EBA/GL/2017/11

21/03/2018

Orientamenti

sulla governance interna

1. Conformità e obblighi di comunicazione

Status giuridico degli orientamenti

1. Il presente documento contiene orientamenti 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 enti finanziari compiono ogni sforzo per conformarsi agli orientamenti.

2. Gli orientamenti presentano 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. Ai sensi dell'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010, le autorità competenti sono tenute a conformarsi a detti orientamenti integrandoli opportunamente nelle rispettive prassi di vigilanza (per esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti sono diretti principalmente agli enti.

Obblighi di comunicazione

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti devono comunicare all'ABE entro 21/05/2018 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 comunicazione 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/2017/11" 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 comunicazioni sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3.

[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 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 i dispositivi, i processi e i meccanismi di governance interna che gli enti creditizi e le imprese di investimento devono attuare in conformità dell'articolo 74, paragrafo 1, della direttiva 2013/36/UE[2], al fine di garantire una gestione efficace e prudente dell'istituzione.

Destinatari

6. I presenti orientamenti si rivolgono alle autorità competenti quali definite all'articolo 4, paragrafo 1, punto 40), del regolamento (UE) n. 575/2013[3], compresa la Banca centrale europea relativamente ai compiti ad essa attribuiti dal regolamento (UE) n. 1024/2013, e agli enti definiti all'articolo 4, paragrafo 1, punto 3), del regolamento (UE) n. 575/2013.

Ambito di applicazione

7. Gli orientamenti si applicano ai dispositivi di governance degli enti, fra cui la loro struttura organizzativa e le rispettive linee di responsabilità, i processi volti a identificare, gestire, monitorare e segnalare i rischi ai quali sono o potrebbero essere esposti e il quadro di controllo interno.

8. 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, essi dovrebbero essere seguiti a prescindere dalla struttura dei consigli in uso (monistica e/o dualistica e/o altra struttura) nei vari Stati membri. L'organo di amministrazione, come definito all'articolo 3, paragrafo 1, punti 7) e 8), della direttiva 2013/36/UE, dovrebbe essere considerato il titolare delle funzioni di gestione (esecutive) e di supervisione strategica (non esecutive)[4].

9. I termini «organo di amministrazione nella sua funzione di gestione» e «organo di amministrazione nella sua funzione di supervisione strategica» sono utilizzati nei presenti

[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] Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pagg. 1-337).

[4] Cfr. inoltre il considerando 56 della direttiva 2013/36/UE.

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 amministrazione si applicano tali funzioni.

10. Negli Stati membri in cui l'organo di amministrazione delega, parzialmente o totalmente, le funzioni esecutive a una persona o a un organo esecutivo interno (ad esempio 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 amministrazione. Ai fini dei presenti orientamenti, qualunque riferimento all'organo di amministrazione nella sua funzione di gestione dovrebbe includere anche i membri dell'organo esecutivo o l'amministratore delegato, secondo la definizione dei presenti orientamenti, anche se non sono stati proposti o nominati membri formali dell'organo o degli organi di gestione dell'ente a norma del diritto nazionale.

11. Negli Stati membri nei quali alcune responsabilità sono esercitate direttamente dagli azionisti, dai membri o dai proprietari dell'ente invece che dall'organo di amministrazione, 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 amministrazione.

12. Le definizioni di amministratore delegato, direttore finanziario e titolare di funzioni 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 unionale o nazionale in materia.

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

Definizioni

14. Salvo diversamente specificato, i termini utilizzati e definiti nella direttiva 2013/36/UE assumono il medesimo significato nei presenti orientamenti. In aggiunta, ai fini dei presenti orientamenti, si applicano le definizioni riportate di seguito.

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.

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.
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.
Enti	gli enti creditizi e le imprese di investimento, così come definiti all'articolo 4, paragrafo 1, punti 1) e 2), rispettivamente, del regolamento (UE) n. 575/2013.
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 amministrazione nella sua funzione di gestione e nella sua funzione di supervisione strategica.
Amministratore delegato	la persona responsabile della gestione e dell'orientamento delle attività complessive di un ente.
Direttore finanziario	la persona responsabile a livello generale della gestione di tutte le attività seguenti: gestione delle risorse finanziarie, pianificazione finanziaria e rendicontazione finanziaria.
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.
Titolari di funzioni 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 amministrazione, e altri titolari di funzioni chiave, laddove individuati dagli enti secondo un approccio basato sul rischio. Altri titolari di funzioni chiave potrebbero essere i responsabili di linee di business significative, succursali dello Spazio economico europeo/Associazione europea di libero scambio, filiazioni di paesi terzi e altre funzioni interne.
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 sub-consolidata, in conformità della parte 1, titolo II,

	capo 2, del regolamento (UE) n. 575/2013. Il consolidamento prudenziale include tutte le filiazioni che sono enti o enti finanziari, secondo la definizione dell'articolo 4, punti 3) e 26), rispettivamente, del regolamento (UE) n. 575/2013, e può includere anche società strumentali, così come definite all'articolo 2, punto 18), del medesimo regolamento, aventi sede nell'UE o in paesi terzi.
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 rilevanti	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, se del caso, 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.
Enti CRD quotati	gli enti i cui strumenti finanziari sono ammessi alla negoziazione su un mercato regolamentato o su un sistema multilaterale di negoziazione, così come definiti all'articolo 4, punti 21) e 22), della direttiva 2014/65/UE, in uno o più Stati membri[5].
Azionista	una persona che detiene le azioni di un ente o, a seconda della forma giuridica dell'ente, altri proprietari o membri dell'ente.
Incarico di amministratore	una posizione in qualità di membro dell'organo di amministrazione di un ente o di un'altra entità giuridica.

3. Attuazione

Data di applicazione

15. I presenti orientamenti si applicano dal 30 giugno 2018.

Abrogazione

[5] 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).

16. Gli orientamenti dell'ABE sulla governance interna (GL 44) del 27 settembre 2011 sono abrogati con effetto dal 30 giugno 2018.

4. Orientamenti

Titolo I. Proporzionalità

17. 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 degli obblighi regolamentari siano raggiunti in modo efficace.

18. 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 rilevanti dovrebbero disporre di dispositivi di governance più sofisticati, mentre enti piccoli e meno complessi possono attuare dispositivi di governance più semplici.

19. Al fine dell'applicazione del principio di proporzionalità e allo scopo di garantire un'adeguata attuazione delle prescrizioni, enti e autorità competenti dovrebbero tener conto dei seguenti criteri:

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

    b. la presenza geografica dell'ente e il volume delle sue 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 o meno in borsa;

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

    f. la tipologia di attività e di servizi autorizzati prestati dall'ente (ad esempio 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. la tipologia di clienti (ad esempio clientela al dettaglio, società, istituzioni, piccole imprese, enti pubblici) e la complessità dei prodotti o dei contratti;

k. le attività esternalizzate e i canali di distribuzione; e

l. i sistemi informatici disponibili, inclusi i sistemi di continuità e le attività di esternalizzazione in quest'area.

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

1 Ruolo e responsabilità dell'organo di amministrazione

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

21. I compiti dell'organo di amministrazione 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 amministrazione dovrebbero essere descritti in un documento scritto e debitamente approvati dall'organo di amministrazione.

