestione della liquidità dell'ente;

f. una politica di remunerazione che sia in linea con i principi stabiliti agli articoli da 92 a 95 della direttiva 2013/36/UE e negli orientamenti dell'ABE su sane politiche di remunerazione ai sensi dell'articolo 74, paragrafo 3, e dell'articolo 75, paragrafo 2, della direttiva 2013/36/UE ([7]);

g. dispositivi volti a garantire che le valutazioni di idoneità, individuali e collettive, dell'organo di gestione siano svolte in modo efficace, che la composizione e la pianificazione della successione dell'organo di gestione siano appropriate e che l'organo di gestione svolga le proprie funzioni in modo efficace ([8]);

h. un processo di selezione e di valutazione di idoneità per il personale che riveste ruoli chiave ([9]);

i. dispositivi volti a garantire il funzionamento interno di ciascun comitato dell'organo di gestione, laddove istituito, che stabiliscano nel dettaglio:

([7]) Orientamenti dell'ABE su sane politiche di remunerazione.
([8]) Cfr. anche gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave.
([9]) Cfr. anche gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave.

i. il ruolo, la composizione e i compiti di ciascuno di essi,

ii. l'adeguato flusso di informazioni, inclusa la documentazione relativa alle raccomandazioni e alle conclusioni, e le linee di segnalazione tra ciascun comitato e l'organo di gestione, le autorità competenti e altre parti;

j. una cultura del rischio in linea con la sezione 9 dei presenti orientamenti, che affronti la consapevolezza del rischio da parte dell'ente e il comportamento relativo all'assunzione del rischio;

k. una cultura e valori aziendali in linea con la sezione 10, che promuovano il comportamento responsabile ed etico, inclusi un codice di condotta o uno strumento equivalente;

l. una politica in materia di conflitti di interesse a livello dell'ente, in linea con la sezione 11 e, per il personale, in linea con la sezione 12;

m. dispositivi volti a garantire l'integrità dei sistemi di contabilità e di rendicontazione finanziaria, compresi i controlli finanziari e operativi e il rispetto delle disposizioni legislative e delle norme pertinenti.

23. Nel fissare, approvare e sorvegliare l'attuazione degli aspetti elencati al paragrafo 22, l'organo di gestione dovrebbe mirare ad assicurare un modello di business e dispositivi di governance, oltre a un quadro di gestione dei rischi che tenga conto di tutti i rischi. Nel prendere in considerazione tutti i rischi a cui sono esposti, gli enti dovrebbero tener conto di tutti i fattori di rischio pertinenti, compresi quelli ambientali, sociali e di governance. Gli enti dovrebbero tener presente che questi ultimi possono condizionare i rispettivi rischi prudenziali, compresi i rischi di credito, ad esempio tramite fattori di rischio legati alla transizione verso un'economia sostenibile o eventi esterni fisici legati al clima suscettibili di interessare i debitori, il mercato, la liquidità, i rischi operativi, e anche i rischi reputazionali, ad esempio mediante fattori di rischio sociale e di governance, come nel contesto di accordi di esternalizzazione ([10]). Tali rischi comprendono, ad esempio, i rischi legali nell'ambito del diritto contrattuale o del lavoro, i rischi relativi a potenziali violazioni dei diritti umani o altri fattori di rischio ambientali, sociali e di governance che possono influenzare il paese dove è stabilito un prestatore di servizi e la sua capacità di fornire i livelli di servizio concordati.

24. L'organo di gestione deve sorvegliare il processo di informativa e la comunicazione con le parti interessate esterne e le autorità competenti.

([10]) Cfr. la relazione dell'ABE sulla gestione e sulla supervisione dei rischi ambientali, sociali e di governance pubblicata ai sensi dell'articolo 98, paragrafo 8, della direttiva sui requisiti patrimoniali per una descrizione dell'interpretazione dei rischi ambientali, sociali e di governance da parte dell'ABE, dei canali di trasmissione e delle raccomandazioni relative a disposizioni, processi, meccanismi e strategie che gli enti devono attuare per individuare, valutare e gestire i rischi ambientali, sociali e di governance.

25. Tutti i membri dell'organo di gestione dovrebbero essere informati dell'attività generale, della situazione finanziaria e di rischio dell'ente, alla luce della situazione economica, nonché delle decisioni prese che si ripercuotono significativamente sull'attività dell'ente.

26. Un membro dell'organo di gestione può essere responsabile di una funzione di controllo interno, come indicato al titolo V, sezione 19.1, a condizione che al membro non siano stati conferiti altri mandati che comprometterebbero le sue attività di controllo interno e l'indipendenza della funzione di controllo interno.

27. L'organo di gestione dovrebbe monitorare, riesaminare periodicamente e risolvere eventuali carenze individuate nell'ambito dell'attuazione dei processi, delle strategie e delle politiche relative alle responsabilità di cui ai paragrafi 22 e 23. Il quadro di governance interna e la relativa attuazione dovrebbero essere rivisti e aggiornati periodicamente, sulla base del principio di proporzionalità, come chiarito ulteriormente al titolo I. Qualora l'ente sia interessato da cambiamenti sostanziali, dovrebbe essere svolta una revisione dettagliata.

2 Funzione di gestione dell'organo di gestione

28. L'organo di gestione nella sua funzione di gestione dovrebbe impegnarsi attivamente nell'ambito dell'attività di un ente e prendere decisioni su basi solide e con cognizione di causa.

29. L'organo di gestione nella sua funzione di gestione dovrebbe essere responsabile dell'attuazione delle strategie stabilite dall'organo di gestione e discutere regolarmente dell'attuazione e dell'idoneità di tali strategie con l'organo di gestione nella sua funzione di supervisione strategica. L'attuazione operativa può essere di competenza della dirigenza dell'ente.

30. L'organo di gestione nella sua funzione di gestione dovrebbe contestare in modo costruttivo e rivedere in modo critico le proposte, le motivazioni e le informazioni ricevute all'atto di formulare giudizi e prendere decisioni. L'organo di gestione nella sua funzione di gestione dovrebbe riferire in maniera esaustiva all'organo di gestione nella sua funzione di supervisione strategica, informarlo regolarmente e, laddove necessario, in modo tempestivo, in merito agli elementi pertinenti alla valutazione di una situazione, dei rischi e degli sviluppi che si ripercuotono o che possono ripercuotersi sull'ente, ad esempio le decisioni sostanziali sulle attività e sui rischi assunti, la valutazione del contesto economico e operativo dell'ente, della sua liquidità e della solidità della base di capitale nonché l'analisi delle sue esposizioni a rischi sostanziali.

31. Fatto salvo il recepimento della direttiva 2015/849/UE in materia di lotta al riciclaggio nella legislazione nazionale, l'organo di gestione dovrebbe identificare uno dei propri membri in linea con quanto prescritto all'articolo 46, paragrafo 4, di detta direttiva, conferendogli la responsabilità di attuare le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi a tale direttiva, comprese le corrispondenti politiche e procedure in materia

di contrasto al riciclaggio e al finanziamento del terrorismo in seno all'ente e a livello dell'organo di gestione ([11]).

3 Funzione di supervisione strategica dell'organo di gestione

32. Il ruolo dei membri dell'organo di gestione nella sua funzione di supervisione strategica dovrebbe includere il monitoraggio e una contestazione costruttiva della strategia dell'ente.

33. Fatto salvo il diritto nazionale, l'organo di gestione nella sua funzione di supervisione strategica dovrebbe essere costituito da membri indipendenti come indicato alla sezione 9.3 degli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave ai sensi delle direttive 2013/36/UE e 2014/65/UE.

34. Fatte salve le responsabilità attribuite a norma del diritto societario nazionale applicabile, l'organo di gestione nella sua funzione di supervisione strategica dovrebbe:

    a. sorvegliare e monitorare il processo decisionale e le azioni dell'organo di gestione nella sua funzione di gestione, nonché provvedere a una sorveglianza efficace dello stesso, inclusi il monitoraggio e l'analisi del suo rendimento individuale e collettivo e dell'attuazione della strategia e degli obiettivi dell'ente;

    b. contestare in modo costruttivo e rivedere in modo critico le proposte e le informazioni fornite dai membri dell'organo di gestione nella sua funzione di gestione, nonché le sue decisioni;

    c. tenendo conto del principio di proporzionalità di cui al titolo I, adempiere adeguatamente ai compiti e al ruolo del comitato dei rischi, del comitato per le remunerazioni e del comitato per le nomine, laddove tali comitati non siano stati istituiti;

    d. garantire e valutare periodicamente l'efficacia del quadro di governance interna dell'ente e adottare le misure appropriate per far fronte a eventuali carenze individuate;

    e. sorvegliare e monitorare la coerente attuazione degli obiettivi strategici, della struttura organizzativa e della strategia in materia di rischio dell'ente, la sua propensione al rischio e il quadro di gestione dei rischi, nonché di altre politiche (ad es. la politica di remunerazione) e del quadro per l'informativa;

    f. monitorare la coerente attuazione della cultura del rischio dell'ente;

([11]) L'organo di gestione in quanto organo collegiale rimane responsabile nel suo insieme.

g. sorvegliare l'attuazione e la tenuta di un codice di condotta o equivalente e di politiche efficaci per individuare, gestire e mitigare conflitti di interesse reali o potenziali;

h. sorvegliare l'integrità delle informazioni e delle relazioni finanziarie e il quadro di controllo interno, incluso un solido ed efficace quadro di gestione dei rischi;

i. garantire che i responsabili delle funzioni di controllo interno siano in grado di agire in modo indipendente e che, a prescindere dalla responsabilità di informare altri organi interni, linee o unità di business, possano sollevare problematiche e avvertire direttamente l'organo di gestione nella sua funzione di supervisione strategica, laddove necessario, nel caso in cui evoluzioni sfavorevoli del rischio si ripercuotano o possano ripercuotersi sull'ente;

j. monitorare l'attuazione del piano di audit interno, dopo il previo coinvolgimento del comitato dei rischi e del comitato per il controllo interno e per la revisione contabile, laddove tali comitati siano istituiti.

4 Ruolo del presidente dell'organo di gestione

35. Il presidente dell'organo di gestione dovrebbe guidare tale organo, contribuire a un efficiente flusso di informazioni all'interno dell'organo di gestione e tra l'organo di gestione e i comitati dello stesso, laddove istituiti, ed essere responsabile del suo efficace funzionamento globale.

36. Il presidente dovrebbe incoraggiare e promuovere discussioni aperte e critiche e garantire che pareri dissenzienti possano essere espressi e discussi nell'ambito del processo decisionale.

37. In generale, il presidente dell'organo di gestione dovrebbe essere un membro non esecutivo. Se al presidente è consentita l'assunzione di compiti esecutivi, l'ente dovrebbe adottare misure atte a mitigare eventuali ripercussioni negative sull'equilibrio dei poteri dell'ente (ad es. nominando un membro capofila o un membro indipendente di grado elevato del consiglio di amministrazione o disponendo di un ampio numero di membri non esecutivi all'interno dell'organo di gestione nella sua funzione di supervisione strategica). In particolare, in conformità dell'articolo 88, paragrafo 1, lettera e), della direttiva 2013/36/UE, il presidente dell'organo di gestione nella sua funzione di supervisione strategica di un ente non deve esercitare simultaneamente le funzioni di amministratore delegato in seno allo stesso ente, a meno che non sia giustificato dall'ente e autorizzato dalle autorità competenti.

38. Il presidente dovrebbe stabilire gli ordini del giorno delle riunioni e garantire che le questioni strategiche siano discusse in via prioritaria. Il presidente dovrebbe garantire che le decisioni dell'organo di gestione siano prese su basi solide e con cognizione di causa e che i documenti e le informazioni siano ricevuti con sufficiente anticipo rispetto alla riunione.

39. Il presidente dell'organo di gestione dovrebbe favorire una ripartizione chiara dei compiti tra i membri dell'organo di gestione e l'esistenza di un efficiente flusso di informazioni tra gli

stessi, al fine di consentire ai membri dell'organo di gestione nella sua funzione di supervisione strategica di contribuire in modo costruttivo alle discussioni e di votare con coscienza e conoscenza.

5 Comitati dell'organo di gestione nella sua funzione di supervisione strategica

5.1 Istituzione di comitati

40. In conformità dell'articolo 109, paragrafo 1, della direttiva 2013/36/UE, in combinato disposto con l'articolo 76, paragrafo 3, l'articolo 88, paragrafo 2, e l'articolo 95, paragrafo 1, della medesima direttiva, tutti gli enti che sono essi stessi significativi, considerati i livelli individuali, subconsolidati e consolidati, devono istituire un comitato dei rischi, un comitato per le nomine ([12]) e un comitato per le remunerazioni ([13]), per fornire consulenza all'organo di gestione nella sua funzione di supervisione strategica e per preparare le decisioni che tale organo deve prendere. Gli enti non significativi, anche quando rientrano nell'ambito del consolidamento prudenziale di un ente significativo in una situazione subconsolidata o consolidata, non sono obbligati a istituire tali comitati.

41. Laddove non venga istituito un comitato dei rischi o un comitato per le nomine, i riferimenti ai suddetti comitati nei presenti orientamenti si intendono applicabili all'organo di gestione nella sua funzione di supervisione strategica, tenendo conto del principio di proporzionalità di cui al titolo I.

42. Gli enti, alla luce dei criteri menzionati al titolo I dei presenti orientamenti, possono istituire altri comitati (ad es., il comitato per il contrasto al riciclaggio e al finanziamento al terrorismo, il comitato per l'etica, il comitato per la condotta e il comitato per la conformità).

43. Gli enti dovrebbero garantire una chiara ripartizione e distribuzione dei doveri e dei compiti tra i comitati specializzati dell'organo di gestione.

44. Ogni comitato dovrebbe avere un mandato documentato, che includa la relativa sfera di competenza, attribuito dall'organo di gestione nella sua funzione di supervisione strategica e stabilire procedure di lavoro adeguate.

45. I comitati dovrebbero coadiuvare la funzione di supervisione strategica in aree specifiche e favorire lo sviluppo e l'attuazione di un sano quadro di governance interna. La delega ai comitati non esime in alcun modo l'organo di gestione nella sua funzione di supervisione strategica dall'adempiere collettivamente ai propri compiti e responsabilità.

([12]) Cfr. anche gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave ai sensi delle direttive 2013/36/UE e 2014/65/UE.
([13]) In merito al comitato per le remunerazioni, si faccia riferimento agli orientamenti dell'ABE su sane politiche di remunerazione.

5.2 Composizione dei comitati ([14])

46. Tutti i comitati dovrebbero essere presieduti da un membro non esecutivo dell'organo di gestione, in grado di esercitare un giudizio obiettivo.

47. I membri indipendenti ([15]) dell'organo di gestione nella sua funzione di supervisione strategica dovrebbero essere attivamente coinvolti nei comitati.

48. Se istituiti conformemente alla direttiva 2013/36/UE o al diritto nazionale, i comitati devono essere composti da almeno tre membri.

49. Gli enti dovrebbero assicurare, tenendo conto delle dimensioni dell'organo di gestione e del numero di membri indipendenti dell'organo di gestione nella sua funzione di supervisione strategica, che i comitati non siano composti dallo stesso gruppo di membri che formano un altro comitato.

