

Orientamenti

sui controlli interni per gli amministratori di indici di riferimento, le agenzie di rating del credito e le infrastrutture per la trasparenza del mercato

Indice

1	Ambito di applicazione	4
2	Riferimenti normativi, abbreviazioni e definizioni	8
2.1	Riferimenti normativi	8
2.2	Abbreviazioni	9
2.3	Definizioni	10
3	Finalità.....	11
4	Obblighi di conformità e comunicazione	11
4.1	Status degli orientamenti	11
4.2	Obblighi di comunicazione	11
5	Orientamenti sui controlli interni.....	13
5.1	Quadro di controllo interno.....	13
	Componente 1.1 Ambiente di controllo	13
	Componente 1.2 Gestione del rischio	14
	Componente 1.3 Attività di controllo	15
	Componente 1.4 Informazione e comunicazione	17
	Componente 1.5 Attività di monitoraggio	18
5.2	Funzioni di controllo interno	19
	Proporzionalità – Funzioni di controllo interno	20
	Componente 2.1 Funzione di controllo della conformità	21
	Componente 2.2 Funzione di gestione dei rischi.....	22
	Componente 2.3 Funzione di gestione della sicurezza delle informazioni (solo per le entità sottoposte a vigilanza non soggette a DORA).....	23
	Componente 2.4 Funzione di audit interno	24
	Componente 2.5 Funzione di revisione (solo per le CRA)	25
	Componente 2.6 Funzione di sorveglianza (solo per i BMA) ().....	25

1 Ambito di applicazione

Destinatari

1. I presenti orientamenti si applicano:

- i) agli amministratori di indici di riferimento autorizzati, registrati o riconosciuti presso l'ESMA (denominati collettivamente «BMA») conformemente al regolamento sugli indici di riferimento (BMR);
- ii) alle agenzie di rating del credito stabilite nell'Unione e registrate presso l'ESMA conformemente al regolamento sulle agenzie di rating del credito (CRAR);
- iii) ai fornitori di servizi di comunicazione dati [esclusi i fornitori di un sistema consolidato di pubblicazione (CTP)] stabiliti nell'Unione e autorizzati dall'ESMA (DRSP) conformemente al regolamento sui mercati degli strumenti finanziari (MiFIR);
- iv) ai repertori di dati sulle cartolarizzazioni stabiliti nell'Unione e registrati presso l'ESMA conformemente al regolamento sulle cartolarizzazioni (SecR);
- v) ai repertori di dati sulle negoziazioni stabiliti nell'Unione e registrati presso l'ESMA conformemente al regolamento sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (EMIR);
- vi) ai repertori di dati sulle negoziazioni stabiliti nell'Unione e registrati presso l'ESMA conformemente al regolamento sulle operazioni di finanziamento tramite titoli (SFTR) (di seguito denominati collettivamente «entità sottoposte a vigilanza»).

Oggetto

2. I presenti orientamenti riguardano gli aspetti relativi alla struttura e ai meccanismi di controllo interno necessari per assicurare: i) l'effettiva conformità da parte di un BMA agli articoli da 4 a 10 del BMR; ii) l'effettiva conformità da parte di un'agenzia di rating del credito (CRA) all'articolo 6, paragrafi 1, 2 e 4, all'articolo 9 e all'allegato I, sezione A, del CRAR; iii) l'effettiva conformità da parte di un DRSP agli articoli 27 *septies*, 27 *octies*, 27 *decies* del MiFIR; e iv) l'effettiva conformità da parte di un repertorio di dati sulle negoziazioni (TR) o di un repertorio di dati sulle cartolarizzazioni (SR) agli articoli 78 e 79 dell'EMIR.

Tempistica

3. I presenti orientamenti si applicano a partire dal 1° ottobre 2026.
4. A decorrere dalla data di cui al paragrafo 3, gli Orientamenti sul controllo interno delle agenzie di rating del credito (ESMA33-9-371) sono abrogati.