22. Tutti i membri di tale organo dovrebbero essere pienamente consapevoli della struttura e delle responsabilità dell'organo di amministrazione e della suddivisione dei compiti tra le diverse funzioni dell'organo di amministrazione e dei suoi comitati. Al fine di conseguire un sistema appropriato di equilibrio dei poteri, il suo processo decisionale non dovrebbe essere dominato da un singolo membro o da una ristretta sottocategoria dei suoi membri. L'organo di amministrazione, nella sua funzione di supervisione strategica e di gestione, dovrebbe interagire in modo efficace. Ciascuna funzione dovrebbe fornire all'altra informazioni sufficienti per permettere a entrambe di svolgere i rispettivi ruoli.

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

a. la strategia aziendale globale 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, inclusi la propensione al rischio e il quadro di gestione dei rischi dell'ente, nonché le misure per garantire che l'organo di amministrazione dedichi tempo sufficiente alle questioni legate al rischio;

c. una governance interna adeguata ed efficace e un quadro di controllo interno che includa una chiara struttura organizzativa e una gestione dei rischi interna indipendente ed efficiente, funzioni di conformità e audit che dispongano nella misura necessaria di autorità, peso e risorse per svolgere le loro funzioni;

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

e. 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[6];

g. dispositivi volti a garantire che le valutazioni di idoneità individuali e collettive dell'organo di amministrazione siano svolte in modo efficace, che la pianificazione della composizione e della successione dell'organo di amministrazione sia appropriata e che l'organo di amministrazione svolga le sue funzioni in modo efficace[7];

h. un processo di selezione e di valutazione dell'idoneità per i titolari di funzioni chiave[8];

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

    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 amministrazione, le autorità competenti e altre parti;

[6] 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).

[7] Cfr. inoltre gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e 2014/65/UE.

[8] Cfr. inoltre gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e 2014/65/UE.

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 per quanto riguarda l'assunzione del rischio;

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

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

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

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

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

26. Un membro dell'organo di amministrazione 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 amministrazione 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 23 e 24. Il quadro di governance interna e la relativa attuazione dovrebbero essere rivisti e aggiornati su base periodica, sulla base del principio di proporzionalità, come chiarito ulteriormente al titolo I. Qualora l'ente risenta di eventuali modifiche sostanziali, dovrebbe essere svolta una revisione dettagliata.

2 Funzione di gestione dell'organo di amministrazione

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

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

30. L'organo di amministrazione 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 amministrazione nella sua funzione di gestione dovrebbe riferire in maniera esaustiva all'organo di amministrazione 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 dell'ambiente economico e commerciale dell'ente, della sua liquidità e della solidità della base di capitale e delle sue esposizioni a rischi sostanziali.

3 Funzione di supervisione strategica dell'organo di amministrazione

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

32. Fatto salvo il diritto nazionale, l'organo di amministrazione 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 gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e 2014/65/UE.

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

    a. sorvegliare e monitorare il processo decisionale e le azioni dell'organo di amministrazione nella sua funzione di gestione, nonché fornire una sorveglianza efficace dello stesso nella sua funzione di gestione, 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 maniera costruttiva e rivedere in modo critico le proposte e le informazioni fornite dai membri dell'organo di amministrazione nella sua funzione di gestione, nonché le sue decisioni;

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

    d. garantire e valutare periodicamente l'efficacia della 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, inclusi la sua propensione al rischio e il quadro di gestione dei rischi, nonché di altre politiche (ad esempio la politica di remunerazione) e del quadro per l'informativa;

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

g. sorvegliare l'attuazione e la tenuta di un codice etico 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 del rischio;

i. garantire che i responsabili delle funzioni del 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 amministrazione nella sua funzione di supervisione strategica, laddove necessario, nel caso in cui evoluzioni sfavorevoli del rischio si ripercuotano o possano ripercuotersi sull'ente; e

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

4 Ruolo del presidente dell'organo di amministrazione

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

35. 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.

36. In generale, il presidente dell'organo di amministrazione dovrebbe essere un membro non esecutivo. Se al presidente è consentita l'assunzione di compiti esecutivi, l'ente dovrebbe disporre di misure atte a mitigare eventuali ripercussioni negative sul bilanciamento dei poteri dell'ente (ad esempio nominando un membro capofila o un membro esperto indipendente del consiglio di amministrazione o disponendo di un ampio numero di membri non esecutivi all'interno dell'organo di amministrazione 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 amministrazione 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.

37. 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 amministrazione siano prese su basi solide e ben informate e che i documenti e le informazioni siano ricevuti con sufficiente anticipo rispetto alla riunione.

38. Il presidente dell'organo di amministrazione dovrebbe contribuire a una ripartizione chiara dei compiti tra i membri dell'organo di amministrazione e alla predisposizione di un efficiente flusso di informazioni tra gli stessi, al fine di consentire ai membri dell'organo di amministrazione nella sua funzione di supervisione strategica di contribuire in modo costruttivo alle discussioni e di votare su basi solide e ben informate.

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

5.1 Istituzione di comitati

39. 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 direttiva 2013/36/UE, tutti gli enti che sono essi stessi rilevanti, considerati i livelli individuali, sub-consolidati e consolidati, devono istituire un comitato rischi, un comitato nomine[9] e un comitato remunerazioni[10], per fornire consulenza all'organo di amministrazione nella sua funzione di supervisione strategica e per preparare le decisioni che tale organo deve prendere. Gli enti non rilevanti, anche quando rientrano nell'ambito del consolidamento prudenziale di un ente significativo in una situazione sub-consolidata o consolidata, non sono obbligati a istituire tali comitati.

40. Laddove non venga istituito alcun comitato rischi o comitato nomine, i suddetti comitati nei presenti orientamenti s'intendono riferiti all'organo di amministrazione nella sua funzione di supervisione strategica, tenendo conto del principio di proporzionalità di cui al titolo I.

41. Gli enti, alla luce dei criteri menzionati al titolo I dei presenti orientamenti, possono istituire altri comitati (ad esempio il comitato etico, di condotta e di conformità).

42. Gli enti dovrebbero garantire una chiara ripartizione e distribuzione dei doveri e dei compiti tra i comitati specifici dell'organo di amministrazione.

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

[9] Cfr. inoltre gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e 2014/65/UE.

[10] In merito al comitato remunerazioni, si faccia riferimento agli orientamenti dell'ABE su sane politiche di remunerazione.

44. 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 amministrazione nella sua funzione di supervisione strategica dall'adempiere collettivamente ai propri compiti e responsabilità.

5.2 Composizione dei comitati[11]

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

46. I membri indipendenti[12] dell'organo di amministrazione nella sua funzione di supervisione strategica dovrebbero essere attivamente coinvolti nei comitati.

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

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

49. Gli enti dovrebbero valutare la rotazione occasionale delle presidenze e dei membri dei comitati, tenendo conto dell'esperienza specifica, delle conoscenze e delle competenze richieste a livello individuale o collettivo per tali comitati.

50. Il comitato rischi e il comitato nomine dovrebbero essere composti da membri non esecutivi dell'organo di amministrazione nella sua funzione di supervisione strategica dell'ente in questione. Il comitato controllo interno e revisione contabile dovrebbe essere composto conformemente all'articolo 41 della direttiva 2006/43/CE [13]. Il comitato remunerazioni dovrebbe essere composto conformemente alla sezione 2.4.1 degli orientamenti dell'ABE su sane politiche di remunerazione[14].

51. Negli enti a rilevanza sistemica a livello globale (G-SII) e negli altri enti a rilevanza sistemica (O-SII), il comitato nomine dovrebbe includere una maggioranza di membri indipendenti ed essere presieduto da un membro indipendente. Negli altri enti rilevanti, sulla base di quanto stabilito

[11] Tale sezione dovrebbe essere letta unitamente agli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e 2014/65/UE.