50. Gli enti dovrebbero valutare la possibilità di procedere a una rotazione occasionale dei presidenti e dei membri dei comitati, tenendo conto dell'esperienza, delle conoscenze e delle competenze specifiche richieste a livello individuale o collettivo per tali comitati.

51. Il comitato dei rischi e il comitato per le nomine dovrebbero essere composti da membri non esecutivi dell'organo di gestione nella sua funzione di supervisione strategica dell'ente in questione. Il comitato per il controllo interno e per la revisione contabile dovrebbe essere composto conformemente all'articolo 41 della direttiva 2006/43/CE ([16]). Il comitato per le remunerazioni dovrebbe essere composto conformemente alla sezione 2.4.1 degli orientamenti dell'ABE su sane politiche di remunerazione ([17]).

52. Nei G-SII e negli O-SII, il comitato per le nomine dovrebbe includere una maggioranza di membri indipendenti ed essere presieduto da un membro indipendente. Negli altri enti significativi, sulla base di quanto stabilito dalle autorità competenti o prescritto dal diritto nazionale, il comitato per le nomine dovrebbe includere un numero sufficiente di membri indipendenti; tali enti possono anche prendere in considerazione la buona pratica di nominare un presidente indipendente per il comitato per le nomine.

53. I membri del comitato per le nomine dovrebbero possedere, a livello individuale e collettivo, conoscenze, capacità e competenze adeguate in merito al processo di selezione e ai requisiti di adeguatezza, come stabilito nella direttiva 2013/36/UE.

([14]) Questa sezione dovrebbe essere letta unitamente agli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave ai sensi delle direttive 2013/36/UE e 2014/65/UE.
([15]) Come definito nella sezione 9.3 degli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave ai sensi delle direttive 2013/36/UE e 2014/65/UE.
([16]) Direttiva 2006/43/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE del Consiglio e abroga la direttiva 84/253/CEE del Consiglio (GU L 157 del 9.6.2006, pag. 87), modificata da ultimo dalla direttiva 2014/56/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014.
([17]) Orientamenti su sane politiche di remunerazione ai sensi dell'articolo 74, paragrafo 3, e dell'articolo 75, paragrafo 2, della direttiva 2013/36/UE e sull'informativa ai sensi dell'articolo 450 del regolamento (UE) n. 575/2013 (ABE/GL/2015/22).

54. Nei G-SII e negli O-SII, il comitato dei rischi dovrebbe essere composto in maggioranza da membri indipendenti. Nei G-SII e negli O-SII, il presidente del comitato dei rischi dovrebbe essere un membro indipendente. Negli altri enti significativi, sulla base di quanto stabilito dalle autorità competenti o prescritto dal diritto nazionale, il comitato dei rischi dovrebbe includere un numero sufficiente di membri indipendenti ed essere presieduto, laddove possibile, da un membro indipendente. In tutti gli enti, la presidenza del comitato dei rischi non dovrebbe coincidere né con la presidenza dell'organo di gestione né con la presidenza di qualsiasi altro comitato.

55. I membri del comitato dei rischi dovrebbero possedere, a livello individuale e collettivo, conoscenze, capacità e competenze adeguate in merito alle pratiche di gestione dei rischi e di controllo.

5.3 Processi dei comitati

56. I comitati dovrebbero informare regolarmente l'organo di gestione nella sua funzione di supervisione strategica.

57. I comitati dovrebbero interagire tra loro, ove opportuno. Fatto salvo il paragrafo 49, tale interazione potrebbe assumere la forma di partecipazione incrociata, in modo tale che il presidente o un membro di un comitato possa essere anche membro di un altro comitato.

58. I membri dei comitati dovrebbero impegnarsi in discussioni aperte e con spirito critico, durante le quali i pareri dissenzienti siano discussi in modo costruttivo.

59. I comitati dovrebbero documentare gli ordini del giorno delle rispettive riunioni nonché i relativi risultati e conclusioni principali.

60. Il comitato dei rischi e il comitato per le nomine dovrebbero quantomeno:

    a. avere accesso a tutte le informazioni e a tutti i dati pertinenti necessari allo svolgimento del loro ruolo, incluse le informazioni e i dati provenienti da funzioni societarie e di controllo pertinenti (ad es. di tipo legale e finanziario e quelli relativi a risorse umane, informatica, audit interno, rischi, conformità, incluse informazioni sulla conformità ai requisiti in materia di contrasto al riciclaggio e al finanziamento del terrorismo e informazioni aggregate su segnalazioni di operazioni sospette e fattori di rischio legati al riciclaggio e al finanziamento del terrorismo);

    b. ricevere periodicamente relazioni, informazioni ad hoc, comunicazioni e pareri dai responsabili delle funzioni di controllo interno, relativamente al profilo di rischio corrente dell'ente, alla sua cultura del rischio e ai suoi limiti in tale ambito, nonché in merito a ogni violazione sostanziale ([18]) che possa verificarsi, corredati di informazioni

([18]) Per quanto riguarda le gravi violazioni in materia di contrasto al riciclaggio e al finanziamento del terrorismo. Cfr. anche agli orientamenti da emanare ai sensi dell'articolo 117, paragrafo 6, della direttiva 2013/36/UE, che precisano le modalità di collaborazione e scambio di informazioni tra le autorità di cui al paragrafo 5 di detto articolo, in particolare in relazione ai gruppi transfrontalieri e all'individuazione di gravi violazioni delle norme antiriciclaggio.

dettagliate e raccomandazioni sulle misure correttive adottate, da adottare o consigliare per farvi fronte; riesaminare su base periodica e prendere decisioni per quanto concerne contenuto, formato e frequenza delle informazioni sul rischio da comunicare loro;

c. laddove necessario, garantire l'adeguato coinvolgimento delle funzioni di controllo interno e di altre funzioni pertinenti (risorse umane, affari giuridici, finanze) nelle loro rispettive aree di competenza e/o consultare un esperto esterno per un parere.

5.4 Ruolo del comitato dei rischi

61. Se istituito, il comitato dei rischi dovrebbe quantomeno:

a. fornire consulenza e assistenza all'organo di gestione nella sua funzione di supervisione strategica relativamente al monitoraggio della strategia in materia di rischio e della propensione al rischio generali dell'ente, sia correnti che future, tenendo in considerazione tutte le tipologie di rischi, per garantire che siano in linea con la strategia aziendale, gli obiettivi, la cultura societaria e i valori dell'ente;

b. fornire assistenza all'organo di gestione nella sua funzione di supervisione strategica nel sorvegliare l'attuazione della strategia dell'ente in materia di rischio e i limiti corrispondenti stabiliti;

c. sorvegliare l'attuazione delle strategie per la gestione del capitale e della liquidità, nonché per tutti gli altri rischi pertinenti di un ente, quali i rischi di mercato, di credito, operativi (inclusi i rischi legali e informatici) e i rischi reputazionali, al fine di valutare la loro idoneità rispetto alla strategia in materia di rischio e alla propensione al rischio approvate;

d. fornire all'organo di gestione nella sua funzione di supervisione strategica le raccomandazioni sugli adeguamenti necessari alla strategia in materia di rischio risultanti, fra le altre cose, da modifiche al modello di business dell'ente, sviluppi di mercato o raccomandazioni formulate dalla funzione di gestione dei rischi;

e. fornire pareri sulla nomina di consulenti esterni che la funzione di supervisione strategica può decidere di impiegare per ottenere pareri o assistenza;

f. riesaminare alcuni possibili scenari, inclusi gli scenari di stress, per valutare in che modo il profilo di rischio dell'ente reagirebbe a eventi esterni e interni;

g. sorvegliare l'allineamento tra tutti i prodotti e i servizi finanziari rilevanti offerti ai clienti, il modello di business e la strategia in materia di rischio dell'ente ([19]). Il comitato dei rischi dovrebbe valutare i rischi associati ai prodotti e servizi finanziari offerti e

([19]) Cfr. anche gli orientamenti dell'ABE sui dispositivi di governance e di controllo sui prodotti bancari al dettaglio, disponibili all'indirizzo http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

tener conto dell'allineamento tra i prezzi attribuiti a tali prodotti e servizi e i profitti ricavati dagli stessi;

h. valutare le raccomandazioni dei revisori interni o esterni e dare seguito all'attuazione appropriata delle misure adottate.

62. Il comitato dei rischi dovrebbe collaborare con gli altri comitati, le cui attività possono ripercuotersi sulla strategia in materia di rischio (ad es. il comitato per il controllo interno e per la revisione contabile e il comitato per le remunerazioni) e comunicare regolarmente con le funzioni di controllo interno dell'ente, in particolare con la funzione di gestione dei rischi.

63. Il comitato dei rischi, qualora istituito, deve esaminare, fatti salvi i compiti del comitato per le remunerazioni, se gli incentivi forniti dalle politiche e pratiche di remunerazione tengano conto dei rischi, del capitale e della liquidità dell'ente, nonché della probabilità e della tempistica degli utili.

5.5 Ruolo del comitato per il controllo interno e per la revisione contabile

64. In conformità della direttiva 2006/43/CE ([20]), laddove istituito, il comitato per il controllo interno e per la revisione contabile dovrebbe, tra le altre cose:

a. controllare l'efficacia dei sistemi di controllo interno della qualità e di gestione del rischio dell'ente e, se del caso, della sua funzione di audit interno, per quanto riguarda l'informativa finanziaria dell'ente sottoposto a revisione, senza violare la sua indipendenza;

b. sorvegliare l'istituzione di politiche contabili da parte dell'ente;

c. monitorare il processo di informativa finanziaria e presentare raccomandazioni volte a garantirne l'integrità;

d. verificare e monitorare l'indipendenza dei revisori legali o delle imprese di revisione contabile a norma degli articoli 22, 22 *bis*, 22 *ter*, 24 *bis* e 24 *ter*, della direttiva 2006/43/CE e dell'articolo 6 del regolamento (UE) n. 537/2014 ([21]), in particolare per quanto concerne l'adeguatezza della prestazione di servizi non di revisione contabile all'ente sottoposto a revisione conformemente all'articolo 5 di tale regolamento;

([20]) Direttiva 2006/43/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE del Consiglio e abroga la direttiva 84/253/CEE del Consiglio (GU L 157 del 9.6.2006, pag. 87), modificata da ultimo dalla direttiva 2014/56/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014.
([21]) Regolamento (UE) n. 537/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sui requisiti specifici relativi alla revisione legale dei conti di enti di interesse pubblico e che abroga la decisione 2005/909/CE della Commissione (GU L 158 del 27.5.2014, pag. 77).

e. monitorare la revisione legale del bilancio d'esercizio e del bilancio consolidato, in particolare la sua esecuzione, tenendo conto di eventuali risultati e conclusioni dell'autorità competente a norma dell'articolo 26, paragrafo 6, del regolamento (UE) n. 537/2014;

f. essere responsabile della procedura volta alla selezione dei revisori legali o delle imprese di revisione contabile esterni e raccomandare i revisori legali o le imprese di revisione contabile da designare, la loro remunerazione e il loro licenziamento, da parte dell'organo competente dell'ente [in conformità dell'articolo 16 del regolamento (UE) n. 537/2014, tranne nel caso in cui si applichi l'articolo 16, paragrafo 8, del regolamento (UE) n. 537/2014];

g. riesaminare l'estensione della revisione contabile e la frequenza della revisione contabile del bilancio d'esercizio o del bilancio consolidato;

h. in conformità dell'articolo 39, paragrafo 6, lettera a), della direttiva 2006/43/CE, informare l'organo di amministrazione o di controllo dell'ente sottoposto a revisione dell'esito della revisione legale dei conti e spiegare in che modo quest'ultima ha contribuito all'integrità dell'informativa finanziaria e il ruolo del comitato per il controllo interno e la revisione contabile in tale processo;

i. ricevere e tenere in conto le relazioni sulla revisione contabile.

5.6 Comitati congiunti

65. In conformità dell'articolo 76, paragrafo 3, della direttiva 2013/36/UE, le autorità competenti possono consentire agli enti non considerati significativi di istituire in forma congiunta il comitato dei rischi e, se previsto, il comitato per il controllo interno e per la revisione contabile di cui all'articolo 39 della direttiva 2006/43/CE.

66. Se istituiti all'interno di enti non significativi, il comitato dei rischi e il comitato per le nomine possono essere costituiti in forma congiunta. In tal caso, tali enti dovrebbero documentare i motivi per i quali hanno scelto di istituire in forma congiunta i comitati e in che modo tale strategia consente di conseguire gli obiettivi dei comitati stessi.

67. Gli enti dovrebbero, in qualunque momento, garantire che i membri di un comitato congiunto posseggano, a livello individuale e collettivo, le conoscenze, capacità e competenze necessarie per comprendere pienamente i doveri che il comitato congiunto è chiamato a svolgere ([22]).

[22] Cfr. anche gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave ai sensi delle direttive 2013/36/UE e 2014/65/UE.

Titolo III. Quadro di governance

6 Quadro e struttura a livello organizzativo

6.1 Quadro organizzativo

68. L'organo di gestione di un ente dovrebbe garantire una struttura organizzativa e operativa adeguata e trasparente per tale ente nonché predisporne una descrizione scritta. La struttura dovrebbe promuovere e dimostrare la gestione efficace e prudente di un ente a livello individuale, subconsolidato e consolidato. L'organo di gestione dovrebbe garantire che le funzioni di controllo interno siano indipendenti dalle linee di business soggette al loro controllo, il che include un'adeguata separazione delle funzioni oltre a risorse finanziarie e umane idonee, nonché poteri per esercitare il proprio ruolo in modo efficace. Le linee di segnalazione e la ripartizione delle responsabilità, in particolare fra il personale che riveste ruoli chiave, all'interno di un ente dovrebbero essere chiare, ben definite, coerenti, applicabili e debitamente documentate. La documentazione dovrebbe essere aggiornata, secondo le esigenze.

69. La struttura dell'ente non dovrebbe costituire un ostacolo alla capacità dell'organo di gestione di sorvegliare e gestire in modo efficace i rischi per l'ente o per il gruppo oppure alla capacità dell'autorità competente di supervisionare l'ente in modo efficace.

70. L'organo di gestione dovrebbe valutare se e in che modo eventuali modifiche sostanziali della struttura del gruppo (ad es. l'istituzione di nuove filiazioni, le fusioni e le acquisizioni, la vendita o la liquidazione di parti del gruppo o sviluppi esterni) incidano sulla solidità del quadro organizzativo dell'ente. Se vengono individuate delle carenze, l'organo di gestione dovrebbe intervenire rapidamente attuando le necessarie misure correttive.

6.2 Conoscere la propria struttura

71. L'organo di gestione dovrebbe conoscere e comprendere pienamente la struttura giuridica, organizzativa e operativa dell'ente (c.d. «*know your structure*») e garantire che essa sia in linea con la strategia aziendale, la strategia in materia di rischio e la propensione al rischio che l'ente stesso ha approvato e che sia inclusa nel suo quadro di gestione dei rischi.