2 Riferimenti normativi, abbreviazioni e definizioni

2.1 Riferimenti normativi

BMR	Regolamento (UE) 2016/1011 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sugli indici usati come indici di riferimento negli strumenti finanziari e nei contratti finanziari o per misurare la performance di fondi di investimento e recante modifica delle direttive 2008/48/CE e 2014/17/UE e del regolamento (UE) n. 596/2014 ⁽¹⁾ .
CRAR	Regolamento (CE) n. 1060/2009 del Parlamento europeo e del Consiglio, del 16 settembre 2009, relativo alle agenzie di rating del credito ⁽²⁾ .
DORA	Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 ⁽³⁾ .
EMIR	Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni ⁽⁴⁾ .
MiFIR	Regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 ⁽⁵⁾ .
SecR	Regolamento (UE) 2017/2402 del Parlamento europeo e del Consiglio, del 12 dicembre 2017, che stabilisce un quadro generale per la cartolarizzazione, instaura un quadro specifico per cartolarizzazioni semplici, trasparenti e standardizzate e modifica le direttive 2009/65/CE, 2009/138/CE e 2011/61/UE e i regolamenti (CE) n. 1060/2009 e (UE) n. 648/2012 ⁽⁶⁾ .
SFTR	Regolamento (UE) 2015/2365 del Parlamento europeo e del Consiglio, del 25 novembre 2015, sulla trasparenza delle

⁽¹⁾ GU L 171 del 29.6.2016, pag. 1.

⁽²⁾ GU L 302 del 17.11.2009, pag. 1.

⁽³⁾ GU L 333 del 27.12.2022, pag. 1.

⁽⁴⁾ GU L 201 del 27.7.2012, pag. 1.

⁽⁵⁾ GU L 173 del 12.6.2014, pag. 84.

⁽⁶⁾ GU L 347 del 28.12.2017, pag. 35.

operazioni di finanziamento tramite titoli e del riutilizzo e che modifica il regolamento (UE) n. 648/2012 ⁽⁷⁾.

2.2 Abbreviazioni

APA	Dispositivo di pubblicazione autorizzato
ARM	Meccanismo di segnalazione autorizzato
BMA	Amministratore di indici di riferimento
CRA	Agenzia di rating del credito
DC	Documento di consultazione
DORA	Regolamento sulla resilienza operativa digitale
DRSP	Fornitore di servizi di comunicazione dati
ESMA	Autorità europea degli strumenti finanziari e dei mercati
Funzione CI	Funzione di controllo interno
IA	Intelligenza artificiale
IG	Informazioni sulla gestione
INED	Amministratore indipendente senza incarico esecutivo
NTR	Norme tecniche di regolamentazione
Quadro CI	Quadro di controllo interno
SR	Repertorio di dati sulle cartolarizzazioni
TIC	Tecnologie dell'informazione e della comunicazione
TR	Repertorio di dati sulle negoziazioni
UE	Unione europea

⁽⁷⁾ GU L 337 del 23.12.2015, pag. 1.

2.3 Definizioni

Alta dirigenza esecutiva	<p>Si riferisce alle persone di grado più alto che dirigono quotidianamente l'entità sottoposta a vigilanza. Si tratta in genere dell'amministratore delegato (CEO), o di una figura equivalente, e dei suoi subordinati diretti.</p>
Entità sottoposte a vigilanza	<p>Ai fini dei presenti orientamenti, ciò si riferisce ai soggetti che rientrano nel mandato di vigilanza dell'ESMA, vale a dire:</p> <ul style="list-style-type: none"> ▪ BMA; ▪ CRA; ▪ DRSP (esclusi i fornitori di un sistema consolidato di pubblicazione); ▪ SR; ▪ TR.
Infrastrutture per la trasparenza del mercato	<p>Ai fini dei presenti orientamenti, ciò si riferisce a quanto segue:</p> <ul style="list-style-type: none"> ▪ fornitori di servizi di comunicazione dati; ▪ repertori di dati sulle cartolarizzazioni e ▪ repertori di dati sulle negoziazioni.
Organo di gestione	<p>L'organo – o gli organi – designato conformemente al diritto nazionale, cui è conferito il potere di stabilire gli indirizzi strategici, gli obiettivi e la direzione generale dell'entità, che supervisiona e monitora le decisioni della dirigenza e comprende persone che dirigono di fatto l'attività dell'entità.</p> <p>Si tratta degli organi direttivi di rango più elevato all'interno di un'organizzazione.</p> <p>Il termine è definito nel BMR, articolo 3, paragrafo 1, punto 20, e nel MiFIR, articolo 2, paragrafo 1, punto 22.</p> <p>Rientrano i concetti di:</p> <ul style="list-style-type: none"> ▪ «consiglio di amministrazione o di sorveglianza», di una CRA, appartenente all'«alta dirigenza», secondo la definizione di cui all'articolo 3, paragrafo 1, punto n), del regolamento sulle agenzie di rating del credito; ▪ «consiglio di amministrazione o di sorveglianza, o entrambi, conformemente al diritto societario nazionale», secondo la definizione di cui all'articolo 2, paragrafo 27, dell'EMIR.
Regolamenti pertinenti	<p>Ai fini dei presenti orientamenti, ciò si riferisce a quanto segue:</p> <ul style="list-style-type: none"> ▪ BMR;

- CRAR;
- EMIR;
- MiFIR;
- SecR;
- SFTR.