[12] Come definito nella sezione 9.3 degli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e direttiva 2014/65/UE.

[13] 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) e modificata da ultimo dalla direttiva 2014/56/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014.

[14] 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).

dalle autorità competenti o prescritto dal diritto nazionale, il comitato nomine dovrebbe includere un numero sufficiente di membri indipendenti; tali enti possono anche prendere in considerazione la buona pratica di disporre di un presidente indipendente per il comitato nomine.

52. I membri del comitato nomine dovrebbero possedere, a livello individuale e collettivo, conoscenze, capacità e competenze adeguate in merito al processo di selezione e ai requisiti di adeguatezza.

53. Nei G-SII e negli O-SII, il comitato rischi dovrebbe essere composto in maggioranza da membri indipendenti. Nei G-SII e negli O-SII, il presidente del comitato rischi dovrebbe essere un membro indipendente. Negli altri enti rilevanti, sulla base di quanto stabilito dalle autorità competenti o prescritto dal diritto nazionale, il comitato 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 rischi non dovrebbe coincidere né con la presidenza dell'organo di amministrazione né con la presidenza di qualunque altro comitato.

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

5.3 Processi dei comitati

55. I comitati dovrebbero informare regolarmente l'organo di amministrazione nella sua funzione di supervisione strategica.

56. I comitati dovrebbero interagire tra loro secondo le esigenze. Fatto salvo il paragrafo 48, tale interazione potrebbe assumere la forma di partecipazione incrociata, in modo tale che il presidente o un membro di un comitato possano essere anche membri di un altro comitato.

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

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

59. Il comitato rischi e il comitato nomine dovrebbero quantomeno:

    a. avere accesso a tutte le informazioni pertinenti e a tutti i dati necessari allo svolgimento del loro ruolo, incluse le informazioni e i dati provenienti da funzioni societarie e di controllo pertinenti (ad esempio di tipo legale e finanziario e quelli relativi a risorse umane, informatica, rischi, conformità, audit, ecc.);

    b. ricevere periodicamente relazioni, informazioni ad hoc, comunicazioni e pareri da parte dei 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 che possa verificarsi, corredati di informazioni dettagliate e raccomandazioni sulle misure correttive adottate, da adottare o consigliate per farvi fronte;

c. riesaminare su base periodica e prendere decisioni per quanto concerne contenuto, formato e frequenza delle informazioni sul rischio da comunicare loro; e

d. laddove necessario, garantire l'adeguato coinvolgimento delle funzioni di controllo interno e di altre funzioni pertinenti (risorse umane, legali, finanziarie) nelle loro rispettive aree di competenza e/o rivolgersi a un esperto esterno per un parere.

5.4 Ruolo del comitato rischi

60. Se istituito, il comitato rischi dovrebbe almeno:

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

b. fornire assistenza all'organo di amministrazione 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 propensione al rischio e alla strategia in materia di rischio approvate;

d. fornire all'organo di amministrazione nella sua funzione di supervisione strategica le raccomandazioni sugli adeguamenti necessari alla strategia in materia di rischio risultante, 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 un numero di 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 sostanziali offerti ai clienti con il modello di business e la strategia in materia di rischio dell'ente[15]. Il comitato rischi dovrebbe valutare i rischi associati ai prodotti e servizi finanziari offerti e tener conto dell'allineamento tra i prezzi attribuiti a tali prodotti e servizi e i profitti ricavati dagli stessi; e

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

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

62. Il comitato rischi, qualora istituito, deve esaminare, fatti salvi i compiti del comitato remunerazioni, se gli incentivi forniti dalle politiche e prassi 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 controllo interno e revisione contabile

63. In conformità della direttiva 2006/43/CE[16], laddove istituito, il comitato controllo interno e revisione contabile dovrebbe, fra l'altro:

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 riguardante 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

[15] Cfr. inoltre 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.

[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.

direttiva 2006/43/UE, e dell'articolo 6 del regolamento (UE) n. 537/2014 [17], 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;

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 remunerazione e il loro licenziamento, da parte dell'organo competente dell'ente (in conformità dell'articolo 16 del regolamento (UE) n. 537/2014, salvo applicazione dell'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/UE, 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 la revisione legale dei conti ha contribuito all'integrità dell'informativa finanziaria e il ruolo del comitato controllo interno e revisione contabile in tale processo; e

i. ricevere e tener conto delle relazioni sulla revisione contabile.

5.6 Comitati congiunti

64. In conformità dell'articolo 76, paragrafo 3, della direttiva 2013/36/UE, le autorità competenti possono consentire agli enti non considerati significativi di combinare il comitato rischi, laddove istituito, con il comitato controllo interno e revisione contabile di cui all'articolo 39 della direttiva 2006/43/CE.

65. Se istituiti all'interno di enti non rilevanti, il comitato rischi e il comitato nomine possono costituirsi congiuntamente. In tal caso, tali enti dovrebbero documentare le ragioni per le quali hanno scelto di costituire in forma congiunta i comitati e in che modo tale strategia consente di conseguire gli obiettivi dei comitati.

[17] 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).

66. Gli enti dovrebbero, in qualunque momento, garantire che i membri di un comitato congiunto posseggano, a livello individuale e collettivo, conoscenze, competenze ed esperienze adeguate per capire a fondo i doveri che il comitato congiunto è chiamato a svolgere[18].

Titolo III. Quadro di governance

6 Quadro e struttura a livello organizzativo

6.1 Quadro organizzativo

67. L'organo di amministrazione 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, sub-consolidato e consolidato. L'organo di amministrazione 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 l'attribuzione di responsabilità, in particolare fra i titolari di funzioni chiave, all'interno di un ente dovrebbero essere chiare, ben definite, coerenti, applicabili e debitamente documentate. La documentazione, se necessario, dovrebbe essere aggiornata.

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

69. L'organo di amministrazione dovrebbe valutare se e in che modo eventuali modifiche sostanziali nella struttura del gruppo (ad esempio 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 amministrazione dovrebbe intervenire rapidamente attuando le necessarie misure correttive.

6.2 Conoscere la propria struttura

70. L'organo di amministrazione dovrebbe conoscere e comprendere a pieno 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.

71. L'organo di amministrazione dovrebbe anche rispondere dell'approvazione di strategie e politiche sane per l'istituzione di nuove strutture. Qualora all'ente facciano capo molte entità giuridiche all'interno del 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

[18] Cfr. inoltre gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e 2014/65/UE.

governance interna dell'ente né per l'efficace gestione e sorveglianza dei rischi del gruppo nel suo complesso. L'organo di amministrazione 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 dell'ente, per gli azionisti e le altre parti interessate, nonché per l'autorità competente.

72. L'organo di amministrazione dovrebbe essere a capo della struttura dell'ente, guidarne l'evoluzione e far fronte ai relativi limiti, e garantire che la struttura sia giustificata ed efficiente e non presenti un grado di complessità eccessivo o non appropriato.

73. L'organo di amministrazione di un ente consolidato 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 con queste ultime. Ciò include la comprensione dei rischi operativi specifici del gruppo, delle esposizioni intragruppo e di come i profili di *funding*, capitale, liquidità e rischio del gruppo potrebbero esserne influenzati in condizioni normali e in circostanze avverse. L'organo di amministrazione dovrebbe garantire che l'ente sia in grado di fornire informazioni sul gruppo in maniera tempestiva, relativamente alla tipologia, 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, sub-consolidata e consolidata.