72. L'organo di gestione dovrebbe anche rispondere dell'approvazione di strategie e politiche sane per l'istituzione di nuove strutture. Qualora un ente crei molte entità giuridiche all'interno del proprio gruppo, il loro numero e, in modo particolare, i legami e le operazioni che intercorrono tra loro non dovrebbero costituire un problema per la definizione della governance interna dell'ente né per l'efficace gestione e sorveglianza dei rischi del gruppo nel suo complesso. L'organo di gestione dovrebbe garantire che la struttura di un ente e, laddove applicabile, le strutture all'interno di un gruppo, tenuto conto dei criteri specificati alla sezione 7, siano chiare, efficienti e trasparenti per il personale, gli azionisti e le altre parti interessate dell'ente, nonché per l'autorità competente.

73. L'organo di gestione dovrebbe dirigere la struttura dell'ente, guidarne l'evoluzione e far fronte ai relativi limiti, oltre a garantire che la struttura sia giustificata ed efficiente e non presenti un grado di complessità eccessivo o non appropriato.

74. L'organo di gestione di un ente consolidante dovrebbe capire non soltanto la struttura giuridica, organizzativa e operativa del gruppo, ma anche il fine e le attività delle diverse entità nonché i legami e le relazioni tra queste ultime. Ciò include la comprensione dei rischi operativi specifici del gruppo, delle esposizioni infragruppo e di come i profili di finanziamento, capitale, liquidità e rischio del gruppo potrebbero esserne influenzati in condizioni normali e in circostanze avverse. L'organo di gestione dovrebbe garantire che l'ente sia in grado di fornire informazioni sul gruppo in maniera tempestiva, relativamente al tipo, alle caratteristiche, all'organigramma, all'assetto proprietario e alle attività di ciascuna entità giuridica, e che gli enti all'interno del gruppo rispettino tutti gli obblighi di segnalazione a fini di vigilanza su base individuale, subconsolidata e consolidata.

75. L'organo di gestione dell'ente consolidante dovrebbe garantire che le diverse entità del gruppo (incluso l'ente consolidante stesso) ricevano informazioni sufficienti per avere un'idea chiara degli obiettivi, delle strategie e del profilo di rischio del gruppo in termini generali e di come l'entità del gruppo interessata sia incorporata nella struttura e nel funzionamento operativo del gruppo. Tali informazioni e le relative revisioni dovrebbero essere documentate e rese disponibili alle funzioni pertinenti interessate, fra cui l'organo di gestione, le linee di business e le funzioni di controllo interno. I membri dell'organo di gestione di un ente consolidante dovrebbero tenersi informati riguardo ai rischi posti dalla struttura del gruppo, prendendo in considerazione i criteri indicati alla sezione 7 degli orientamenti. Ciò include il ricevimento di:

    a. informazioni sui principali fattori di rischio;

    b. relazioni periodiche che valutino la struttura generale dell'ente e la conformità delle attività delle singole entità alla strategia approvata all'interno dell'intero gruppo;

    c. relazioni periodiche su argomenti per i quali il quadro normativo richiede conformità a livello individuale, subconsolidato e consolidato.

6.3 Strutture complesse e attività non standard o non trasparenti

76. Gli enti dovrebbero evitare di istituire strutture complesse e potenzialmente non trasparenti. Gli enti dovrebbero tener conto, nel loro processo decisionale, dei risultati della valutazione dei rischi effettuata allo scopo di valutare se tali strutture possano essere utilizzate a fini di riciclaggio, finanziamento del terrorismo o altri reati finanziari, nonché dei rispettivi controlli e del quadro normativo in vigore ([23]). A tal fine, gli enti dovrebbero tener conto quantomeno:

([23]) Per ulteriori dettagli sulla valutazione del rischio paese e del rischio associato a singoli prodotti e clienti, gli enti dovrebbero fare riferimento anche agli orientamenti congiunti sui fattori di rischio di riciclaggio/finanziamento del terrorismo (EBA GL JC/2017/37) attualmente in fase di revisione.

a. della misura in cui il paese nel quale sarà istituita la struttura rispetta effettivamente le norme dell'Unione e internazionali in materia di trasparenza fiscale, contrasto al riciclaggio e al finanziamento del terrorismo ([24]);

b. della misura in cui la struttura serve un evidente obiettivo economico e lecito;

c. della misura in cui la struttura potrebbe essere utilizzata per nascondere l'identità del titolare effettivo;

d. della misura in cui la richiesta del cliente che porta alla possibile istituzione di una struttura sollevi preoccupazioni;

e. se la struttura possa impedire la sorveglianza appropriata da parte dell'organo di gestione dell'ente o la capacità dell'ente di gestire il rischio correlato;

f. se la struttura ponga ostacoli a un'efficace vigilanza da parte delle autorità competenti.

77. In ogni caso, gli enti non dovrebbero istituire strutture poco chiare o inutilmente complesse che non abbiano una chiara motivazione economica o un obiettivo lecito, o strutture che potrebbero far pensare che siano state create per un obiettivo legato a reati finanziari.

78. Nell'istituzione di tali strutture, l'organo di gestione dovrebbe comprenderne le caratteristiche, l'obiettivo e i rischi specifici a queste associati, e garantire che le funzioni di controllo interno siano adeguatamente coinvolte. Tali strutture dovrebbero essere approvate e mantenute soltanto quando il loro obiettivo è stato definito e compreso in modo chiaro e quando l'organo di gestione abbia accertato che tutti i rischi sostanziali, inclusi i rischi reputazionali, siano stati individuati, che tutti i rischi possano essere gestiti in modo efficace e debitamente comunicati, e che venga garantita una sorveglianza efficace. Quanto più complessa e poco chiara è la struttura organizzativa e operativa, tanto più elevati sono i rischi e tanto più intensa dovrebbe essere la sorveglianza della struttura.

79. Gli enti dovrebbero documentare le loro decisioni ed essere in grado di giustificarle alle autorità competenti.

80. L'organo di gestione dovrebbe garantire che siano adottate opportune misure per evitare o mitigare i rischi di attività all'interno di tali strutture. Ciò include la garanzia che:

a. l'ente disponga di politiche e procedure adeguate e di processi documentati (ad es. limiti applicabili, flussi d'informazione) per la valutazione, la conformità, l'approvazione e la gestione dei rischi di tali attività, tenendo conto delle conseguenze per la struttura organizzativa e operativa del gruppo, del suo profilo di rischio e del relativo rischio reputazionale;

([24]) Cfr. anche: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries

b. le informazioni relative a tali attività e ai rischi associati siano accessibili da parte dell'ente consolidante e dei revisori contabili interni ed esterni e vengano comunicate all'organo di gestione nella sua funzione di supervisione strategica e all'autorità competente che ha rilasciato l'autorizzazione;

c. l'ente valuti periodicamente la continua necessità di mantenere tali strutture.

81. Tali strutture e attività, inclusa la rispettiva conformità alla legislazione e alle norme professionali, dovrebbero essere soggette a revisione periodica da parte della funzione di audit interno sulla base di un approccio basato sul rischio.

82. Gli enti dovrebbero adottare le stesse misure di gestione dei rischi di cui si avvalgono per le proprie attività operative quando svolgono attività non standard o non trasparenti per i clienti (ad es. assistenza ai clienti per istituire società veicolo in paesi offshore, sviluppo di strutture complesse, finanziamento di transazioni per queste ultime o prestazione di servizi fiduciari) che pongono analoghe sfide di governance interna e creano significativi rischi operativi e reputazionali. In particolare, gli enti dovrebbero analizzare il motivo per cui un cliente intende istituire una determinata struttura.

7 Quadro organizzativo in un contesto di gruppo

83. In conformità dell'articolo 109, paragrafo 2, della direttiva 2013/36/UE, le imprese madri e le filiazioni soggette a tale direttiva garantiscono che i dispositivi, i processi e i meccanismi di governance siano coerenti e ben integrati su base consolidata e subconsolidata. A tal fine, le imprese madri e le filiazioni rientranti nell'ambito del consolidamento prudenziale dovrebbero attuare nelle loro filiazioni non soggette alla direttiva 2013/36/UE, comprese quelle stabilite in paesi terzi, tra cui centri finanziari offshore, dispositivi, processi e meccanismi tali da garantire solidi dispositivi di governance su base consolidata e subconsolidata. Per quanto riguarda i requisiti in materia di remunerazione, si applicano alcune eccezioni conformemente all'articolo 109, paragrafi 4 e 5 ([25]). Le funzioni competenti all'interno dell'ente consolidante e delle sue filiazioni dovrebbero interagire e scambiare dati e informazioni, a seconda dei casi. I dispositivi, i processi e i meccanismi di governance dovrebbero garantire che l'ente consolidante disponga di dati e informazioni sufficienti e sia in grado di valutare il profilo di rischio del gruppo, come specificato nella sezione 6.2.

84. L'organo di gestione di una filiazione soggetta alla direttiva 2013/36/UE dovrebbe adottare e attuare a livello individuale le politiche di governance del gruppo, stabilite a livello consolidato o subconsolidato, in modo da rispettare tutti gli obblighi specifici in conformità del diritto dell'Unione e nazionale.

85. Al livello consolidato e subconsolidato, l'ente consolidante dovrebbe garantire l'osservanza delle politiche in materia di governance e del quadro di controllo interno del gruppo di cui al titolo V da parte di tutti gli enti e delle altre entità rientranti nell'ambito del consolidamento

([25]) Cfr. anche gli orientamenti dell'ABE su sane politiche di remunerazione.

prudenziale, incluse le loro filiazioni non soggette alla direttiva 2013/36/UE. Nell'applicare le politiche in materia di governance, l'ente consolidante dovrebbe garantire la presenza di solidi dispositivi di governance per ciascuna filiazione e prendere in considerazione dispositivi, processi e meccanismi specifici in cui le attività siano organizzate non in entità giuridiche separate, ma all'interno di una matrice di linee di business che includa entità giuridiche multiple.

86. Un ente consolidante dovrebbe prendere in considerazione gli interessi di tutte le sue filiazioni e i modi in cui le strategie e le politiche contribuiscono all'interesse di ciascuna filiazione, nonché l'interesse del gruppo nel suo insieme sul lungo termine.

87. Le imprese madri e le loro filiazioni dovrebbero garantire che gli enti e le entità all'interno del gruppo rispettino tutti gli obblighi normativi specifici in ciascun paese interessato.

88. L'ente consolidante dovrebbe garantire che le filiazioni istituite nei paesi terzi e rientranti nell'ambito del consolidamento prudenziale abbiano messo in atto dispositivi, processi e meccanismi di governance compatibili con le politiche di governance del gruppo e che rispettino le prescrizioni degli articoli da 74 a 96 della direttiva 2013/36/UE e dei presenti orientamenti, purché ciò non contravvenga alle leggi del paese terzo.

89. Gli obblighi in materia di governance di cui alla direttiva 2013/36/UE e le disposizioni dei presenti orientamenti si applicano agli enti indipendentemente dal fatto che essi siano o meno filiazioni di un'impresa madre di un paese terzo. Qualora una filiazione nell'Unione europea di un'impresa madre stabilita in un paese terzo sia un ente consolidante, l'ambito del consolidamento prudenziale non comprende il livello dell'impresa madre ubicata nel paese terzo e altre filiazioni dirette di tale impresa madre. L'ente consolidante dovrebbe assicurare che la politica di governance di gruppo dell'ente impresa madre in un paese terzo sia presa in considerazione nell'ambito della propria politica di governance, nella misura in cui ciò non sia contrario agli obblighi stabiliti sulla base del diritto pertinente dell'Unione europea, fra cui la direttiva 2013/36/UE e le ulteriori specificazioni contenute nei presenti orientamenti.

90. Nell'istituire tali politiche e nel documentare i dispositivi di governance, gli enti dovrebbero tener conto degli aspetti elencati nell'allegato I degli orientamenti. Benché le politiche e la documentazione possano essere incluse in documenti separati, gli enti dovrebbero considerare la possibilità di combinarle o di fare riferimento alle stesse in un unico documento sul quadro di governance.

8 Politica di esternalizzazione ([26])

91. L'organo di gestione dovrebbe approvare nonché riesaminare e aggiornare regolarmente la politica di esternalizzazione di un ente, garantendo che le modifiche del caso siano attuate in modo tempestivo.

92. La politica di esternalizzazione dovrebbe considerare l'impatto dell'esternalizzazione sulle attività di un ente e sui rischi ai quali l'ente è esposto (quali i rischi operativi, inclusi i rischi legali e informatici, i rischi reputazionali e i rischi di concentrazione). Tale politica dovrebbe includere i dispositivi di segnalazione e monitoraggio da attuare per tutta la durata del contratto di esternalizzazione (inclusi la redazione di una giustificazione economica dell'esternalizzazione, la stipula di un contratto di esternalizzazione, l'esecuzione del contratto fino alla sua scadenza, i piani di emergenza e le strategie di uscita). Un ente resta pienamente responsabile di tutti i servizi e di tutte le attività esternalizzati, nonché delle decisioni di gestione da questi derivanti. Ne consegue che la politica di esternalizzazione dovrebbe chiarire che l'esternalizzazione non esime l'ente dai propri obblighi di legge né dalle proprie responsabilità nei confronti dei clienti.

93. Tale politica dovrebbe indicare che il ricorso all'esternalizzazione non dovrebbe ostacolare l'efficace vigilanza ispettiva o cartolare dell'ente né essere in contrasto con le restrizioni in termini di vigilanza in relazione a servizi e attività. La politica dovrebbe coprire, inoltre, l'esternalizzazione infragruppo (ossia i servizi prestati da un'entità giuridica separata all'interno del gruppo di un ente) e prendere in considerazione eventuali circostanze specifiche del gruppo.

Titolo IV. Cultura del rischio e condotta professionale

9 Cultura del rischio

94. Una cultura del rischio sana, diligente e coerente dovrebbe essere un elemento chiave nell'efficace gestione dei rischi da parte degli enti e consentire a questi ultimi di prendere decisioni adeguate con la debita informazione.

95. Gli enti dovrebbero sviluppare una cultura del rischio integrata ed estesa a tutto l'ente, basata sulla piena comprensione e su una visione olistica dei rischi a cui sono esposti e di come tali rischi vengono gestiti, alla luce della propensione al rischio dell'ente.

96. Gli enti dovrebbero sviluppare una cultura del rischio tramite politiche, comunicazione e formazione del personale riguardo alle attività, alla strategia e al profilo di rischio dell'ente, e dovrebbero adattare la comunicazione e la formazione del personale per prendere in considerazione le responsabilità di quest'ultimo nell'assunzione e nella gestione dei rischi.

([26]) Cfr. anche gli orientamenti dell'ABE sugli accordi di esternalizzazione, disponibili all'indirizzo https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.

97. Il personale dovrebbe essere pienamente consapevole delle proprie responsabilità in merito alla gestione dei rischi. La gestione dei rischi non dovrebbe essere confinata agli esperti in materia di rischi o alle funzioni di controllo interno. Le unità operative, sotto la sorveglianza dell'organo di gestione, dovrebbero essere principalmente responsabili della gestione dei rischi su base quotidiana, in linea con le politiche, le procedure e i controlli dell'ente, tenendo in considerazione la sua propensione al rischio e la sua capacità di rischio.