3 Finalità

5. I presenti orientamenti definiscono le aspettative dell'ESMA in merito alle componenti e alle caratteristiche di un quadro di controllo interno efficace e alle funzioni dei diversi controlli interni all'interno di un'entità sottoposta a vigilanza.

4 Obblighi di conformità e comunicazione

4.1 Status degli orientamenti

6. Il presente documento contiene orientamenti emanati ai sensi dell'articolo 16 del regolamento ESMA. Ai sensi dell'articolo 16, paragrafo 3, del regolamento ESMA, le entità sottoposte a vigilanza devono compiere ogni sforzo per conformarsi ai presenti orientamenti.

4.2 Obblighi di comunicazione

7. I partecipanti ai mercati finanziari ai quali si applicano i presenti orientamenti non sono tenuti a comunicare se si conformano a questi ultimi. L'ESMA valuterà l'applicazione dei presenti orientamenti da parte delle entità sottoposte a vigilanza tramite la vigilanza e il monitoraggio costanti delle loro attività.
8. Ai fini dell'applicazione dei presenti orientamenti, l'ESMA applicherà il principio di proporzionalità. Sebbene tutte le entità sottoposte a vigilanza siano tenute a dimostrare di possedere le componenti e le caratteristiche di un sistema di controllo interno efficace descritte nei presenti orientamenti, l'ESMA calibrerà le proprie aspettative di cui alla sezione 4.2 in base alla natura, alla dimensione, alla complessità e al profilo di rischio complessivo di un'entità sottoposta a vigilanza e in funzione del modo in cui tali caratteristiche possono influire sulla tutela degli investitori, sul regolare funzionamento del mercato e sulla stabilità finanziaria.

9. Nel valutare la natura di un'entità sottoposta a vigilanza, l'ESMA prenderà in considerazione l'attività e il tipo di operazioni di tale entità, compresi il suo ruolo/la sua missione di mercato, il tipo, la diversità e la criticità dei prodotti e dei servizi offerti dall'entità sottoposta a vigilanza.
10. Nel valutare la dimensione dell'attività di un'entità sottoposta a vigilanza, l'ESMA terrà conto di fattori rilevanti quali il numero di dipendenti, il fatturato, il numero di clienti e di prodotti, la quota di mercato, le interconnessioni con altri settori/altre infrastrutture, i servizi accessori e la loro relazione con i servizi principali, nonché altri fattori specifici relativi alla dimensione e all'impatto sul mercato dell'entità sottoposta a vigilanza.
11. Nel valutare la complessità di un'entità sottoposta a vigilanza, l'ESMA terrà conto, tra gli altri fattori, della sua struttura organizzativa e delle sue modalità operative (struttura/relazioni del gruppo, servizi condivisi, esternalizzazione ecc.), nonché delle sue caratteristiche operative in relazione a persone, processi, tecnologia, offerta di prodotti e interconnessioni.
12. Nel calibrare le proprie aspettative, l'ESMA tiene conto delle condizioni della registrazione o del riconoscimento di un'entità sottoposta a vigilanza. La natura, la dimensione e la complessità di un'entità sottoposta a vigilanza possono cambiare dopo la registrazione o il riconoscimento ed è sua responsabilità garantire che i suoi controlli interni siano commisurati alla natura, alla dimensione e alla complessità della stessa. L'ESMA comunicherà, nell'ambito della propria attività di vigilanza, se le aspettative di cui alle sezioni 5.1 e 5.2 sono più elevate rispetto a quelle stabilite al momento della registrazione o del riconoscimento.

5 Orientamenti sui controlli interni

13. Al fine di dimostrare che le entità sottoposte a vigilanza si conformano al paragrafo 2 dei presenti orientamenti, queste dovrebbero dimostrare che le loro politiche, procedure e prassi di lavoro conseguono gli obiettivi di cui alle sezioni **5.1** (Quadro di controllo interno) e **5.2** (Funzioni di controllo interno) dei presenti orientamenti.

5.1 Quadro di controllo interno

14. Per garantire un quadro CI efficace, le entità sottoposte a vigilanza dovrebbero dotare le proprie politiche, procedure e prassi di lavoro delle componenti e caratteristiche indicate di seguito.