74. L'organo di amministrazione dell'ente consolidante dovrebbe garantire che le diverse entità del gruppo (incluso l'ente consolidante stesso) ricevano informazioni sufficienti per avere una percezione chiara degli obiettivi generali, delle strategie e del profilo di rischio del gruppo 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 amministrazione, le linee di business e le funzioni di controllo interno. I membri dell'organo di amministrazione 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 con la strategia approvata all'interno dell'intero gruppo; e

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

6.3 Strutture complesse e attività non standard o non trasparenti

75. 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 stabilire se tali strutture possano essere utilizzate per un fine legato al riciclaggio di denaro o ad altri reati finanziari, e dei rispettivi controlli e del quadro giuridico vigente[19]. A tal fine, gli enti dovrebbero tener conto quantomeno:

    a. della misura in cui la giurisdizione nella quale sarà istituita la struttura rispetta effettivamente le norme UE e internazionali in materia di trasparenza fiscale, anti-riciclaggio e lotta al finanziamento del terrorismo;

    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 ultimo;

    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 amministrazione dell'ente o la capacità dell'ente di gestire il rischio correlato; e

    f. se la struttura ponga ostacoli alla supervisione strategica efficace da parte delle autorità competenti.

76. In ogni caso, gli enti non dovrebbero istituire strutture poco chiare o inutilmente complesse senza una chiara motivazione economica o un obiettivo lecito o se gli enti temono che tali strutture possano essere utilizzate per un obiettivo legato a reati finanziari.

77. Nell'istituzione di tali strutture, l'organo di amministrazione dovrebbe comprenderle e comprenderne l'obiettivo e i rischi specifici a queste associati, nonché 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 amministrazione abbia accertato che tutti i rischi sostanziali siano stati individuati, inclusi i rischi reputazionali, che tutti i rischi possano essere gestiti in modo efficace e debitamente comunicati e che venga garantita una sorveglianza efficace. Tanto 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.

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

[19] Per ulteriori dettagli sulla valutazione del rischio paese e del rischio associato ai singoli prodotti e clienti, gli enti dovrebbero far riferimento anche agli orientamenti congiunti finali (una volta emessi) sui fattori di rischio: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper.

79. L'organo di amministrazione 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 esempio limiti applicabili, obblighi 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;

    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 amministrazione nella sua funzione di supervisione strategica, nonché all'autorità competente che ha concesso l'autorizzazione; e

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

80. 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.

81. Gli enti dovrebbero adottare le stesse misure di gestione dei rischi che adottano per le proprie attività quando svolgono attività non standard o non trasparenti per i clienti (ad esempio assistenza ai clienti per istituire società veicolo in paesi offshore, sviluppo di strutture complesse, finanziamento di transazioni per queste ultime o fornitura di servizi fiduciari) che pongono simili sfide di governance interna e creano significativi rischi operativi e reputazionali. In particolare, gli enti dovrebbero analizzare la ragione per la quale un cliente intende istituire una determinata struttura.

7 Quadro organizzativo in un contesto di gruppo

82. 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 sub-consolidata. A tal fine, le imprese madri e le filiazioni, nell'ambito del consolidamento prudenziale, dovrebbero attuare nelle loro filiazioni non soggette alla direttiva 2013/36/UE dispositivi, processi e meccanismi tali da garantire solidi dispositivi di governance su base consolidata e sub-consolidata. Le funzioni competenti all'interno dell'ente consolidante e delle sue filiazioni dovrebbero interagire e scambiare dati e informazioni, se del caso. 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.

83. L'organo di amministrazione 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 sub-consolidato, in modo da rispettare tutti gli obblighi specifici in conformità del diritto unionale e nazionale.

84. Al livello consolidato e sub-consolidato, l'ente consolidante dovrebbe garantire l'osservanza delle politiche del gruppo in materia di governance da parte di tutti gli enti e delle altre entità nell'ambito del consolidamento prudenziale, incluse le loro filiazioni non soggette alla direttiva 2013/36/UE. Nell'applicazione delle 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 non sono organizzate in entità giuridiche separate, ma all'interno di una matrice di linee di business che include entità giuridiche multiple.

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

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

87. L'ente consolidante dovrebbe garantire che le filiazioni istituite nei paesi terzi e rientranti nell'ambito del consolidamento prudenziale dispongano di 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 seguano i presenti orientamenti, purché ciò non contravvenga alle leggi del paese terzo.

88. Gli obblighi in materia di governance di cui alla direttiva 2013/36/UE e i 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'UE 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 in un 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 siano prese 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'UE, fra cui la direttiva 2013/36/UE e i presenti orientamenti.

89. Nell'istituire tali politiche e nel documentare i dispositivi di governance, gli enti dovrebbero tener conto degli aspetti elencati nell'allegato I degli orientamenti. Nonostante 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[20]

90. L'organo di amministrazione dovrebbe approvare nonché riesaminare e aggiornare regolarmente la politica di esternalizzazione di un ente, garantendo che le modifiche appropriate siano attuate in modo tempestivo.

91. La politica di esternalizzazione dovrebbe valutare l'impatto dell'esternalizzazione sulle attività di un ente e sui rischi ai quali l'ente è esposto (ad esempio i rischi operativi, inclusi i rischi legali e informatici, reputazionali e di concentrazione). Tale politica dovrebbe includere i dispositivi d'informazione e monitoraggio da attuare per tutta la durata del contratto di esternalizzazione (inclusi la redazione di uno studio di fattibilità per l'esternalizzazione, la sottoscrizione 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.

92. Tale politica dovrebbe indicare che il ricorso all'esternalizzazione non dovrebbe ostacolare l'efficace vigilanza ispettiva o la vigilanza 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 intragruppo (ad esempio i servizi forniti da un'entità giuridica separata all'interno di un gruppo dell'ente) e prendere in considerazione eventuali circostanze specifiche del gruppo.

93. Nella selezione di prestatori di servizi esterni sostanziali o nell'esternalizzazione delle attività, la politica dovrebbe prevedere l'obbligo per l'ente di tenere conto del fatto che il prestatore di servizi disponga o non disponga di standard etici o di un codice etico adeguati.

Titolo IV. Cultura del rischio e codice etico

9 Cultura del rischio

94. Una cultura del rischio sana e coerente dovrebbe essere un elemento chiave nella gestione efficace dei rischi da parte degli enti e consentire a questi ultimi di prendere decisioni adeguate e informate.

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 fanno fronte e di come tali rischi vengono gestiti, alla luce della propensione al rischio dell'ente.

[20] I presenti orientamenti si limitano a trattare la politica generale di esternalizzazione; gli aspetti specifici in materia di esternalizzazione sono trattati negli orientamenti del CEBS in materia di esternalizzazione, dei quali è prevista una revisione. Tali orientamenti sono disponibili all'indirizzo: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

96. Gli enti dovrebbero sviluppare una cultura del rischio attraverso 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.

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 amministrazione, 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 conto la sua propensione al rischio e la sua capacità di rischio.