98. Una forte cultura del rischio dovrebbe anche prevedere, a titolo non esaustivo, quanto segue.

    a. L'adozione di una linea dall'alto: l'organo di gestione dovrebbe essere responsabile della definizione e della comunicazione dei valori fondamentali e delle aspettative dell'ente. Il comportamento dei suoi membri dovrebbe riflettere tali valori. La dirigenza dell'ente, compreso il personale che riveste ruoli chiave, dovrebbe favorire la comunicazione interna dei valori fondamentali e delle aspettative al personale. Il personale dovrebbe agire in osservanza di tutte le leggi e i regolamenti applicabili e segnalare prontamente le situazioni non conformi osservate all'interno o all'esterno dell'ente (ad es. all'autorità competente mediante una procedura di denuncia di irregolarità). L'organo di gestione dovrebbe continuamente promuovere, monitorare e valutare la cultura del rischio dell'ente, considerare l'impatto di tale cultura sulla stabilità finanziaria, sul profilo di rischio e sulla solida governance dell'ente, nonché apportare modifiche laddove necessario.

    b. Responsabilità: il personale pertinente di ogni livello dovrebbe conoscere e comprendere i valori fondamentali dell'ente e, nella misura necessaria per il ruolo rivestito, la propensione al rischio e la capacità di rischio dell'ente. Dovrebbe essere in grado di svolgere il proprio ruolo ed essere consapevole che sarà ritenuto responsabile delle proprie azioni riguardanti il comportamento relativo all'assunzione di rischi dell'ente.

    c. Comunicazione e messa in discussione efficaci: una solida cultura del rischio dovrebbe promuovere un ambiente dove viga una comunicazione aperta e una messa in discussione efficace, in cui i processi decisionali incoraggino pareri ampiamente diversificati, consentano di testare le pratiche esistenti, stimolino un atteggiamento critico costruttivo fra il personale e promuovano un ambiente all'insegna di un impegno aperto e costruttivo nell'intera organizzazione.

    d. Incentivi: incentivi appropriati dovrebbero svolgere un ruolo chiave nell'allineamento del comportamento relativo all'assunzione di rischi con il profilo di rischio dell'ente e il suo interesse a lungo termine ([27]).

([27]) Cfr. anche gli orientamenti dell'ABE su sane politiche di remunerazione ai sensi dell'articolo 74, paragrafo 3, e dell'articolo 75, paragrafo 2, della direttiva 2013/36/UE e sull'informativa ai sensi dell'articolo 450 del regolamento (UE) n. 575/2013 (ABE/GL/2015/22), disponibili all'indirizzo https://www.eba.europa.eu/regulation-and-policy/remuneration.

10 Valori aziendali e codice di condotta

99. L'organo di gestione dovrebbe sviluppare, adottare, rispettare e promuovere elevati standard etici e professionali, prendendo in considerazione le esigenze e le caratteristiche specifiche dell'ente, e dovrebbe garantirne l'attuazione (mediante un codice di condotta o uno strumento analogo). Dovrebbe anche monitorare il rispetto di tali standard da parte del personale. Laddove applicabile, l'organo di gestione può adottare e attuare gli standard relativi al gruppo dell'ente o gli standard comuni pubblicati da associazioni o altre organizzazioni pertinenti.

100. Gli enti dovrebbero garantire che il personale non sia oggetto di discriminazioni fondate sul genere, sulla razza, sul colore, sull'origine etnica o sociale, sulle caratteristiche genetiche, sulla lingua, sulla religione o sulle credenze, sulle opinioni politiche o di altra natura, sull'appartenenza a una minoranza nazionale, sul patrimonio, sulla nascita, sulla disabilità, sull'età o sull'orientamento sessuale.

101. Le politiche dell'ente dovrebbero essere neutrali rispetto al genere. Ciò comprende, tra l'altro, la remunerazione, le politiche di assunzione, lo sviluppo della carriera e i piani di successione, l'accesso alla formazione e la possibilità di candidarsi per i posti vacanti interni. Gli enti dovrebbero garantire pari opportunità ([28]) a tutto il personale indipendentemente dal genere, anche per quanto riguarda le prospettive di carriera, e puntare a migliorare la rappresentanza del genere sottorappresentato nelle posizioni all'interno dell'organo di gestione, nonché nel gruppo del personale che ha responsabilità manageriali come definito nel regolamento delegato della Commissione (norme tecniche di regolamentazione sul personale più rilevante) ([29]). Gli enti dovrebbero monitorare separatamente l'andamento del divario retributivo di genere per il personale più rilevante (esclusi i membri dell'organo di gestione), per i membri dell'organo di gestione nella sua funzione di gestione, per i membri dell'organo di gestione nella sua funzione di supervisione e per il resto del personale. Gli enti dovrebbero avvalersi di politiche che facilitino la reintegrazione del personale dopo la maternità, la paternità o il congedo parentale.

102. Gli standard attuati dovrebbero mirare a potenziare i robusti dispositivi di governance dell'ente e a ridurre i rischi ai quali l'ente è esposto, in particolare i rischi operativi e reputazionali, che possono avere un considerevole impatto negativo sulla redditività e sostenibilità dell'ente sotto forma di ammende, spese di contenzioso, restrizioni imposte dalle autorità competenti o altre sanzioni finanziarie o penali e la perdita di valore del marchio e della fiducia dei consumatori.

([28]) Cfr. anche la direttiva 2006/54/CE del Parlamento europeo e del Consiglio, del 5 luglio 2006, riguardante l'attuazione del principio delle pari opportunità e della parità di trattamento fra uomini e donne in materia di occupazione e impiego.
([29]) Cfr. anche gli orientamenti dell'ABE sulle politiche di remunerazione neutrali rispetto al genere.

103. L'organo di gestione dovrebbe adottare politiche chiare e documentate per delineare le modalità con le quali tali standard dovrebbero essere rispettati. Tali politiche dovrebbero:

a. ricordare al personale che tutte le attività dell'ente dovrebbero essere condotte in conformità del diritto applicabile e dei valori aziendali dell'ente;

b. promuovere la consapevolezza del rischio attraverso una forte cultura del rischio, in linea con la sezione 9 degli orientamenti, trasmettendo l'aspettativa dell'organo di gestione secondo cui le attività non si spingeranno oltre la propensione al rischio e oltre i limiti definiti dall'ente e le rispettive responsabilità del personale;

c. stabilire principi e fornire esempi in merito a comportamenti accettabili o inaccettabili legati, in particolare, a informazioni inesatte o illeciti professionali in ambito finanziario, reati economici e finanziari, fra cui, ma non solo, frode, riciclaggio e finanziamento del terrorismo (ML/TF), pratiche antitrust, sanzioni finanziarie, corruzione, manipolazione di mercato, vendita di prodotti inadeguati e altre violazioni della normativa a tutela dei consumatori, illeciti fiscali, commessi direttamente o indirettamente, anche mediante sistemi di arbitraggio dei dividendi illegali o vietati;

d. chiarire che, oltre a rispettare i requisiti giuridici e regolamentari e le politiche interne, il personale è chiamato a comportarsi in modo onesto e integro e a svolgere i propri doveri con la dovuta capacità, attenzione e diligenza;

e. garantire che il personale sia consapevole delle potenziali azioni disciplinari interne ed esterne, delle azioni legali e delle sanzioni che possono seguire comportamenti scorretti o inaccettabili.

104. Gli enti dovrebbero monitorare il rispetto di tali standard e garantire la sensibilizzazione del personale, ad esempio mediante la sua formazione. Gli enti dovrebbero definire la funzione responsabile del monitoraggio della conformità al codice di condotta o a uno strumento analogo e valutarne le violazioni, nonché dotarsi di una procedura per gestire i casi di non conformità. L'organo di gestione dovrebbe essere informato periodicamente del risultato.

11 Politica in materia di conflitti di interesse a livello dell'ente

105. L'organo di gestione dovrebbe essere responsabile della definizione, dell'approvazione e della sorveglianza dell'attuazione e del mantenimento di politiche efficaci volte a individuare, valutare, gestire e mitigare o prevenire conflitti di interesse reali o potenziali a livello dell'ente, derivanti ad esempio dalle varie attività e dai vari ruoli dell'ente, dei diversi enti rientranti nell'ambito del consolidamento prudenziale o delle diverse linee di business o unità operative all'interno di un ente, o in relazione a parti interessate esterne.

106. Gli enti dovrebbero adottare, nell'ambito dei loro dispositivi organizzativi e amministrativi, misure adeguate per evitare che i conflitti di interesse incidano in modo negativo sugli interessi dei loro clienti.

107. Le misure dell'ente volte a gestire e, laddove appropriato, mitigare i conflitti di interesse dovrebbero essere documentate e includere, tra le altre cose:

a. un'adeguata separazione delle funzioni, ad esempio affidando a persone diverse le attività confliggenti nell'ambito dell'elaborazione delle operazioni o nella prestazione di servizi, oppure attribuendo a persone diverse le responsabilità di supervisione e segnalazione relativamente ad attività confliggenti;

b. l'istituzione di barriere all'informazione, ad esempio attraverso la separazione fisica di alcune linee di business o unità operative.

12 Politica in materia di conflitti di interesse per il personale ([30])

108. L'organo di gestione dovrebbe essere responsabile della definizione, dell'approvazione e della sorveglianza dell'attuazione e del mantenimento di politiche efficaci volte a individuare, valutare, gestire e mitigare o prevenire conflitti reali o potenziali tra gli interessi dell'ente e gli interessi privati del personale, inclusi i membri dell'organo di gestione, che potrebbero influire in modo negativo sull'espletamento dei loro compiti e delle loro responsabilità. Un ente consolidante dovrebbe prendere in considerazione gli interessi nell'ambito di una politica in materia di conflitti di interesse a livello di gruppo, su base consolidata o subconsolidata.

109. La politica dovrebbe mirare a individuare i conflitti di interesse del personale, inclusi gli interessi dei familiari più stretti. L'ente dovrebbe tener conto del fatto che i conflitti di interesse possono emergere non soltanto dai rapporti personali o professionali in essere, ma anche da quelli passati. Qualora emergano conflitti di interesse, gli enti dovrebbero valutare la loro rilevanza e decidere e attuare misure di mitigazione appropriate.

110. Per quanto concerne i conflitti di interesse che possono scaturire da rapporti passati, gli enti dovrebbero definire tempistiche appropriate entro cui desiderano che il personale segnali tali conflitti di interesse, sulla base del fatto che questi ultimi possono ancora ripercuotersi sul comportamento e sulla partecipazione del personale al processo decisionale.

111. La politica dovrebbe trattare quantomeno le seguenti situazioni o i seguenti rapporti in cui possono emergere conflitti di interesse:

a. interessi economici (ad es. azioni, altri diritti di proprietà e partecipazioni, posizioni finanziarie e altri interessi economici presso clienti commerciali, diritti di proprietà intellettuale, prestiti concessi dall'ente a una società di proprietà dei dipendenti, appartenenza a un organismo o proprietà di un organismo o di un'entità con interessi confliggenti);

([30]) Questa sezione dovrebbe essere letta unitamente agli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave ai sensi delle direttive 2013/36/UE e 2014/65/UE.

b. rapporti personali o professionali con i proprietari di partecipazioni qualificate nell'ente;

c. rapporti personali o professionali con il personale dell'ente o delle entità incluse nell'ambito del consolidamento prudenziale (ad es. legami di parentela);

d. un'altra occupazione o un'occupazione svolta in precedenza (ad es. negli ultimi cinque anni);

e. rapporti personali o professionali con parti interessate esterne pertinenti (ad es. associazione con fornitori, consulenti o altri prestatori di servizi sostanziali);

f. influenza politica o relazioni politiche.

112. Ciò nonostante, gli enti dovrebbero prendere in considerazione il fatto che essere un azionista di un ente o detenere conti privati o prestiti presso lo stesso o utilizzare altri suoi servizi non dovrebbe dar luogo a una situazione in cui si ritiene che il personale si trovi in conflitto di interesse se rimane entro una soglia «de minimis» appropriata.

113. La politica dovrebbe stabilire i processi di segnalazione e comunicazione alla funzione responsabile in virtù di tale politica. Il personale dovrebbe essere tenuto a divulgare internamente e tempestivamente qualunque questione che possa dar luogo o che abbia già dato luogo a un conflitto di interesse.

114. La politica dovrebbe distinguere tra i conflitti di interesse che persistono e devono essere gestiti su base permanente e i conflitti di interesse che si verificano inaspettatamente in relazione a un singolo evento (ad es. un'operazione, la selezione di un prestatore di servizi ecc.) e che possono di solito essere gestiti con una misura una tantum. In tutti i casi, l'interesse dell'ente dovrebbe essere al centro delle decisioni prese.

115. La politica dovrebbe stabilire procedure, misure, elementi in tema di documentazione e responsabilità per l'identificazione e la prevenzione di conflitti di interesse, per la valutazione della loro rilevanza e per l'adozione di misure di mitigazione. Tali procedure, elementi, responsabilità e misure dovrebbero includere le seguenti azioni:

a. affidare attività o operazioni confliggenti a persone diverse;

b. evitare che il personale che svolge anche attività esterne all'ente eserciti un'influenza indebita in seno all'ente relativamente a tali altre attività;

c. stabilire la responsabilità dei membri dell'organo di gestione di astenersi dal voto in merito a qualunque questione sulla quale un membro abbia o possa trovarsi in una situazione di conflitto di interesse o sulla quale l'obiettività del membro o la sua capacità di adempiere adeguatamente ai doveri nei confronti dell'ente possano essere in altro modo compromessi;

d. evitare che i membri dell'organo di gestione ricoprano incarichi amministrativi in enti concorrenti, salvo che questi siano all'interno di enti appartenenti allo stesso sistema di tutela istituzionale, come indicato all'articolo 113, paragrafo 7, del regolamento (UE) n. 575/2013, enti creditizi permanentemente affiliati a un organismo centrale, come indicato all'articolo 10 del regolamento (UE) n. 575/2013, o enti che rientrano nell'ambito del consolidamento prudenziale.

116. La politica dovrebbe coprire, nello specifico, il rischio di conflitti di interesse a livello dell'organo di gestione e fornire indicazioni sufficienti in merito all'individuazione e alla gestione di conflitti di interesse che possano ostacolare la capacità dei membri dell'organo di gestione di prendere decisioni obiettive e imparziali mirate a soddisfare pienamente gli interessi dell'ente. Gli enti dovrebbero prendere in considerazione il fatto che i conflitti di interesse possono avere un impatto sull'indipendenza di giudizio dei membri dell'organo di gestione ([31]).

117. Nel mitigare i conflitti di interesse individuati dei membri dell'organo di gestione, gli enti dovrebbero documentare le misure adottate, compreso il ragionamento su come queste siano efficaci per assicurare un processo decisionale obiettivo.

118. I conflitti di interesse reali o potenziali, segnalati alla funzione responsabile all'interno dell'ente, dovrebbero essere adeguatamente valutati e gestiti. Qualora sia individuato un conflitto di interesse del personale, l'ente dovrebbe documentare la decisione presa, in particolare se il conflitto di interesse e i relativi rischi sono stati accettati e, in tal caso, in che modo tale conflitto sia stato mitigato o risolto in modo soddisfacente.

119. Tutti i conflitti di interesse reali e potenziali a livello dell'organo di gestione, individualmente e collettivamente, dovrebbero essere documentati in modo adeguato, comunicati all'organo di gestione e formare l'oggetto di discussioni e decisioni ed essere gestiti debitamente dall'organo di gestione.