Principi generali

15. L'organo di gestione dell'entità sottoposta a vigilanza dovrebbe essere responsabile della supervisione e dell'approvazione di tutte le componenti del quadro CI, oltre ad assicurare che dette componenti siano oggetto di monitoraggio e di aggiornamento periodico da parte dell'alta dirigenza esecutiva. Dovrebbe spettare all'alta dirigenza esecutiva dell'entità sottoposta a vigilanza creare, attuare e aggiornare le politiche, le procedure e le prassi scritte riguardanti il controllo interno a sostegno delle componenti del quadro CI.
16. Al fine di porre in essere tali politiche e procedure, un'entità sottoposta a vigilanza dovrebbe prevedere un processo decisionale chiaro, trasparente e documentato nonché una chiara ripartizione dei ruoli e delle responsabilità nell'ambito del quadro CI, comprese le sue aree di attività e le sue funzioni CI.

Componente 1.1 Ambiente di controllo

17. L'organo di gestione e l'alta dirigenza esecutiva di un'entità sottoposta a vigilanza contribuiscono entrambi a dare il massimo risalto all'importanza del controllo interno. L'alta dirigenza esecutiva è responsabile di definire ed eseguire il controllo interno nonché di valutare l'adeguatezza e l'efficacia dell'ambiente di controllo. In tali ambiti, l'organo di gestione dovrebbe esercitare una sorveglianza sull'alta dirigenza esecutiva.

Caratteristiche

- 1.1.1** L'alta dirigenza esecutiva dell'entità sottoposta a vigilanza dovrebbe avere la responsabilità di creare una solida cultura dell'etica e della conformità all'interno dell'entità sottoposta a vigilanza attuando politiche e procedure che disciplinano il comportamento del personale della suddetta entità.

- 1.1.2** L'alta dirigenza esecutiva dell'entità sottoposta a vigilanza dovrebbe avere la responsabilità di assicurare che le politiche e le procedure di quest'ultima:
- i. specificino che l'attività dell'entità sottoposta a vigilanza dovrebbe essere condotta conformemente ai regolamenti pertinenti e ai valori aziendali dell'entità sottoposta a vigilanza;
 - ii. chiariscano che, oltre a ottemperare a requisiti di natura legale e regolamentare nonché a politiche interne, il personale è chiamato a comportarsi in modo onesto e integro e a svolgere i propri compiti con la dovuta competenza, cura e diligenza; e
 - iii. garantiscano che il personale sia consapevole delle potenziali azioni disciplinari interne ed esterne, delle azioni legali e delle sanzioni che possono scaturire da condotte illecite.
- 1.1.3** L'alta dirigenza esecutiva dell'entità sottoposta a vigilanza dovrebbe creare, mantenere e aggiornare periodicamente e per iscritto politiche, procedure e meccanismi di controllo interno adeguati.
- 1.1.4** L'alta direzione esecutiva dell'entità sottoposta a vigilanza dovrebbe mantenere la responsabilità delle attività esternalizzate a fornitori di servizi esterni o delegate a partner commerciali.

Componente 1.2 Gestione del rischio

18. Ai fini di una gestione del rischio efficace, le entità sottoposte a vigilanza dovrebbero garantire di disporre di un processo dinamico e in continua evoluzione per identificare, valutare e misurare tutti i rischi che potrebbero influire sulla capacità di una tale entità di adempiere ai propri obblighi derivanti dai regolamenti pertinenti o sulla sua continuità operativa. Sono inclusi, ad esempio, i rischi derivanti dall'utilizzo di nuove tecnologie da parte dell'entità sottoposta a vigilanza e i cambiamenti nel panorama esterno dei rischi. Il processo dovrebbe consentire all'entità sottoposta a vigilanza di monitorare, gestire, attenuare e adeguatamente segnalare i rischi rilevanti per il conseguimento di tali obiettivi.

Caratteristiche

- 1.2.1** L'entità sottoposta a vigilanza dovrebbe svolgere le valutazioni interne del rischio conformemente a una metodologia di valutazione del rischio ben definita e completa.
- 1.2.2** L'entità sottoposta a vigilanza dovrebbe stabilire la propria propensione al rischio e individuare i livelli di tolleranza al rischio.

- 1.2.3** La metodologia di valutazione del rischio dell'entità sottoposta a vigilanza dovrebbe comprendere tutte le aree di attività e le funzioni CI dell'entità sottoposta a vigilanza.
- 1.2.4** Il processo di valutazione del rischio dell'entità sottoposta a vigilanza dovrebbe identificare e valutare i cambiamenti che potrebbero avere un impatto significativo sul sistema di controllo interno. Ciò comprende modifiche dell'ambiente, dell'organizzazione, delle attività e delle operazioni.
- 1.2.5** La metodologia di valutazione del rischio dell'entità sottoposta a vigilanza dovrebbe essere soggetta a evoluzione e miglioramento costanti.