98. Una forte cultura del rischio dovrebbe anche prevedere quanto segue:

    a. l'adozione di una linea dall'alto: l'organo di amministrazione dovrebbe essere responsabile della definizione e della comunicazione dei valori chiave e delle aspettative dell'ente. Il comportamento dei suoi membri dovrebbe riflettere i valori adottati. La dirigenza dell'ente, compresi i titolari di funzioni chiave, dovrebbero favorire la comunicazione interna al personale dei valori chiave e delle aspettative. Il personale dovrebbe agire in osservanza di tutte le leggi e di tutti i regolamenti applicabili e segnalare prontamente le situazioni non conformi osservate all'interno o all'esterno dell'ente (ad esempio all'autorità competente mediante una procedura di denuncia delle irregolarità). L'organo di amministrazione dovrebbe continuamente promuovere, monitorare e valutare la cultura del rischio dell'ente, valutare 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 chiave 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 riguardo al comportamento dell'ente relativo all'assunzione del rischio.

    c. Comunicazione e messa in discussione efficaci: una cultura del rischio solida dovrebbe promuovere un ambiente dove viga una comunicazione aperta e una messa in discussione efficace, in cui i processi decisionali incoraggiano pareri ampiamente diversificati, consentono di testare le pratiche attuali, stimolano un atteggiamento critico costruttivo fra il personale e promuovono 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 di assunzione del rischio con il profilo di rischio dell'ente e il suo interesse a lungo termine[21].

10 Valori aziendali e codice etico

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

100. Gli standard attuati dovrebbero mirare a ridurre i rischi ai quali l'ente è esposto, in particolare i rischi di tipo operativo e reputazionale, che possono avere un impatto considerevolmente 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 del cliente.

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

a. ricordare ai lettori 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 il messaggio secondo cui l'organo di amministrazione si aspetta che 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 frode, riciclaggio di denaro e pratiche anti-trust, sanzioni finanziarie, corruzione, manipolazione di mercato, vendita di prodotti inadeguati e altre violazioni della normativa che tutela i consumatori);

[21] Si rimanda anche agli 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.

d. chiarire che, oltre a rispettare le disposizioni giuridiche 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

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.

102. 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 etico o a uno strumento analogo e valutarne le violazioni, nonché un processo per gestire i casi di non conformità. L'organo di amministrazione dovrebbe essere informato periodicamente del risultato.

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

103. L'organo di amministrazione dovrebbe essere responsabile della definizione, dell'approvazione e del monitoraggio 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 dalle varie attività e dai vari ruoli dell'ente, dei diversi enti nell'ambito del consolidamento prudenziale o delle diverse linee di business o unità operative all'interno di un ente, o in relazione ad azionisti esterni.

104. 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.

105. 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 dei compiti, ad esempio affidando a persone diverse le attività confliggenti nei processi riguardanti operazioni o servizi, o attribuendo a persone diverse i compiti di vigilanza e di informativa per le attività confliggenti;

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

c. istituire procedure adeguate per le operazioni con le parti correlate, ad esempio richiedendo che le operazioni siano condotte a condizioni di mercato.

12 Politica in materia di conflitto di interesse per il personale[22]

[22] Tale sezione dovrebbe essere letta unitamente agli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e 2014/65/UE.

106. L'organo di amministrazione dovrebbe essere responsabile della definizione, dell'approvazione e del monitoraggio dell'attuazione e della gestione 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 amministrazione, 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 sul conflitto di interesse a livello di gruppo, su base consolidata o sub-consolidata.

107. 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 da rapporti personali o professionali in essere, ma anche passati. Qualora emergano conflitti di interesse, gli enti dovrebbero valutare la loro rilevanza e decidere e attuare misure di mitigazione appropriate.

108. In merito ai 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.

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

    a. interessi economici (ad esempio azioni, altri diritti di proprietà e partecipazioni, partecipazioni 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);

    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 esempio legami di parentela);

    d. un'altra attività professionale o un'attività professionale svolta precedentemente (ad esempio negli ultimi cinque anni);

    e. rapporti personali o professionali con azionisti esterni pertinenti (ad esempio associazione con fornitori sostanziali, consulenti o altri prestatori di servizi); e

    f. influenza politica o relazioni politiche.

110. 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.

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

112. 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 evento singolo (ad esempio 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.

113. La politica dovrebbe stabilire procedure, misure, prescrizioni 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, prescrizioni, 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 amministrazione 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. definire procedure adeguate per le operazioni con parti correlate (gli enti possono considerare, tra l'altro, di richiedere che le operazioni siano condotte in condizioni di libera concorrenza, di richiedere che tutte le procedure di controllo interno pertinenti siano integralmente applicate a tali operazioni, di richiedere il parere consultivo vincolante dei membri indipendenti dell'organo di amministrazione, di richiedere l'approvazione da parte degli azionisti della maggior parte delle operazioni pertinenti e di limitare l'esposizione a tali operazioni); e

    e. evitare che i membri dell'organo di amministrazione ricoprano incarichi amministrativi in enti concorrenti, salvo 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 affiliati permanentemente a un organismo centrale, come indicato all'articolo 10 del regolamento (UE) n. 575/2013 o enti che rientrano nell'ambito di applicazione del consolidamento prudenziale.

114. La politica dovrebbe coprire, nello specifico, il rischio di conflitti di interesse a livello dell'organo di amministrazione 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 amministrazione 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 sono suscettibili di pregiudicare l'indipendenza di giudizio dei membri dell'organo di amministrazione[23].

115. I conflitti di interesse reali o potenziali, segnalati alla funzione responsabile all'interno dell'ente, dovrebbero essere adeguatamente valutati e gestiti. In caso 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.

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

13 Procedure interne di segnalazione

117. Gli enti dovrebbero adottare e mantenere adeguate politiche e procedure interne di segnalazione rivolte al personale, allo scopo di comunicare violazioni effettive o potenziali agli obblighi normativi o interni, compresi quelli stabiliti nel regolamento (UE) n. 575/2013 e dalle leggi 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 costituire una ragione sufficiente per aprire un'indagine.

118. Al fine di evitare conflitti di interesse, il personale dovrebbe poter segnalare violazioni al di fuori delle tradizionali linee di segnalazione (ad esempio 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 della direttiva 95/46/CE.

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

120. Le informazioni fornite dal personale mediante le procedure di segnalazione dovrebbero, se del caso, essere messe a disposizione dell'organo di amministrazione e di altre funzioni di responsabilità definite nella politica interna di segnalazione. Laddove richiesto dal personale che segnala la violazione, le informazioni dovrebbero essere fornite all'organo di

[23] Cfr. inoltre gli orientamenti congiunti dell'ESMA e dell'ABE sulla valutazione dell'idoneità dei membri dell'organo gestorio e del personale che riveste ruoli chiave, in conformità delle direttive 2013/36/UE e 2014/65/UE.

amministrazione e ad altre funzioni di responsabilità in forma anonima. Gli enti possono anche prevedere una procedura di denuncia di irregolarità che consenta di trasmettere le informazioni in forma anonima.

121. 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.

122. Gli enti dovrebbero inoltre proteggere da eventuali effetti negativi le persone segnalate nel caso in cui dall'indagine non emergano prove che giustifichino l'adozione di provvedimenti nei confronti di tali persone. Se sono adottate misure, l'ente dovrebbe farlo in modo da mirare alla protezione della persona in questione da effetti negativi involontari che vadano oltre l'obiettivo dei provvedimenti adottati.

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

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

b. fornire regole chiare atte a garantire che l'informazione sulla segnalazione e sulle persone segnalate e sulla violazione siano trattate in modo riservato, in conformità della direttiva 95/46/CE, salvo tale comunicazione sia richiesta dalla normativa nazionale nel contesto di ulteriori indagini o di successivi procedimenti giudiziari;

c. proteggere la persona che esprime preoccupazione dal 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 al controllo del rispetto della legge;

e. garantire, laddove possibile, che sia fornita la 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; e

g. garantire la tenuta di un apposito registro.