12.1 Politica in materia di conflitti di interesse nel contesto di prestiti e altre operazioni con i membri dell'organo di gestione e le loro parti correlate

120. Nell'ambito delle loro politiche in materia di conflitti di interesse per il personale (sezione 12) e della gestione dei conflitti di interesse dei membri dell'organo di gestione di cui al paragrafo 117, l'organo di gestione dovrebbe definire un quadro per identificare e gestire i conflitti di interesse nel contesto della concessione di prestiti e della conclusione di altre operazioni (ad es. factoring, leasing, operazioni immobiliari, ecc.) con membri dell'organo di gestione e le loro parti correlate.

([31]) Cfr. anche gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo di gestione e del personale che riveste ruoli chiave ai sensi delle direttive 2013/36/UE e 2014/65/UE.

121. Fatto salvo il recepimento nella legislazione nazionale della direttiva 2013/36/UE ([32]), gli enti possono considerare ulteriori categorie di parti correlate alle quali applicare, in tutto o in parte, il loro quadro relativo ai conflitti di interesse per quanto riguarda i prestiti e altre operazioni.

122. Il quadro relativo ai conflitti di interesse dovrebbe garantire che le decisioni riguardanti la concessione di prestiti e la conclusione di altre operazioni con i membri dell'organo di gestione e le loro parti correlate siano prese in modo obiettivo, senza l'indebita influenza di conflitti di interesse, e che tali operazioni siano, come principio generale, condotte a condizioni di mercato.

123. L'organo di gestione dovrebbe stabilire i processi decisionali applicabili per la concessione di prestiti e la conclusione di altre operazioni con i membri dell'organo di gestione e le loro parti correlate. Questo quadro può prevedere una differenziazione tra le operazioni commerciali standard ([33]) effettuate nel corso ordinario degli affari e concluse a normali condizioni di mercato, e i prestiti e le operazioni riguardanti il personale, che sono conclusi a condizioni disponibili per tutto il personale. Inoltre, il quadro relativo ai conflitti di interesse e il processo decisionale possono operare una distinzione tra prestiti e altre operazioni sostanziali e non sostanziali, tra diversi tipi di prestiti e altre operazioni e tra il livello dei conflitti di interesse reali o potenziali che possono generare.

124. Nell'ambito del quadro relativo ai conflitti di interesse, l'organo di gestione dovrebbe stabilire soglie appropriate (ad es. per tipo di prodotto, o a seconda delle condizioni) oltre le quali il prestito o un'altra operazione con un membro dell'organo di gestione o le sue parti correlate richiede sempre l'approvazione dell'organo di gestione. Le decisioni relative a prestiti o altre operazioni sostanziali con i membri dell'organo di gestione che non vengono concluse alle normali condizioni di mercato, ma a condizioni disponibili per tutto il personale, dovrebbero sempre essere prese dall'organo di gestione.

125. Il membro dell'organo di gestione che beneficia di tale prestito o altra operazione sostanziale o il membro che è correlato alla controparte non dovrebbe essere coinvolto nel processo decisionale.

126. Prima di prendere una decisione in merito a un prestito o ad un'altra operazione con un membro dell'organo di gestione o le sue parti correlate, gli enti dovrebbero valutare il rischio al quale potrebbero essere esposti a seguito dell'operazione.

127. Qualora i prestiti siano concessi sotto forma di linea di credito (ad es. scoperti), la decisione iniziale e le sue modifiche dovrebbero essere documentate. Qualsiasi uso di tali facilitazioni di credito concordate entro i limiti stabiliti non dovrebbe essere considerato alla stregua di una nuova decisione su un prestito a un membro dell'organo di gestione o a una sua parte

([32]) Cfr. anche il principio fondamentale 20 di Basilea.
([33]) Le operazioni commerciali comprendono prestiti e altre operazioni (ad es. leasing, factoring, servizi nel contesto di offerte pubbliche iniziali, fusioni e acquisizioni, compravendita di immobili).

correlata. Laddove la modifica di una linea di credito sia considerata sostanziale in linea con la politica dell'ente, si dovrebbe procedere a una nuova valutazione e decisione.

128. Per assicurare la conformità con le loro politiche in materia di conflitti di interesse, gli enti dovrebbero garantire che ai prestiti e alle altre operazioni con i membri dell'organo di gestione o le loro parti correlate si applichino pienamente tutte le procedure di controllo interno pertinenti e che a livello dell'organo di gestione nella sua funzione di supervisione strategica sia in atto un quadro di sorveglianza adeguato.

12.2 Documentazione dei prestiti ai membri dell'organo di gestione e alle loro parti correlate e informazioni supplementari

129. Ai fini dell'articolo 88, paragrafo 1, della direttiva 2013/36/UE, gli enti dovrebbero documentare correttamente i dati relativi ai prestiti ([34]) concessi ai membri dell'organo di gestione e alle loro parti correlate, includendo almeno:

a. il nome del debitore e il suo status (ovvero membro dell'organo di gestione o parte correlata) e, per quanto riguarda i prestiti a una parte correlata, il membro dell'organo di gestione al quale la parte è correlata e la natura del rapporto con la parte correlata;

b. il tipo/natura del prestito e l'importo;

c. le condizioni applicabili al prestito;

d. la data di approvazione del prestito;

e. il nome della persona o dell'organo (compresa la sua composizione) che prende la decisione di approvare il prestito e le condizioni applicabili;

f. il fatto (sì/no) che il prestito sia stato concesso o meno a condizioni di mercato;

g. il fatto (sì/no) che il prestito sia stato concesso o meno a condizioni disponibili per tutto il personale.

130. Gli enti dovrebbero garantire che la documentazione di tutti i prestiti concessi ai membri dell'organo di gestione e alle loro parti correlate sia completa e aggiornata e che l'ente sia in grado di mettere a disposizione delle autorità competenti la documentazione completa in un formato opportuno su richiesta e senza indebito ritardo.

([34]) Cfr. anche gli orientamenti dell'ABE in materia di concessione e monitoraggio dei prestiti, disponibili all'indirizzo https://eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring

131. Nel caso di un prestito di importo superiore a 200 000 EUR concesso a un membro dell'organo di gestione o alle sue parti correlate, gli enti dovrebbero essere in grado di fornire all'autorità competente, su richiesta, le seguenti informazioni supplementari:

a. la percentuale del prestito e la percentuale della somma di tutti gli importi in essere dei prestiti concessi allo stesso debitore rispetto a:

i. la somma del suo capitale di classe 1 e del suo capitale di classe 2,

ii. il capitale primario di classe 1 dell'ente;

b. se il prestito fa parte di una grande esposizione ([35]);

c. il peso relativo della somma aggregata degli importi in essere di tutti i prestiti concessi allo stesso debitore, calcolato in percentuale dividendo l'importo totale in essere per l'importo totale di tutti i prestiti in essere concessi a membri dell'organo di gestione e loro parti correlate.

13 Procedure interne di segnalazione

132. Gli enti dovrebbero adottare e mantenere adeguate politiche e procedure interne di segnalazione rivolte al personale, allo scopo di comunicare violazioni reali o potenziali dei requisiti normativi o interni, compresi, tra l'altro, quelli stabiliti nel regolamento (UE) n. 575/2013 e nelle disposizioni nazionali che recepiscono la direttiva 2013/36/UE, oppure nei dispositivi di governance interna, avvalendosi di uno specifico canale indipendente e autonomo. Il personale segnalante non è tenuto a dimostrare la violazione; tuttavia, dovrebbe possedere un livello di certezza tale da fornire un motivo sufficiente per aprire un'indagine. Gli enti dovrebbero inoltre attuare processi e procedure adeguati che garantiscano il rispetto degli obblighi derivanti dal recepimento nella legislazione nazionale della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

133. Al fine di evitare conflitti di interesse, il personale dovrebbe poter segnalare violazioni al di fuori delle tradizionali linee di segnalazione (ad es. per il tramite della funzione di conformità o della funzione di audit interno o mediante una procedura interna di denuncia di irregolarità). Le procedure di segnalazione dovrebbero garantire la protezione dei dati personali sia della persona fisica che segnala la violazione sia della persona fisica sospettata di essere responsabile della violazione, in conformità del regolamento (UE) 2016/679 ([36]) o regolamento generale sulla protezione dei dati.

134. Le procedure di segnalazione dovrebbero essere accessibili a tutto il personale dell'ente.

([35]) Cfr. anche la parte IV del regolamento (UE) n. 575/2013, in particolare l'articolo 392.
([36]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

135. Le informazioni fornite dal personale mediante le procedure di segnalazione dovrebbero, se del caso, essere messe a disposizione dell'organo di gestione e di altre funzioni responsabili definite nella politica interna di segnalazione. Laddove richiesto dal personale che segnala la violazione, le informazioni dovrebbero essere fornite all'organo di gestione e ad altre funzioni responsabili in forma anonima. Gli enti possono anche prevedere una procedura di denuncia di irregolarità che consenta di trasmettere le informazioni in forma anonima.

136. Gli enti dovrebbero garantire che la persona che segnala la violazione sia adeguatamente protetta da eventuali ripercussioni negative, come ritorsioni, discriminazioni o altri tipi di trattamento iniquo. L'ente dovrebbe garantire che nessuna persona sotto il suo controllo operi atti di vittimizzazione nei confronti di una persona che ha segnalato una violazione e dovrebbe adottare misure appropriate contro i responsabili di tali atti.

137. Gli enti dovrebbero inoltre proteggere da eventuali ripercussioni negative le persone segnalate nel caso in cui dall'indagine non emergano prove che giustifichino l'adozione di provvedimenti nei loro confronti. Qualora siano adottate misure, l'ente dovrebbe farlo in modo da mirare a proteggere la persona in questione da effetti negativi involontari che vadano oltre l'obiettivo dei provvedimenti adottati.

138. In particolare, le procedure interne di segnalazione dovrebbero:

a. essere documentate (ad es. nel manuale del personale);

b. fornire regole chiare atte a garantire che le informazioni sulla segnalazione e sulle persone segnalate e sulla violazione siano trattate in modo riservato, in conformità del regolamento (UE) 2016/679, salvo che tale comunicazione sia richiesta dalla normativa nazionale nel contesto di ulteriori indagini o di successivi procedimenti giudiziari;

c. proteggere la persona che esprime il timore di divenire oggetto di atti di vittimizzazione per aver comunicato violazioni soggette a segnalazione;

d. garantire che le violazioni potenziali o reali notificate siano valutate e segnalate anche, se del caso, all'autorità competente o all'organismo deputato all'applicazione della legge;

e. garantire, laddove possibile, che sia fornita conferma della ricezione delle informazioni al personale che ha notificato violazioni potenziali o reali;

f. garantire il monitoraggio dell'esito dell'indagine sulla violazione segnalata;

g. garantire la tenuta di un apposito registro.

14 Segnalazione delle violazioni alle autorità competenti

139. Le autorità competenti dovrebbero stabilire meccanismi efficaci e affidabili per permettere al personale degli enti di segnalare alle autorità competenti violazioni reali o potenziali dei requisiti normativi, compresi, tra l'altro, quelli stabiliti nel regolamento (UE) n. 575/2013 e nelle disposizioni nazionali che recepiscono la direttiva 2013/36/UE. Tali meccanismi dovrebbero includere quantomeno:

a. procedure specifiche per la ricezione delle segnalazioni sulle violazioni e per le attività di follow-up, come ad esempio un dipartimento, un'unità o una funzione preposti alle denunce di irregolarità;

b. un'idonea protezione, come indicato alla sezione 13;

c. la protezione dei dati personali sia della persona fisica che segnala la violazione sia della persona fisica sospettata di essere responsabile della violazione, in conformità del regolamento 2016/679;

d. procedure chiare, come definite alla sezione 13.

140. Fatta salva la possibilità di segnalare violazioni mediante i meccanismi delle autorità competenti, queste ultime possono incoraggiare il personale a tentare di utilizzare, innanzitutto, le procedure interne di segnalazione istituite dall'ente.

Titolo V. Quadro e meccanismi di controllo interno

15 Quadro di controllo interno

141. Gli enti dovrebbero sviluppare e mantenere una cultura che incoraggi un atteggiamento positivo nei confronti del controllo dei rischi e della conformità all'interno dell'ente, nonché un quadro di controllo interno solido e completo. Sulla base di tale quadro, le linee di business degli enti dovrebbero essere responsabili della gestione dei rischi nei quali incorrono durante l'esercizio delle loro attività e disporre di controlli volti a garantire la conformità con i requisiti interni ed esterni. In tale ambito, gli enti dovrebbero disporre di funzioni di controllo interno dotate di autorità, peso e accesso all'organo di gestione che siano idonei e sufficienti per adempiere alla loro missione, nonché di un quadro di gestione dei rischi.

142. Il quadro di controllo interno dell'ente dovrebbe essere adattato, su base individuale, alla specificità della sua attività, alla sua complessità e ai rischi associati, tenendo conto del contesto del gruppo. Gli enti dovrebbero organizzare lo scambio delle informazioni necessarie in modo da garantire che ogni organo di gestione, linea di business e unità interna, inclusa ciascuna funzione di controllo interno, sia in grado di svolgere i propri compiti. Ciò significa, ad esempio, porre in essere uno scambio necessario di informazioni adeguate tra le linee di business e la funzione di conformità e la funzione di conformità ai requisiti in materia di

contrasto al riciclaggio e al finanziamento del terrorismo, laddove questa sia una funzione separata, a livello di gruppo e tra i responsabili delle funzioni di controllo interno a livello di gruppo e di organo di gestione dell'ente.

143. Gli enti dovrebbero attuare processi e procedure adeguati che garantiscano il rispetto dei loro obblighi nel contesto della lotta al riciclaggio e al finanziamento del terrorismo. Gli enti dovrebbero valutare la loro esposizione al rischio di essere utilizzati a scopo di riciclaggio e finanziamento del terrorismo e, se necessario, adottare misure di mitigazione volte a ridurre tali rischi, nonché i rischi operativi e reputazionali a questi collegati. Gli enti dovrebbero prendere misure per garantire che il loro personale sia consapevole dei rischi di riciclaggio e di finanziamento del terrorismo e degli effetti del riciclaggio e del finanziamento del terrorismo sull'ente e sull'integrità del sistema finanziario.

144. Il quadro di controllo interno dovrebbe coprire l'intera organizzazione, incluse le responsabilità e i compiti dell'organo di gestione e le attività di tutte le linee di business e delle unità interne, fra cui le funzioni di controllo interno, le attività esternalizzate e i canali di distribuzione.

145. Il quadro di controllo interno di un ente dovrebbe garantire:

a. operazioni efficaci ed efficienti;

b. norme di comportamento prudenti;

c. opportuna individuazione, valutazione e mitigazione dei rischi;

d. affidabilità di informazioni finanziarie e non finanziarie segnalate sia internamente che esternamente;

e. sane procedure amministrative e contabili;

f. conformità a leggi, regolamenti, obblighi di vigilanza e alle politiche, ai processi, alle norme e alle decisioni interni dell'ente.

16 Attuazione di un quadro di controllo interno

146. L'organo di gestione dovrebbe essere responsabile della definizione e del monitoraggio dell'adeguatezza e dell'efficacia dei processi, dei meccanismi e del quadro di controllo interno, nonché della sorveglianza di tutte le linee di business e unità interne, incluse le funzioni di controllo interno (quali le funzioni di gestione dei rischi, di conformità, di conformità ai requisiti in materia di contrasto al riciclaggio e al finanziamento del terrorismo laddove separata dalla funzione di conformità nonché di audit interno). Gli enti dovrebbero stabilire, mantenere e aggiornare periodicamente e per iscritto politiche, meccanismi e

procedure di controllo interno adeguati, che dovrebbero essere approvati dall'organo di gestione.

147. Un ente dovrebbe disporre di un processo decisionale chiaro, trasparente e documentato e di una chiara ripartizione delle responsabilità e dell'autorità all'interno del suo quadro di controllo interno, incluse le sue linee di business, le unità interne e le funzioni di controllo interno.

148. Gli enti dovrebbero comunicare tali politiche, meccanismi e procedure a tutto il personale e ogniqualvolta vengano apportate modifiche sostanziali.

149. Nell'attuare il quadro di controllo interno, gli enti dovrebbero stabilire un'adeguata separazione delle funzioni (ad es. affidando a persone diverse le attività confliggenti nell'ambito dell'elaborazione delle operazioni o nella prestazione di servizi, oppure attribuendo a persone diverse le responsabilità di supervisione e di segnalazione relativamente ad attività confliggenti) e istituire barriere all'informazione, ad esempio attraverso la separazione fisica di taluni dipartimenti.

150. Le funzioni di controllo interno dovrebbero verificare che le politiche, i meccanismi e le procedure stabiliti nel quadro di controllo interno siano attuati correttamente nelle rispettive aree di competenza.

151. Le funzioni di controllo interno dovrebbero sottoporre regolarmente all'organo di gestione relazioni scritte sulle principali carenze individuate. Queste relazioni dovrebbero includere, per ciascuna nuova importante carenza individuata, i relativi rischi connessi, una valutazione d'impatto, le raccomandazioni e le misure correttive da adottare. L'organo di gestione dovrebbe dare seguito tempestivamente ed efficacemente alle risultanze evidenziate dalle funzioni di controllo interno e richiedere misure correttive adeguate. Dovrebbe essere messa in atto una procedura formale di follow-up sui risultati rilevati e sulle misure correttive adottate.

17 Quadro di gestione dei rischi

152. Nell'ambito del quadro generale di controllo interno, gli enti dovrebbero disporre di un quadro olistico di gestione dei rischi a livello dell'intero ente, che si estenda a tutte le linee di business e unità interne, comprese le funzioni di controllo interno, riconoscendo pienamente la sostanza economica di tutte le sue esposizioni al rischio. La gestione dei rischi dovrebbe consentire all'ente di prendere decisioni sull'assunzione di rischi in maniera pienamente consapevole. Il quadro di gestione dei rischi dovrebbe includere i rischi in bilancio e fuori bilancio, nonché i rischi correnti e quelli futuri ai quali l'ente può essere esposto. I rischi dovrebbero essere valutati a partire dal basso e a partire dall'alto, all'interno e attraverso le linee di business, utilizzando una terminologia coerente e metodologie compatibili nell'intero ente e a un livello consolidato e subconsolidato. Tutti i rischi pertinenti dovrebbero essere inseriti nel quadro di gestione dei rischi con l'appropriata valutazione dei rischi sia finanziari

sia non finanziari, compresi i rischi di credito, di mercato, di liquidità, di concentrazione, operativi, informatici, reputazionali, legali, di condotta, di conformità riguardante il riciclaggio e il finanziamento del terrorismo e altri reati finanziari, rischi ambientali, sociali e di governance e rischi strategici.

153. Il quadro di gestione dei rischi di un ente dovrebbe prevedere politiche, procedure, limiti di rischio e controlli dei rischi che garantiscano l'individuazione, la misurazione o la valutazione, il monitoraggio, la gestione, la mitigazione e la segnalazione dei rischi, in maniera adeguata, tempestiva e continua, a livello delle linee di business e dell'ente e a livello consolidato e subconsolidato.

154. Il quadro di gestione dei rischi di un ente dovrebbe fornire indicazioni specifiche sull'attuazione delle strategie dell'ente. Tali indicazioni dovrebbero, eventualmente, stabilire e mantenere limiti interni coerenti con la propensione al rischio dell'ente e commisurati al sano funzionamento, alla solidità finanziaria, alla base di capitale e agli obiettivi strategici dello stesso. Il profilo di rischio dell'ente dovrebbe essere mantenuto entro tali limiti stabiliti. Il quadro di gestione dei rischi dovrebbe garantire che, laddove si verifichino violazioni dei limiti di rischio, vi sia un processo definito per segnalarle e gestirle con un'apposita procedura di follow-up.

155. Il quadro di gestione dei rischi dovrebbe essere sottoposto a una revisione interna indipendente, svolta ad esempio dalla funzione di audit interno, e rivalutato regolarmente sulla base della propensione al rischio dell'ente, tenendo conto delle informazioni fornite dalla funzione di gestione dei rischi e, laddove istituito, dal comitato dei rischi. Fra i fattori da considerare vi sono gli sviluppi interni ed esterni, come le variazioni di bilancio e delle entrate; l'eventuale maggiore complessità delle attività dell'ente, del profilo di rischio o della struttura operativa; l'espansione geografica; le fusioni e le acquisizioni; e l'introduzione di nuovi prodotti o di nuove linee di business.

156. Nell'individuazione e nella misurazione o valutazione dei rischi, un ente dovrebbe sviluppare metodologie idonee, inclusi strumenti prospettici e retrospettivi. Le metodologie dovrebbero consentire l'aggregazione delle esposizioni al rischio attraverso le linee di business e facilitare l'individuazione delle concentrazioni dei rischi. Gli strumenti dovrebbero includere la valutazione dell'effettivo profilo di rischio a fronte della propensione al rischio dell'ente, nonché l'individuazione e la valutazione di esposizioni al rischio potenziali e in condizioni di stress, sulla base di una serie di presunte circostanze avverse rispetto alla capacità di rischio dell'ente. Gli strumenti dovrebbero fornire informazioni su eventuali necessità di adattare il profilo di rischio. Gli enti dovrebbero formulare ipotesi adeguatamente prudenti nel delineare scenari di stress.

157. Gli enti dovrebbero tenere conto del fatto che i risultati delle metodologie delle valutazioni quantitative, comprese le prove di stress, dipendono in larga misura dalle limitazioni e dalle ipotesi dei modelli (fra cui l'entità e la durata dello shock e i rischi sottostanti). Ad esempio, il fatto che i modelli mostrino rendimenti molto elevati sul capitale economico potrebbe

derivare da una debolezza nei modelli stessi (ad es. l'esclusione di alcuni rischi pertinenti) anziché da una migliore strategia o dall'ottimale esecuzione di una strategia da parte dell'ente. Pertanto, la determinazione del livello di rischio assunto non dovrebbe basarsi soltanto sulle informazioni quantitative o sui risultati dei modelli, ma dovrebbe anche includere un approccio qualitativo (fra cui un parere di esperti e un'analisi critica). Dovrebbero essere esplicitamente esaminati gli andamenti e i dati rilevanti del contesto macroeconomico al fine di individuare il loro possibile impatto su esposizioni e portafogli.

158. La responsabilità finale della valutazione dei rischi spetta unicamente all'ente, che dovrebbe di conseguenza valutare con spirito critico i propri rischi e non dovrebbe fare affidamento esclusivamente su valutazioni esterne. Ad esempio, un ente dovrebbe convalidare un modello di rischio acquistato e adeguarlo alle proprie circostanze per garantire che il rischio sia individuato e analizzato in modo preciso ed esaustivo.

159. Gli enti dovrebbero essere pienamente consapevoli dei limiti dei modelli e delle metriche e utilizzare strumenti di valutazione non soltanto quantitativa, ma anche qualitativa dei rischi (fra cui un parere di esperti e un'analisi critica).

160. Oltre alle proprie valutazioni, gli enti possono ricorrere a valutazioni esterne dei rischi (inclusi rating del credito esterni o modelli di rischio acquistati esternamente). Gli enti dovrebbero essere pienamente consapevoli della portata esatta di tali valutazioni e dei loro limiti.

161. Dovrebbero essere istituiti meccanismi di segnalazione periodici e trasparenti, affinché l'organo di gestione, il suo comitato dei rischi, laddove istituito, e tutte le unità pertinenti di un ente ricevano le informazioni in maniera tempestiva, precisa, sintetica, comprensibile e significativa, e possano condividere le informazioni pertinenti in materia di individuazione, misurazione o valutazione, monitoraggio e gestione dei rischi. Il quadro di segnalazione dovrebbe essere ben definito e documentato.

162. L'efficace comunicazione e sensibilizzazione in merito ai rischi e alla strategia in materia di rischio è fondamentale per l'intero processo di gestione dei rischi, inclusi i processi di revisione e quelli decisionali, e contribuisce a impedire la presa di decisioni che potrebbero involontariamente aumentare il rischio. L'efficace segnalazione dei rischi implica la sana valutazione e comunicazione interna della strategia in materia di rischio e dei dati relativi ai rischi (ad es. le esposizioni e i principali indicatori di rischio) sia trasversalmente all'interno dell'ente sia verticalmente nei processi di gestione.

18 Nuovi prodotti e modifiche sostanziali ([37])

163. Gli enti dovrebbero disporre di una politica aziendale ben documentata per l'approvazione di nuovi prodotti, che sia approvata dall'organo di gestione e affronti lo sviluppo di nuovi

([37]) Cfr. anche gli orientamenti dell'ABE sui dispositivi di governance e di controllo sui prodotti bancari al dettaglio, disponibili all'indirizzo https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

mercati, prodotti e servizi e le modifiche sostanziali di quelli esistenti, nonché le operazioni straordinarie. La politica dovrebbe, inoltre, includere le modifiche sostanziali apportate ai relativi processi (ad es. nuovi accordi di esternalizzazione) e sistemi (ad es. i processi di cambiamento in ambito informatico). La politica aziendale per l'approvazione di nuovi prodotti dovrebbe garantire che i prodotti e le modifiche approvati siano compatibili con la strategia in materia di rischio e la propensione al rischio dell'ente nonché con i limiti corrispondenti dell'ente stesso, o che vengano effettuate le necessarie revisioni.

164. Le modifiche sostanziali o le operazioni straordinarie possono comprendere fusioni e acquisizioni, fra cui le potenziali conseguenze di una due diligence insufficiente che non riesca a individuare i rischi e le passività successivamente alla fusione; la creazione di strutture (ad es. nuove filiazioni o società veicolo); nuovi prodotti; modifiche ai sistemi o al quadro o alle procedure di gestione dei rischi; e cambiamenti intervenuti nell'organizzazione dell'ente.

165. Un ente dovrebbe disporre di procedure specifiche per valutare la conformità a tali politiche, tenendo conto del contributo della funzione di gestione dei rischi. Ciò dovrebbe includere una valutazione preventiva sistematica e un parere documentato da parte della funzione di conformità per i nuovi prodotti o per le modifiche sostanziali ai prodotti esistenti.

166. La politica aziendale per l'approvazione di nuovi prodotti di un ente dovrebbe riguardare tutti gli elementi da prendere in considerazione prima di decidere di entrare in nuovi mercati, trattare nuovi prodotti, lanciare un nuovo servizio o apportare modifiche sostanziali a prodotti o servizi esistenti. La politica aziendale per l'approvazione di nuovi prodotti dovrebbe inoltre includere le definizioni di «nuovo prodotto/mercato/attività» e «modifiche sostanziali» da utilizzare nell'organizzazione e indicare le funzioni interne da coinvolgere nel processo decisionale.

167. La politica aziendale per l'approvazione di nuovi prodotti dovrebbe indicare le principali questioni da trattare prima dell'adozione di una decisione. Tali questioni dovrebbero includere il rispetto della normativa, la contabilità, i modelli di determinazione del prezzo, l'impatto sul profilo di rischio, sull'adeguatezza patrimoniale e sulla redditività, la disponibilità di risorse adeguate per le attività di «front office», «back office» e «middle office» nonché la disponibilità di strumenti interni e competenze adeguate per la comprensione e il monitoraggio dei rischi associati. Inoltre, nel rispetto degli obblighi previsti dalla direttiva (UE) 2015/849, gli enti dovrebbero identificare e valutare il rischio di riciclaggio e di finanziamento del terrorismo associato al nuovo prodotto o alla nuova pratica commerciale, e stabilire le misure da adottare per mitigare tali rischi. 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 associati.

168. La funzione di gestione dei rischi e la funzione di conformità dovrebbero partecipare all'approvazione dei nuovi prodotti o delle modifiche sostanziali ai prodotti, processi e sistemi esistenti. Il loro contributo dovrebbe prevedere una valutazione esaustiva e oggettiva dei

rischi derivanti da nuove attività in diversi scenari, delle potenziali carenze nei quadri di gestione dei rischi e di controllo interno dell'ente, e della capacità dell'ente di gestire efficacemente eventuali nuovi rischi. La funzione di gestione dei rischi dovrebbe avere anche una chiara visione d'insieme del processo di introduzione di nuovi prodotti (o delle modifiche sostanziali apportate ai prodotti, processi e sistemi 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.

19 Funzioni di controllo interno

169. Le funzioni di controllo interno dovrebbero includere una funzione di gestione dei rischi (cfr. sezione 20), una funzione di conformità (cfr. sezione 21) e una funzione di audit interno (cfr. sezione 22). Le funzioni di gestione dei rischi e di conformità dovrebbero essere soggette a revisione da parte della funzione di audit interno. Le responsabilità delle funzioni di controllo includono anche quella di assicurare la conformità ai requisiti in materia di contrasto al riciclaggio e al finanziamento del terrorismo.

170. Le attività operative delle funzioni di controllo interno possono essere esternalizzate, tenendo conto dei criteri di proporzionalità elencati nel titolo I, all'ente consolidante o a un'altra entità, all'interno o all'esterno del gruppo, con l'assenso degli organi di gestione degli enti interessati. Anche quando le attività operative di controllo interno sono esternalizzate in tutto o in parte, il responsabile della funzione di controllo interno interessata e l'organo di gestione rimangono responsabili di tali attività e del mantenimento di una funzione di controllo interno nell'ente.

171. Fatta salva la legislazione nazionale che recepisce la direttiva 2015/849/UE, gli enti dovrebbero assegnare la responsabilità di garantire la conformità dell'ente ai requisiti di tale direttiva e alle politiche e procedure dell'ente a un membro del personale (ad es. il responsabile della conformità). Gli enti possono istituire una separata funzione di conformità ai requisiti in materia di contrasto al riciclaggio e al finanziamento del terrorismo come funzione di controllo indipendente ([38]). La persona responsabile della conformità ai requisiti in materia di contrasto al riciclaggio e al finanziamento del terrorismo dovrebbe, se necessario, essere in grado di riferire direttamente all'organo di gestione nelle sue funzioni di gestione e di supervisione strategica.

19.1 Responsabili delle funzioni di controllo interno

172. I responsabili delle funzioni di controllo interno dovrebbero essere stabiliti a un livello gerarchico adeguato che fornisca al responsabile della funzione di controllo l'autorità appropriata e il peso necessario per adempiere alle proprie responsabilità. Fatta salva la responsabilità generale dell'organo di gestione, i responsabili delle funzioni di controllo interno dovrebbero essere indipendenti dalle linee di business o dalle unità soggette al loro

([38]) Cfr. anche gli orientamenti dell'ABE sulla funzione di conformità ai requisiti in materia di contrasto al riciclaggio e al finanziamento del terrorismo (attualmente in fase di elaborazione).

controllo. A tal fine, i responsabili delle funzioni di gestione dei rischi, di conformità e di audit interno dovrebbero riferire e rispondere direttamente all'organo di gestione, che dovrebbe esaminarne le prestazioni.