14 Segnalazione delle violazioni alle autorità competenti

124. Le autorità competenti dovrebbero stabilire meccanismi efficaci e affidabili per permettere al personale degli enti di segnalare alle autorità competenti violazioni, potenziali o reali, degli obblighi normativi, compresi anche quelli stabiliti nel regolamento (UE) n. 575/2013 e nelle

previsioni nazionali che recepiscono la direttiva 2013/36/UE. Tali meccanismi dovrebbero includere almeno:

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 che segnala la violazione sia della persona fisica sospettata di essere responsabile della violazione, in conformità della direttiva 95/46/CE; e

d. procedure chiare, come definite al paragrafo 123.

125. Fatta salva la possibilità di segnalare violazioni mediante i meccanismi delle autorità competenti, tali autorità 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

126. Gli enti dovrebbero sviluppare e mantenere una cultura che incoraggi un atteggiamento positivo nei confronti del controllo del rischio 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 amministrazione che siano idonee e sufficienti per adempiere alla loro missione, nonché di un quadro di gestione dei rischi.

127. Il quadro di controllo interno dell'ente interessato 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 interessati dovrebbero organizzare il necessario scambio delle informazioni in modo da garantire che ogni organo di amministrazione, 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 a livello di gruppo e tra i responsabili delle funzioni di controllo interno a livello di gruppo e di organo di amministrazione dell'ente.

128. Il quadro di controllo interno dovrebbe coprire l'intera organizzazione, incluse le responsabilità e i compiti dell'organo di amministrazione 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.

129. 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; e

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

16 Attuazione di un quadro di controllo interno

130. L'organo di amministrazione dovrebbe essere responsabile della definizione e del monitoraggio dell'adeguatezza e dell'efficacia del quadro di controllo interno, dei processi e dei meccanismi, e del monitoraggio di tutte le linee di business e unità interne, incluse le funzioni di controllo interno (quali le funzioni di gestione dei rischi, di conformità e 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 amministrazione.

131. Un ente dovrebbe disporre di un processo decisionale chiaro, trasparente e documentato e di una distribuzione chiara 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.

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

133. Nell'attuare il quadro di controllo interno, gli enti dovrebbero stabilire un'opportuna separazione delle funzioni (ad esempio assegnando a persone diverse le attività confliggenti nell'ambito dell'elaborazione delle operazioni o nella prestazione di servizi, oppure affidando a persone diverse responsabilità di supervisione strategica e di segnalazione relativamente ad attività confliggenti) e stabilire barriere all'informazione, ad esempio operando una separazione fisica di taluni dipartimenti.

134. 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.

135. Le funzioni di controllo interno dovrebbero sottoporre regolarmente all'organo di amministrazione relazioni scritte sulle principali carenze individuate. Tali relazioni dovrebbero includere, per ciascuna nuova carenza individuata, i rischi pertinenti connessi, una valutazione d'impatto, raccomandazioni e misure correttive da adottare. L'organo di amministrazione dovrebbe dar seguito ai risultati delle funzioni di controllo interno in modo tempestivo ed efficace e richiedere misure correttive adeguate. Dovrebbe essere applicata una procedura formale di follow-up dei risultati e delle misure correttive adottate.

17 Quadro di gestione dei rischi

136. 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, fra cui le funzioni di controllo interno, riconoscendo pienamente la natura economica di tutte le sue esposizioni al rischio. La gestione dei rischi dovrebbe consentire all'ente di prendere decisioni pienamente informate sull'assunzione del rischio. Il quadro di gestione dei rischi dovrebbe includere 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 sub-consolidato. 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 e strategici.

137. Il quadro di gestione dei rischi di un ente dovrebbe prevedere politiche, procedure, limiti e controlli del rischio 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, dell'ente e a un livello consolidato e sub-consolidato.

138. Il quadro di gestione dei rischi di un ente dovrebbe fornire indicazioni specifiche sull'attuazione degli indirizzi strategici dell'ente. Tali indicazioni dovrebbero, se del caso, stabilire e mantenere limiti interni coerenti con la propensione al rischio dell'ente e commisurati al sano funzionamento, alla solidità finanziaria, alla base del 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 ai limiti del rischio, vi sia un processo definito per segnalarle e gestirle con un'apposita procedura di follow-up.

139. Il quadro di gestione dei rischi dovrebbe essere sottoposto a una revisione interna indipendente, svolta ad esempio dalla funzione di audit interno e rivalutata 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 rischi. Fra i fattori da considerare vi sono inoltre 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.

140. 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 ai rischi 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.

141. Gli enti dovrebbero tenere conto del fatto che i risultati delle metodologie delle valutazioni quantitative, compreso lo stress test, dipendono in larga misura dalle limitazioni e dalle ipotesi dei modelli (fra cui l'entità e la durata dello shock e i rischi sottostanti). A titolo esemplificativo, il fatto che i modelli mostrino rendimenti molto elevati sul capitale economico potrebbe derivare da una debolezza nei modelli (ad esempio 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 del modello 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.

142. 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. Per 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.

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

144. 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.

145. Dovrebbero essere istituiti meccanismi di segnalazione periodici e trasparenti, affinché l'organo di amministrazione, il suo comitato 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.

146. 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 esempio 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 significative[24]

147. Gli enti dovrebbero disporre di una politica aziendale per l'approvazione di nuovi prodotti (New Product Approval Policy, NPAP) ben documentata, approvata dall'organo di amministrazione, che fa fronte allo sviluppo di nuovi mercati, prodotti e servizi e alle modifiche rilevanti apportate a quelli esistenti, nonché alle operazioni straordinarie. La politica dovrebbe, inoltre, includere le modifiche sostanziali apportate ai relativi processi (ad esempio nuovi dispositivi di esternalizzazione) e sistemi (ad esempio i processi delle modifiche 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 di rischio e la propensione al rischio dell'ente nonché con i limiti corrispondenti, o che vengano effettuate le necessarie revisioni.

148. 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 esempio nuove filiazioni o società costituite ad hoc (*single purpose vehicles*]; nuovi prodotti; modifiche ai sistemi o al quadro o alle procedure di gestione dei rischi; e cambiamenti intervenuti nell'organizzazione dell'ente.

149. 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

[24] Cfr. inoltre 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.

valutazione preventiva sistematica e un parere documentato da parte della funzione di conformità per i nuovi prodotti o per le modifiche significative ai prodotti esistenti.

150. 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, avviare un nuovo servizio o apportare modifiche significative 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 significative» da utilizzare nell'organizzazione e indicare le funzioni interne da coinvolgere nel processo decisionale.

151. 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 quantificazione del rischio, l'impatto sul profilo di rischio, l'adeguatezza patrimoniale e la redditività, la disponibilità di risorse adeguate per le attività di «front-office», «back-office» e «middle-office» e la disponibilità di adeguati strumenti interni e competenze per la comprensione e il monitoraggio dei rischi associati. La decisione di avviare una nuova attività dovrebbe indicare chiaramente l'unità operativa e le persone che ne sono responsabili. Nessuna nuova attività dovrebbe essere avviata fino a quando non siano disponibili risorse adeguate per comprendere e gestire i rischi associati.