173. Laddove necessario, i responsabili delle funzioni di controllo interno dovrebbero poter accedere e riferire direttamente all'organo di gestione nella sua funzione di supervisione strategica, al fine di sollevare dubbi e avvisare la funzione di supervisione strategica, laddove opportuno, in merito a sviluppi specifici che interessano o possano interessare l'ente. Ciò non dovrebbe impedire ai responsabili delle funzioni di controllo di trasmettere informazioni anche all'interno delle normali linee di segnalazione.

174. Gli enti dovrebbero disporre di processi documentati per assegnare la posizione di responsabile di una funzione di controllo interno e per revocarne le responsabilità. In ogni caso, i responsabili delle funzioni di controllo interno non dovrebbero essere rimossi (e, in conformità dell'articolo 76, paragrafo 5, della direttiva 2013/36/UE, il responsabile della funzione di gestione dei rischi non può essere rimosso) senza la previa approvazione dell'organo di gestione nella sua funzione di supervisione strategica. Negli enti significativi, le autorità competenti dovrebbero essere prontamente informate dell'approvazione e dei principali motivi della rimozione del responsabile di una funzione di controllo interno.

19.2 Indipendenza delle funzioni di controllo interno

175. Al fine di garantire l'indipendenza delle funzioni di controllo interno, dovrebbero essere soddisfatte le seguenti condizioni:

a. il loro personale non svolge compiti operativi che rientrano nell'ambito delle attività che le funzioni di controllo interno sono tenute a monitorare e controllare;

b. dal punto di vista organizzativo, tali funzioni sono separate dalle attività che sono tenute a monitorare e controllare;

c. fatta salva la responsabilità generale dei membri dell'organo di gestione per l'ente, il responsabile di una funzione di controllo interno non dovrebbe essere subordinato a una persona responsabile di gestire le attività che la funzione di controllo interno monitora e controlla;

d. la remunerazione del personale adibito alla funzione di controllo interno non dovrebbe essere legata ai risultati delle attività che la funzione di controllo interno monitora e controlla, né ad altro che ne comprometta l'obiettività ([39]).

([39]) Cfr. anche gli orientamenti dell'ABE su sane politiche di remunerazione, disponibili all'indirizzo https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

19.3 Combinazione delle funzioni di controllo interno

176. Tenendo conto dei criteri di proporzionalità di cui al titolo I, la funzione di gestione dei rischi e la funzione di conformità possono essere combinate. La funzione di audit interno non dovrebbe essere combinata con un'altra funzione di controllo interno.

19.4 Risorse delle funzioni di controllo interno

177. Le funzioni di controllo interno dovrebbero disporre di risorse sufficienti, in particolare di personale qualificato in numero adeguato (a livello sia di impresa madre sia di filiazioni). Il personale dovrebbe mantenere costantemente aggiornate le proprie qualifiche e ricevere la formazione necessaria.

178. Le funzioni di controllo interno dovrebbero disporre di sistemi informatici e di supporto adeguati, con accesso alle informazioni interne ed esterne necessarie per adempiere le proprie responsabilità. Tali funzioni dovrebbero avere accesso a tutte le informazioni necessarie relative alle linee di business e alle pertinenti filiazioni soggette a rischi, in particolare a quelle che possono potenzialmente generare rischi sostanziali per gli enti.

20 Funzione di gestione dei rischi

179. Gli enti dovrebbero istituire una funzione di gestione dei rischi che si occupi dell'intero ente. La funzione di gestione dei rischi dovrebbe disporre di autorità, peso e risorse in misura sufficiente, tenendo conto dei criteri di proporzionalità di cui al titolo I, per attuare politiche in materia di rischi e il quadro di gestione dei rischi, come stabilito alla sezione 17.

180. La funzione di gestione dei rischi dovrebbe disporre, se necessario, di accesso diretto all'organo di gestione nella sua funzione di supervisione strategica e ai relativi comitati, laddove istituiti, incluso in particolare il comitato dei rischi.

181. La funzione di gestione dei rischi dovrebbe avere accesso a tutte le linee di business e ad altre unità interne che hanno il potenziale di generare rischi, nonché a tutte le relative filiazioni e affiliate.

182. Il personale della funzione di gestione dei rischi dovrebbe possedere conoscenze, competenze ed esperienza sufficienti riguardo alle tecniche e alle procedure di gestione dei rischi, nonché ai mercati e ai prodotti, e dovrebbe avere accesso a una formazione regolare.

183. La funzione di gestione dei rischi dovrebbe essere indipendente dalle linee e unità di business di cui controlla i rischi, ma non le dovrebbe essere impedito di interagire con esse. L'interazione tra le funzioni operative e la funzione di gestione dei rischi dovrebbe conseguire l'obiettivo di responsabilizzare tutto il personale dell'ente rispetto alla gestione dei rischi.

184. La funzione di gestione dei rischi dovrebbe essere un elemento organizzativo centrale dell'ente, strutturato in modo tale da poter attuare politiche in materia di rischi e controllare

il quadro di gestione dei rischi. La funzione di gestione dei rischi dovrebbe svolgere un ruolo fondamentale nel garantire che l'ente disponga di efficaci processi di gestione dei rischi. La funzione di gestione dei rischi dovrebbe partecipare attivamente a tutte le decisioni di gestione dei rischi sostanziali.

185. Gli enti significativi possono prevedere l'istituzione di funzioni di gestione dei rischi dedicate per ciascuna linea di business rilevante. Tuttavia, dovrebbe esserci una funzione di gestione dei rischi centrale, che includa una funzione di gestione dei rischi a livello di gruppo nell'ente consolidante, per assicurare una visione olistica in merito a tutti i rischi a livello di ente e di gruppo e per garantire che venga rispettata la strategia in materia di rischio.

186. La funzione di gestione dei rischi dovrebbe fornire informazioni, analisi e pareri di esperti sull'esposizione ai rischi che siano pertinenti e indipendenti, e consulenza su proposte e decisioni in materia di rischi adottate dalle linee di business o dalle unità interne; dovrebbe inoltre segnalare all'organo di gestione se queste siano conformi alla strategia in materia di rischio e alla propensione al rischio dell'ente. La funzione di gestione dei rischi può raccomandare l'apporto di miglioramenti al quadro di gestione dei rischi e misure correttive per porre rimedio a violazioni delle politiche, delle procedure e dei limiti in materia di rischi.

20.1 Ruolo della funzione di gestione dei rischi nella strategia e nelle decisioni in materia di rischio

187. La funzione di gestione dei rischi dovrebbe essere attivamente coinvolta in una fase iniziale nell'elaborazione della strategia in materia di rischio dell'ente e nell'assicurare che l'ente disponga di efficaci processi di gestione dei rischi. La funzione di gestione dei rischi dovrebbe fornire all'organo di gestione tutte le informazioni pertinenti relative ai rischi, per consentire a quest'ultimo di stabilire il livello di propensione al rischio dell'ente. La funzione di gestione dei rischi dovrebbe valutare la solidità e la sostenibilità della strategia in materia di rischio e della propensione al rischio. Dovrebbe garantire che la propensione al rischio sia debitamente tradotta in limiti di rischio specifici. La funzione di gestione dei rischi dovrebbe anche valutare le strategie in materia di rischi e la propensione al rischio delle unità operative, inclusi gli obiettivi proposti da queste ultime, ed essere coinvolta prima che l'organo di gestione prenda una decisione sulle strategie in materia di rischi e sulla propensione al rischio. Gli obiettivi dovrebbero essere plausibili e coerenti con la strategia dell'ente in materia di rischi.

188. Il coinvolgimento della funzione di gestione dei rischi nei processi decisionali dovrebbe garantire che i rischi siano tenuti in debita considerazione. Tuttavia, la responsabilità delle decisioni adottate dovrebbe restare in capo alle unità operative e interne e, in ultima analisi, all'organo di gestione.

20.2 Ruolo della funzione di gestione dei rischi nelle modifiche sostanziali

189. In linea con la sezione 18, prima che si prendano decisioni in merito a modifiche sostanziali o operazioni straordinarie, la funzione di gestione dei rischi dovrebbe essere coinvolta nella valutazione dell'impatto di tali modifiche e operazioni straordinarie sul rischio dell'ente e dell'intero gruppo e trasmettere i propri risultati direttamente all'organo di gestione.

190. La funzione di gestione dei rischi dovrebbe valutare le modalità con cui i rischi individuati potrebbero ripercuotersi sulla capacità dell'ente o del gruppo di gestire il proprio profilo di rischio, la propria liquidità e la solidità della propria base di capitale in condizioni normali e in circostanze avverse.

20.3 Ruolo della funzione di gestione dei rischi nell'individuazione, misurazione, valutazione, gestione, mitigazione, monitoraggio e segnalazione dei rischi

191. La funzione di gestione dei rischi dovrebbe garantire che sia stato predisposto un quadro adeguato di gestione dei rischi e che tutti i rischi siano individuati, valutati, misurati, monitorati, gestiti e debitamente segnalati da parte delle unità interessate dell'ente.

192. La funzione di gestione dei rischi dovrebbe garantire che l'individuazione e la valutazione non siano basate soltanto su informazioni quantitative o risultati dei modelli, ma che si tenga conto anche di approcci qualitativi. La funzione di gestione dei rischi dovrebbe tener informato l'organo di gestione in merito alle ipotesi utilizzate nei modelli e nelle analisi di rischio, nonché alle eventuali lacune.

193. La funzione di gestione dei rischi dovrebbe garantire che le operazioni con parti correlate siano oggetto di verifica e che i rischi che queste comportano per l'ente siano individuati e adeguatamente valutati.

194. La funzione di gestione dei rischi dovrebbe garantire che tutti i rischi individuati siano monitorati in modo efficace da parte delle unità operative.

195. La funzione di gestione dei rischi dovrebbe monitorare regolarmente il profilo di rischio effettivo dell'ente e valutarlo rispetto agli obiettivi strategici e alla propensione al rischio dello stesso al fine di consentire all'organo di gestione di adottare decisioni nell'esercizio della funzione di gestione e di metterle in discussione nell'esercizio della funzione di supervisione strategica.

196. La funzione di gestione dei rischi dovrebbe analizzare le tendenze e riconoscere i nuovi rischi o quelli emergenti e l'aumento dei rischi che deriva dal mutare delle circostanze e delle condizioni. Essa dovrebbe anche riesaminare con regolarità i risultati effettivi in materia di

rischi raffrontandoli con le stime precedenti (ossia test retrospettivi o back-testing) al fine di valutare e migliorare l'accuratezza e l'efficacia del processo di gestione dei rischi.

197. La funzione di gestione dei rischi dovrebbe valutare possibili modalità di mitigazione dei rischi. La segnalazione all'organo di gestione dovrebbe includere una proposta di azioni adeguate per mitigare il rischio.

20.4 Ruolo della funzione di gestione dei rischi in presenza di esposizioni non autorizzate

198. La funzione di gestione dei rischi dovrebbe valutare in maniera indipendente le violazioni della propensione al rischio o dei limiti di rischio (anche accertando la causa ed eseguendo un'analisi giuridica ed economica dei costi effettivi di eliminazione, riduzione o copertura dell'esposizione rispetto al costo potenziale del suo mantenimento). La funzione di gestione dei rischi dovrebbe informare le unità operative interessate e l'organo di gestione e raccomandare possibili misure correttive. La funzione di gestione dei rischi dovrebbe segnalare direttamente eventuali violazioni gravi all'organo di gestione nella sua funzione di supervisione strategica, fatta salva la possibilità per la funzione di gestione dei rischi di informare altre funzioni e comitati interni.

199. La funzione di gestione dei rischi dovrebbe svolgere un ruolo fondamentale nel garantire che una decisione sia adottata al livello appropriato su propria raccomandazione, che le unità operative interessate si conformino alla stessa e che di tale decisione siano opportunamente informati l'organo di gestione e, laddove istituito, il comitato dei rischi.

20.5 Responsabile della funzione di gestione dei rischi

200. Il responsabile della funzione di gestione dei rischi dovrebbe avere il compito di fornire informazioni esaurienti e comprensibili sui rischi e di consigliare l'organo di gestione, consentendo a quest'ultimo di comprendere il profilo di rischio complessivo dell'ente. Ciò si applica anche al responsabile della funzione di gestione dei rischi di un ente impresa madre con riferimento alla situazione consolidata.

201. Il responsabile della funzione di gestione dei rischi dovrebbe disporre di competenze, indipendenza e anzianità di servizio in misura sufficiente per mettere in discussione le decisioni che si ripercuotono sull'esposizione al rischio di un ente. Se il responsabile della funzione di gestione dei rischi non è un membro dell'organo di gestione, gli enti significativi dovrebbero nominare un responsabile indipendente della funzione di gestione dei rischi che non abbia responsabilità in altre funzioni e che riferisca direttamente all'organo di gestione. Se non è proporzionato nominare una persona che si dedichi soltanto al ruolo di responsabile della funzione di gestione dei rischi, tenendo conto del principio di proporzionalità di cui al titolo I, tale funzione può essere combinata con quella di responsabile della funzione di conformità o può essere esercitata da un'altra persona di grado elevato, a condizione che non

ci sia alcun conflitto di interesse tra le funzioni combinate. In ogni caso, tale persona dovrebbe avere sufficiente autorità, peso e indipendenza (ad es. il responsabile dell'ufficio legale).

202. Il responsabile della funzione di gestione dei rischi dovrebbe essere in grado di mettere in discussione le decisioni prese dalla dirigenza dell'ente e dal relativo organo di gestione, e i motivi delle obiezioni dovrebbero essere formalmente documentati. Se un ente intende concedere al responsabile della funzione di gestione dei rischi il diritto di porre il veto alle decisioni (ad es. una decisione relativa al credito o a un investimento o la definizione di un limite) prese a un livello inferiore rispetto all'organo di gestione, esso dovrebbe specificare la portata di tale diritto di veto, le procedure di segnalazione o di appello e le modalità di coinvolgimento dell'organo di gestione.

203. Gli enti dovrebbero istituire processi rafforzati per l'approvazione di decisioni a proposito delle quali il responsabile della funzione di gestione dei rischi ha espresso un parere negativo. L'organo di gestione nella sua funzione di supervisione strategica dovrebbe essere in grado di comunicare direttamente con il responsabile della funzione di gestione dei rischi sulle questioni chiave riguardanti i rischi, inclusi gli sviluppi che possono essere non conformi alla strategia in materia di rischio e alla propensione al rischio dell'ente.

21 Funzione di conformità

204. Gli enti dovrebbero istituire una funzione di conformità permanente ed efficace per gestire il rischio di conformità e dovrebbero nominare una persona in qualità di responsabile di tale funzione nell'intero ente (il preposto alla conformità o il responsabile della conformità).