152. La funzione di gestione dei rischi e la funzione di conformità dovrebbero partecipare all'approvazione dei nuovi prodotti o delle modifiche significative ai prodotti, processi e sistemi esistenti. Il loro contributo dovrebbe prevedere una valutazione esaustiva e oggettiva dei rischi derivanti da nuove attività in diverse ipotesi di scenario, 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 significative 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

153. Le funzioni di controllo interno dovrebbero includere una funzione di gestione dei rischi (cfr. la sezione 20), una funzione di conformità (cfr. la sezione 21) e una funzione di audit interno (cfr. la sezione 22). Le funzioni di gestione dei rischi e di conformità dovrebbero essere soggette a riesame da parte della funzione di audit interno.

154. 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, parzialmente o completamente, il responsabile della funzione di controllo interno interessata e l'organo di

amministrazione restano responsabili di tali attività e del mantenimento di una funzione di controllo interno nell'ente.

19.1 Responsabili delle funzioni di controllo interno

155. 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 amministrazione, i responsabili delle funzioni di controllo interno dovrebbero essere indipendenti dalle linee di business o dalle unità che controllano. A tal fine, i responsabili delle funzioni di gestione dei rischi, di conformità e di audit interno dovrebbero riferire ed essere direttamente responsabili dinnanzi all'organo di amministrazione, e le loro prestazioni dovrebbero essere esaminate dall'organo di amministrazione.

156. Laddove necessario, i responsabili delle funzioni di controllo interno dovrebbero poter accedere e riferire direttamente all'organo di amministrazione nella sua funzione di supervisione strategica, al fine di sollevare dubbi e informare la funzione di supervisione strategica, laddove necessario, in presenza di evoluzioni specifiche che interessino 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.

157. 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, il responsabile delle funzioni di controllo interno non dovrebbe (e, in conformità dell'articolo 76, paragrafo 5, della direttiva 2013/36/UE, il responsabile della funzione di gestione dei rischi non deve) essere deposto senza previa approvazione dell'organo di amministrazione nella sua funzione di supervisione strategica. Negli enti rilevanti, le autorità competenti dovrebbero essere prontamente informate dell'approvazione e delle principali ragioni della destituzione di un responsabile di una funzione di controllo interno.

19.2 Indipendenza delle funzioni di controllo interno

158. 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, sono separate dalle attività che sono tenute a monitorare e controllare;

c. fatta salva la responsabilità generale dei membri dell'organo di amministrazione 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; e

d. la remunerazione del personale preposto alla funzione di controllo interno non dovrebbe essere associata alle prestazioni delle attività che la funzione di controllo interno monitora e controlla, né ad altro che ne possa compromettere l'obiettività[25].

19.3 Combinazione delle funzioni di controllo interno

159. Tenendo conto dei criteri di proporzionalità enunciati 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

160. Le funzioni di controllo interno dovrebbero disporre di risorse sufficienti. Dovrebbero disporre di un numero adeguato di personale qualificato (a livello sia d'impresa madre sia di filiazioni). Il personale dovrebbe mantenere costantemente aggiornate le proprie qualifiche e ricevere la formazione necessaria.

161. 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. 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

162. 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 sufficiente autorità, peso e risorse, tenendo conto dei criteri di proporzionalità elencati nel titolo I, per attuare politiche in materia di rischio e il quadro di gestione dei rischi, come stabilito alla sezione 17.

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

164. 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.

[25] 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.

165. Il personale all'interno 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 regolari formazioni.

166. 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 responsabilizzazione rispetto alla gestione dei rischi presso tutto il personale dell'ente.

167. 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.

168. Gli enti rilevanti 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 un gruppo di funzione di gestione dei rischi nell'ente consolidante, per fornire 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.

169. La funzione di gestione dei rischi dovrebbe fornire informazioni, analisi e pareri di specialisti sull'esposizione ai rischi 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 amministrazione se queste siano conformi alla propensione al rischio e alla strategia in materia di 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 operativi in materia di rischi.

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

170. La funzione di gestione dei rischi dovrebbe partecipare attivamente nelle fasi iniziali a stendere una strategia in materia di rischio dell'ente e a garantire che l'ente disponga di processi efficaci di gestione dei rischi. La funzione di gestione dei rischi dovrebbe fornire all'organo di amministrazione tutte le informazioni 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 di rischio e della propensione al rischio. Dovrebbe garantire che la propensione al rischio trovi debito riscontro nei limiti di rischio specifici. La funzione di gestione dei rischi dovrebbe anche valutare le strategie in materia di rischio delle unità operative, inclusi gli obiettivi proposti dalle unità operative ed essere

coinvolta prima che una decisione sulle strategie in materia di rischio venga presa da parte dell'organo di amministrazione. Gli obiettivi dovrebbero essere plausibili e in linea con la strategia dell'ente in materia di rischio.

171. 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 amministrazione.

20.2 Ruolo della funzione di gestione dei rischi nelle modifiche sostanziali

172. In linea con la sezione 18, prima di prendere 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 amministrazione, prima che sia presa una decisione.

173. 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 propria base di capitale solida 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

174. La funzione di gestione dei rischi dovrebbe garantire che tutti i rischi siano individuati, valutati, misurati, monitorati, gestiti e debitamente segnalati da parte delle unità interessate dell'ente.

175. 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 e tener conto anche di approcci qualitativi. La funzione di gestione dei rischi dovrebbe tener informato l'organo di amministrazione in merito alle ipotesi utilizzate nei modelli e nelle analisi di rischio, nonché alle eventuali lacune.

176. 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.

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

178. La funzione di gestione dei rischi dovrebbe monitorare regolarmente il profilo di rischio reale dell'ente e valutarlo rispetto agli obiettivi strategici e alla propensione per il rischio dello stesso al fine di consentire all'organo di amministrazione di adottare decisioni nell'esercizio della funzione di gestione e di verificarle nell'esercizio della funzione di supervisione strategica.

179. La funzione di gestione dei rischi dovrebbe analizzare gli andamenti 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 reali 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.

180. La funzione di gestione dei rischi dovrebbe valutare possibili modalità di mitigazione dei rischi. La segnalazione all'organo di amministrazione dovrebbe includere una proposta adeguata di azioni intese a mitigare il rischio.

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

181. La funzione di gestione dei rischi dovrebbe valutare in maniera indipendente le violazioni o i limiti della propensione al rischio (fra cui l'accertamento della causa e l'esecuzione di un'analisi giuridica ed economica dei costi di eliminazione effettivi, 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 amministrazione e raccomandare possibili misure correttive. La funzione di gestione dei rischi dovrebbe segnalare direttamente eventuali violazioni gravi all'organo di amministrazione nella sua funzione di supervisione strategica, fatta salva la possibilità per la funzione di gestione dei rischi di informare altre funzioni interne e comitati.

182. 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 amministrazione e, laddove istituito, il comitato rischi.

20.5 Responsabile della funzione di gestione dei rischi

183. Il responsabile della funzione di gestione dei rischi dovrebbe avere il compito di fornire informazioni esaurienti e di facile comprensione sui rischi e di consigliare l'organo di amministrazione, consentendo a tale organo 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.

184. Il responsabile della funzione di gestione dei rischi dovrebbe disporre di competenze, indipendenza e anzianità di servizio sufficienti per intervenire nelle 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 amministrazione, gli enti rilevanti 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 amministrazione. Se non è proporzionato nominare una persona che si dedichi soltanto al ruolo di responsabile della funzione di gestione dei rischi, tenendo in considerazione il principio di proporzionalità stabilito al titolo I, tale funzione può essere combinata con quella di responsabile della funzione di conformità o può essere esercitata da un'altra persona esperta, 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 esempio il responsabile dell'ufficio legale).

185. Il responsabile della funzione di gestione dei rischi dovrebbe essere in grado di intervenire nelle decisioni prese dalla gestione dell'ente e dal relativo organo di amministrazione; le ragioni delle obiezioni dovrebbero essere formalmente documentate. Se un ente intende concedere al responsabile della funzione di gestione dei rischi il diritto di porre il veto alle decisioni (ad esempio una decisione relativa al credito o a un investimento o la definizione di un limite) prese a un livello inferiore rispetto all'organo di amministrazione, dovrebbe specificare la portata di tale veto, le procedure di segnalazione o di appello e le modalità di partecipazione dell'organo di amministrazione.

186. 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 amministrazione, 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 propensione al rischio e alla strategia in materia di rischio dell'ente.

21 Funzione di conformità

187. Gli enti dovrebbero istituire una funzione di conformità permanente ed efficace per gestire i rischi 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).

188. Se non è proporzionato nominare una persona che si dedichi soltanto al ruolo di responsabile della conformità tenendo in considerazione il principio di proporzionalità stabilito 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 esperta (ad esempio il responsabile dell'ufficio legale), a condizione che non ci sia alcun conflitto di interesse tra le funzioni combinate.

189. La funzione di conformità, incluso il responsabile della conformità, dovrebbe essere indipendente dalle linee di business e dalle unità interne che controlla e disporre di autorità, peso e risorse sufficienti. Tenendo conto dei criteri di proporzionalità stabiliti 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 la divisione degli affari giuridici o il dipartimento risorse umane.

190. 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 formazioni periodiche.

191. L'organo di amministrazione nella sua funzione di supervisione strategica dovrebbe sorvegliare l'attuazione di politiche di conformità ben documentate, che dovrebbero essere comunicate 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.

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

193. 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 amministrazione e comunicare, se del caso, 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 opportune per svolgere i rispettivi compiti. I risultati dell'attività della funzione di conformità dovrebbero essere tenuti in considerazione dall'organo di amministrazione e dalla funzione di gestione dei rischi nell'ambito dei processi decisionali.

194. 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'unità degli affari giuridici, che i nuovi prodotti e le nuove procedure rispettino l'attuale quadro normativo e, se del caso, qualunque modifica imminente della legislazione, dei regolamenti e degli obblighi di vigilanza.

195. Gli enti dovrebbero adottare misure adeguate nei confronti di comportamenti fraudolenti interni ed esterni e di violazioni della disciplina (ad esempio violazione delle procedure interne o dei limiti).

196. Gli enti dovrebbero garantire che le loro filiazioni e succursali intraprendano azioni per garantire 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 informarne il preposto alla conformità o il responsabile della conformità dell'ente consolidante.

22 Funzione di audit interno

197. Gli enti dovrebbero istituire una funzione di audit interno indipendente ed efficace, tenendo conto dei criteri di proporzionalità stabiliti 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 sufficienti. In particolare, l'ente dovrebbe garantire che la qualifica degli addetti 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.

198. 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.

199. 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 esterni. Ciascuna entità all'interno del gruppo dovrebbe rientrare nella sfera di competenza della funzione di audit interno.

200. 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 limiti di rischio. Tuttavia, ciò non dovrebbe impedire all'organo di amministrazione, nella sua funzione di gestione, di richiedere un contributo dall'audit interno su questioni legate al rischio, ai controlli interni e alla conformità alle norme applicabili.

201. La funzione di audit interno dovrebbe valutare se il quadro di controllo interno dell'ente sia efficiente ed efficace, secondo quanto stabilito alla sezione 15. 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 propensione al rischio e alla strategia in materia di rischio dell'ente;

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

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

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

202. La funzione di audit interno dovrebbe verificare, in particolare, l'integrità dei processi che garantiscono l'affidabilità dei metodi e delle tecniche, delle ipotesi e delle fonti di informazioni utilizzati dall'ente nei modelli interni (ad esempio la modellazione dei rischi e le misurazioni contabili). Essa dovrebbe anche valutare la qualità e l'uso di strumenti qualitativi di individuazione e valutazione dei rischi e le misure di mitigazione del rischio adottate.

203. 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 della gestione e ai verbali di tutti i comitati e organi decisionali.

204. La funzione di audit interno dovrebbe rispettare gli standard professionali nazionali e internazionali. Un esempio di standard professionali cui si fa riferimento nel testo sono gli standard stabiliti dall'Institute of Internal Auditors.

205. 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.

206. 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 amministrazione.

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

Titolo VI. Gestione della continuità operativa

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

209. Gli enti possono istituire una funzione di continuità operativa indipendente specifica, ad esempio come parte della funzione di gestione dei rischi[26].

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

[26] Si rimanda anche all'articolo 312 del regolamento (UE) n. 575/2013.

211. Al fine di stabilire un piano efficace di gestione della continuità operativa, un ente dovrebbe analizzare attentamente la propria esposizione a gravi interruzioni delle attività 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 ripresa dell'ente.

212. 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 critiche in caso di interruzione delle proprie procedure operative ordinarie; e

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

213. I piani di emergenza, di continuità operativa e di risanamento 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

214. Gli indirizzi strategici, le politiche e le procedure dovrebbero essere comunicati 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 attenervisi.

215. Di conseguenza, l'organo di amministrazione dovrebbe informare e aggiornare in maniera chiara e coerente il personale interessato in merito agli indirizzi strategici 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.

216. Se alle imprese madri è 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[27], per paese.

217. 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 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 amministrazione, incluso il numero dei relativi membri e il numero dei membri indipendenti, e che specifichino il sesso e la durata del mandato di ciascun membro dell'organo di amministrazione;

e. le responsabilità principali dell'organo di amministrazione;

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

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

h. una panoramica del quadro di controllo interno; e

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

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 nella documentare le politiche e i dispositivi di governance interna:

[27] 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).

1. struttura azionaria
2. struttura del gruppo, se applicabile (struttura giuridica e di funzionamento)
3. composizione e funzionamento dell'organo di amministrazione
   a) criteri di selezione
   b) numero, durata del mandato, rotazione, età
   c) membri indipendenti dell'organo di amministrazione
   d) membri esecutivi dell'organo di amministrazione
   e) membri non esecutivi dell'organo di amministrazione
   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. titolari di funzioni 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) altri titolari di funzioni chiave
6. il quadro di controllo interno
   a) descrizione di ciascuna funzione, inclusa l'organizzazione, le risorse, il peso e l'autorità
   b) descrizione del quadro di gestione dei rischi, inclusa la strategia in materia di rischio
7. Struttura organizzativa (con impatto sul gruppo, se applicabile)
   a) struttura organizzativa, linee di business e attribuzione delle competenze e delle responsabilità
   b) esternalizzazione
   c) gamma di prodotti e servizi
   d) portata geografica dell'attività
   e) prestazione gratuita di servizi
   f) succursali
   g) filiazioni, joint venture, ecc.

h) utilizzo di centri offshore

8. codice etico 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 di gestione del conflitto di interesse
   d) denuncia di irregolarità
9. stato della politica di governance interna, corredato di data
   a) sviluppo
   b) ultima modifica
   c) ultima valutazione
   d) approvazione da parte dell'organo di amministrazione.