205. Se non è proporzionato nominare una persona che si dedichi soltanto al ruolo di responsabile della conformità, tenendo conto del principio di proporzionalità di cui al titolo I, tale funzione può essere combinata con quella di responsabile della funzione di gestione dei rischi o può essere esercitata da un'altra persona di grado elevato (ad es. il responsabile dell'ufficio legale), a condizione che non ci sia alcun conflitto di interesse tra le funzioni combinate.

206. La funzione di conformità, incluso il responsabile della conformità, dovrebbe essere indipendente dalle linee di business e dalle unità interne soggette al suo controllo e disporre di autorità, peso e risorse in misura sufficiente. Tenendo conto dei criteri di proporzionalità di cui al titolo I, tale funzione può essere assistita dalla funzione di gestione dei rischi o combinata con quest'ultima o con altre funzioni appropriate, ad esempio con l'ufficio legale o il dipartimento risorse umane.

207. Il personale preposto alla funzione di conformità dovrebbe possedere conoscenze, competenze ed esperienza sufficienti in materia di conformità e relative procedure e avere accesso a una formazione regolare.

208. L'organo di gestione nella sua funzione di supervisione strategica dovrebbe sorvegliare l'attuazione di una politica di conformità ben documentata, che dovrebbe essere comunicata

a tutto il personale. Gli enti dovrebbero istituire un processo per valutare regolarmente le modifiche intervenute nella legislazione e nei regolamenti applicabili alle proprie attività.

209. La funzione di conformità dovrebbe consigliare l'organo di gestione in merito alle misure da adottare per garantire la conformità a leggi, norme, regolamenti e standard applicabili e dovrebbe valutare il possibile impatto di eventuali modifiche del contesto giuridico o normativo sulle attività e sul quadro di conformità dell'ente.

210. La funzione di conformità dovrebbe garantire che il monitoraggio della conformità sia eseguito mediante un programma di monitoraggio della conformità strutturato e ben definito a tale scopo e che la politica di conformità sia rispettata. La funzione di conformità dovrebbe informare l'organo di gestione e comunicare, eventualmente, con la funzione di gestione dei rischi, in merito al rischio di conformità dell'ente e alla sua gestione. La funzione di conformità e la funzione di gestione dei rischi dovrebbero cooperare e scambiarsi le informazioni necessarie per svolgere i rispettivi compiti. I risultati dell'attività della funzione di conformità dovrebbero essere tenuti in considerazione dall'organo di gestione e dalla funzione di gestione dei rischi nell'ambito dei processi decisionali.

211. In linea con la sezione 18 dei presenti orientamenti, la funzione di conformità dovrebbe anche verificare, in stretta cooperazione con la funzione di gestione dei rischi e con l'ufficio legale, che i nuovi prodotti e le nuove procedure rispettino il quadro normativo vigente e, se del caso, qualunque modifica imminente della legislazione, dei regolamenti e degli obblighi di vigilanza.

212. Gli enti dovrebbero adottare misure adeguate nei confronti di comportamenti interni ed esterni che possano facilitare o consentire frodi, riciclaggio di denaro, finanziamento del terrorismo o altri reati finanziari e violazioni della disciplina (ad es. violazione delle procedure interne o dei limiti).

213. Gli enti dovrebbero garantire che le loro filiazioni e succursali prendano misure volte ad assicurare che le loro operazioni siano conformi alla leggi e ai regolamenti locali. Se le leggi e i regolamenti locali ostacolano l'applicazione di procedure e sistemi di conformità più rigorosi attuati dal gruppo, in particolare se impediscono la divulgazione e lo scambio di informazioni necessarie tra le entità all'interno del gruppo, le filiazioni e le succursali dovrebbero informare di questo fatto il preposto alla conformità o il responsabile della conformità dell'ente consolidante.

22 Funzione di audit interno

214. Gli enti dovrebbero istituire una funzione di audit interno indipendente ed efficace, tenendo conto dei criteri di proporzionalità di cui al titolo I, e nominare una persona che assuma la responsabilità di tale funzione in seno all'ente. La funzione di audit interno dovrebbe essere indipendente e disporre di autorità, peso e risorse in misura sufficiente. In particolare, l'ente dovrebbe garantire che le qualifiche del personale addetto alla funzione di

audit interno e le risorse di quest'ultima, in particolare i suoi strumenti di audit e i metodi di analisi del rischio, siano adeguate alle dimensioni e alle sedi dell'ente, nonché alla natura, alla portata e alla complessità dei rischi associati al modello di business, alle attività, alla cultura del rischio e alla propensione al rischio dell'ente.

215. La funzione di audit interno dovrebbe essere indipendente dalle attività soggette ad audit. Pertanto, la funzione di audit interno non dovrebbe essere combinata con altre funzioni.

216. La funzione di audit interno dovrebbe, secondo un approccio basato sul rischio, riesaminare in modo indipendente e offrire una garanzia obiettiva della conformità di tutte le attività e le unità di un ente, incluse le attività esternalizzate, alle politiche e alle procedure dell'ente e ai requisiti normativi. Ciascuna entità all'interno del gruppo dovrebbe rientrare nella sfera di competenza della funzione di audit interno.

217. La funzione di audit interno non dovrebbe essere coinvolta nello sviluppo, nella selezione, nella determinazione e nell'attuazione di politiche, meccanismi e procedure di controllo interno specifici e dei limiti di rischio. Tuttavia, ciò non dovrebbe impedire all'organo di gestione nella sua funzione di gestione di richiedere un contributo dalla funzione di audit interno su questioni legate al rischio, ai controlli interni e alla conformità alle norme applicabili.

218. La funzione di audit interno dovrebbe valutare se il quadro di controllo interno dell'ente, come descritto alla sezione 15, sia efficiente ed efficace. In particolare, la funzione di audit interno dovrebbe valutare:

a. l'adeguatezza del quadro di governance dell'ente;

b. se le politiche e le procedure esistenti restino adeguate e conformi ai requisiti di legge e normativi e alla strategia in materia di rischio e alla propensione al rischio dell'ente;

c. la conformità delle procedure alle leggi e ai regolamenti applicabili e alle decisioni dell'organo di gestione;

d. se le procedure siano attuate in modo corretto ed efficace (ad es. la conformità delle operazioni, il livello di rischio realmente sostenuto, ecc.);

e. l'adeguatezza, la qualità e l'efficacia dei controlli eseguiti e delle segnalazioni effettuate dalle unità operative di difesa e dalle funzioni di gestione dei rischi e di conformità.

219. La funzione di audit interno dovrebbe verificare, in particolare, l'integrità dei processi che garantiscono l'affidabilità dei metodi e delle tecniche dell'ente, e delle ipotesi e delle fonti di informazioni utilizzate nei modelli interni (ad es. la modellazione dei rischi e le misurazioni

contabili). Essa dovrebbe inoltre valutare la qualità e l'uso di strumenti qualitativi di individuazione e valutazione dei rischi e le misure di mitigazione del rischio adottate.

220. La funzione di audit interno dovrebbe avere un accesso illimitato a tutti i dati, i documenti, le informazioni e gli immobili dell'ente. Ciò dovrebbe includere l'accesso ai sistemi informativi gestionali e ai verbali di tutti i comitati e gli organi decisionali.

221. La funzione di audit interno dovrebbe rispettare gli standard professionali nazionali e internazionali, quali ad esempio quelli stabiliti dall'Institute of Internal Auditors.

222. L'attività di audit interno dovrebbe essere eseguita sulla base di un piano di audit e di un dettagliato programma di audit che seguano un approccio basato sul rischio.

223. Almeno una volta all'anno dovrebbe essere redatto un piano di audit interno, sulla base degli obiettivi annuali di controllo di audit interno. Il piano di audit interno dovrebbe essere approvato dall'organo di gestione.

224. Tutte le raccomandazioni in materia di audit dovrebbero essere sottoposte a una procedura formale di follow-up da parte dei livelli appropriati della dirigenza, al fine di garantire e riferire in merito alla loro efficace e tempestiva attuazione.

Titolo VI. Gestione della continuità operativa ([40])

225. Gli enti dovrebbero predisporre un efficace piano di gestione della continuità operativa e di ripristino al fine di assicurare la propria capacità di operare su base continuativa e limitare le perdite in caso di grave interruzione dell'operatività.

226. Gli enti possono istituire una specifica funzione di continuità operativa indipendente, ad esempio come parte della funzione di gestione dei rischi ([41]).

227. L'operatività di un ente dipende da diversi processi critici (ad es. i sistemi informatici, inclusi i servizi di cloud, i sistemi di comunicazione, il personale di base e gli immobili). Lo scopo della gestione della continuità operativa è quello di ridurre le ricadute operative, finanziarie, giuridiche, reputazionali e altre ripercussioni sostanziali derivanti da incidenti o catastrofi o da blocchi prolungati che colpiscono tali risorse, e dalla conseguente interruzione delle procedure operative ordinarie dell'ente. Altre misure di gestione dei rischi potrebbero essere finalizzate a ridurre la probabilità di tali incidenti o a trasferirne gli effetti finanziari a terzi (ad es. mediante un'assicurazione).

228. Al fine di stabilire un efficace piano di gestione della continuità operativa, un ente dovrebbe analizzare attentamente i fattori di rischio e la propria esposizione a gravi interruzioni

([40]) Gli enti dovrebbero anche fare riferimento agli orientamenti dell'ABE sulla gestione dei rischi ICT e di sicurezza, disponibili all'indirizzo https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
([41]) Cfr. anche all'articolo 312 del regolamento (UE) n. 575/2013.

dell'operatività e valutare (dal punto di vista quantitativo e qualitativo) le possibili ripercussioni di tali eventi, ricorrendo a un'analisi dei dati e degli scenari interni e/o esterni. Tale analisi dovrebbe riguardare tutte le linee di business e le unità interne, inclusa la funzione di gestione dei rischi, e tenere conto della loro interdipendenza. I risultati dell'analisi dovrebbero contribuire a definire le priorità e gli obiettivi di ripristino dell'ente.

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

a. piani di emergenza e di continuità operativa al fine di garantire che l'ente reagisca in maniera adeguata alle emergenze e sia in grado di mantenere le attività operative più importanti in caso di interruzione delle proprie procedure operative ordinarie;

b. piani di ripristino per le risorse critiche per consentire all'ente di ristabilire le procedure operative ordinarie in un intervallo di tempo appropriato. Tutti i rischi residui derivanti da possibili interruzioni dell'operatività dovrebbero essere coerenti con la propensione al rischio dell'ente.

230. I piani di emergenza, di continuità operativa e di ripristino dovrebbero essere documentati e attentamente attuati. La relativa documentazione dovrebbe essere disponibile all'interno delle linee di business, delle unità interne e della funzione di gestione 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 test dovrebbero essere documentati e analizzati, e i piani dovrebbero essere rivisti di conseguenza.

Titolo VII. Trasparenza

231. Le strategie, le politiche e le procedure dovrebbero essere comunicate a tutto il personale interessato in seno all'ente. Il personale di un ente dovrebbe comprendere le politiche e le procedure associate ai propri compiti e responsabilità e attenersi ad esse.

232. Di conseguenza, l'organo di gestione dovrebbe informare e aggiornare in maniera chiara e coerente il personale interessato in merito alle strategie e alle politiche dell'ente, almeno al livello necessario per svolgere i propri compiti specifici. Allo scopo possono essere utilizzati orientamenti scritti, manuali o altri mezzi.

233. Qualora alle imprese madri sia richiesto dalle autorità competenti, in conformità dell'articolo 106, paragrafo 2, della direttiva 2013/36/UE, di pubblicare annualmente una descrizione della loro struttura giuridica e di governance, nonché della struttura dell'organizzazione del gruppo di enti, le informazioni devono includere tutte le entità

all'interno della struttura del gruppo, come definito nella direttiva 2013/34/UE ([42]), per paese.

234. Tale pubblicazione dovrebbe includere almeno:

a. una panoramica dell'organizzazione interna degli enti e della struttura del gruppo, come definito nella direttiva 2013/34/UE, e le relative modifiche, incluse le principali linee di segnalazione e responsabilità;

b. qualunque modifica sostanziale rispetto alla pubblicazione precedente e la data di tale modifica sostanziale;

c. nuove strutture giuridiche, di governance o organizzative;

d. informazioni sulla struttura, sull'organizzazione e sui membri dell'organo di gestione, incluso il numero dei relativi membri e il numero di quelli indipendenti, specificando il sesso e la durata del mandato di ciascun membro dell'organo di gestione;

e. le responsabilità principali dell'organo di gestione;

f. un elenco dei comitati dell'organo di gestione nella sua funzione di supervisione strategica e la loro composizione;

g. una panoramica della politica in materia di conflitti di interesse applicabile agli enti e all'organo di gestione;

h. una panoramica del quadro di controllo interno;

i. una panoramica del quadro di gestione della continuità operativa.

([42]) Direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese, recante modifica della direttiva 2006/43/CE del Parlamento europeo e del Consiglio e abrogazione delle direttive 78/660/CEE e 83/349/CEE del Consiglio (GU L 182 del 29.6.2013, pag. 19).

Allegato I. Aspetti da prendere in considerazione nel definire una politica di governance interna

In linea con il titolo III, gli enti dovrebbero considerare i seguenti aspetti nel documentare le politiche e i dispositivi di governance interna:

1. struttura azionaria;
2. struttura del gruppo, se applicabile (struttura giuridica e di funzionamento);
3. composizione e funzionamento dell'organo di gestione:
   a) criteri di selezione, compreso il modo in cui si tiene conto della diversità;
   b) numero, durata del mandato, rotazione, età;
   c) membri indipendenti dell'organo di gestione;
   d) membri esecutivi dell'organo di gestione;
   e) membri non esecutivi dell'organo di gestione;
   f) suddivisione interna dei compiti, se applicabile;
4. struttura di governance e organigramma (con impatto sul gruppo, se applicabile);
   a) comitati specializzati:
      i. composizione;
      ii. funzionamento;
   b) comitato esecutivo, se esistente:
      i. composizione;
      ii. funzionamento;
5. personale che riveste ruoli chiave:
   a) responsabile della funzione di gestione dei rischi;
   b) responsabile della funzione di conformità;
   c) responsabile della funzione di audit interno;
   d) direttore finanziario;
   e) altro personale che riveste ruoli chiave;
6. quadro di controllo interno:
   a) descrizione di ciascuna funzione, inclusa l'organizzazione, le risorse, il peso e l'autorità;
7. descrizione della strategia in materia di rischio e del quadro di gestione dei rischi;

8. struttura organizzativa (con impatto sul gruppo, se applicabile):
    a) struttura organizzativa, linee di business e ripartizione delle competenze e delle responsabilità;
    b) esternalizzazione;
    c) gamma di prodotti e servizi;
    d) portata geografica dell'attività;
    e) prestazione di servizi in regime di libera prestazione di servizi;
    f) succursali;
    g) filiazioni, joint venture, ecc.;
    h) utilizzo di centri offshore;
9. codice di condotta e di comportamento (con impatto sul gruppo, se applicabile):
    a) obiettivi strategici e valori aziendali;
    b) codici e regolamenti interni, politica di prevenzione;
    c) politica in materia di conflitti di interesse;
    d) denuncia di irregolarità;
10. Stato della politica di governance interna, corredato di data:
    a) sviluppo;
    b) ultima modifica;
    c) ultima valutazione;
    d) approvazione da parte dell'organo di gestione.