Componente 1.3 Attività di controllo

19. Le attività di controllo dovrebbero avere natura preventiva, investigativa, correttiva o dissuasiva.

Caratteristiche

- 1.3.1** *Separazione delle funzioni* – L'entità sottoposta a vigilanza dovrebbe garantire un'adeguata separazione delle funzioni per gestire i rischi di conflitti di interessi, frode ed errore umano. La separazione delle funzioni dovrebbe garantire che i membri del personale responsabili dell'esecuzione di un compito non siano gli unici responsabili dell'approvazione dell'esito della sua esecuzione. In particolare, i membri del personale responsabili dello sviluppo, dell'attuazione o dell'approvazione di un compito/lavoro non sono gli unici responsabili della sua convalida, valutazione e revisione ⁽⁸⁾. Laddove ciò non sia evitabile, è opportuno mitigare i rischi evitando che i membri del personale siano gli unici responsabili dell'attività ⁽⁹⁾.
- 1.3.2** *Documentazione* – L'entità sottoposta a vigilanza dovrebbe documentare le proprie politiche e procedure riguardanti tutti i settori delle attività soggette alle disposizioni dei regolamenti pertinenti.

⁽⁸⁾ Ad esempio, i membri del personale responsabili delle attività di sviluppo del sistema non dovrebbero essere coinvolti nell'amministrazione delle banche dati, nelle operazioni informatiche, nell'amministrazione e nella manutenzione dei sistemi informatici e della rete. Per le CRA, i) le persone che effettuano l'analisi di un rating del credito non dovrebbero essere le uniche responsabili dell'approvazione del rating stesso; ii) le persone responsabili dello sviluppo delle metodologie di rating del credito non dovrebbero essere le uniche responsabili della loro approvazione; iii) le persone responsabili della convalida, della valutazione o della revisione di una metodologia di rating del credito non dovrebbero essere le uniche responsabili dell'approvazione della convalida, della valutazione o della revisione.

⁽⁹⁾ Ad esempio, mediante un controllo da parte di una seconda persona.

- 1.3.3** *Controlli documentati e verifica dei controlli* – L’entità sottoposta a vigilanza dovrebbe documentare i controlli essenziali posti in essere per assicurare l’osservanza delle politiche e delle procedure istituite ai sensi dei regolamenti pertinenti.
- 1.3.4** *Designazione delle responsabilità* – L’entità sottoposta a vigilanza dovrebbe designare in modo chiaro e ben definito i ruoli o le funzioni responsabili di effettuare i controlli relativi agli obblighi derivanti dai regolamenti pertinenti e specificarne i rispettivi compiti e responsabilità. A tal fine, l’entità sottoposta a vigilanza dovrebbe distinguere i controlli essenziali di routine a livello di attività da quelli effettuati dalle funzioni di controllo specifiche.
- 1.3.5** *Autorizzazioni e approvazioni* – L’entità sottoposta a vigilanza dovrebbe disporre di processi o meccanismi di autorizzazione per garantire che solo le persone autorizzate abbiano accesso a informazioni e strumenti in base al principio della «necessità di sapere» e al principio del privilegio minimo. L’entità sottoposta a vigilanza dovrebbe inoltre disporre di processi o meccanismi in tutte le attività per garantire che tali attività siano autorizzate ed eseguite solo da membri del personale che agiscono nell’ambito di competenza della propria autorità (10).
- 1.3.6** *Verifiche, convalide, riconciliazioni e riesami* – L’entità sottoposta a vigilanza dovrebbe adottare misure atte a individuare e contrastare tempestivamente attività inopportune, non autorizzate, errate o fraudolente (11).
- 1.3.7** *Controlli generali relativi alle tecnologie dell’informazione e della comunicazione (TIC)* (solo per le entità sottoposte a vigilanza non soggette a DORA) – L’entità sottoposta a vigilanza dovrebbe attuare strategie, politiche e procedure che garantiscano la resilienza operativa digitale dei sistemi TIC di tale entità a sostegno dei processi operativi dell’entità sottoposta a vigilanza.

L’entità sottoposta a vigilanza dovrebbe definire i propri controlli e le proprie soluzioni TIC in modo proporzionato. Pertanto, i controlli relativi alle TIC varieranno da un’organizzazione all’altra a seconda della natura, della portata e della complessità dei processi operativi sottostanti e delle funzioni pertinenti supportate da tali sistemi.

⁽¹⁰⁾ Ad esempio, per le CRA, solo le persone designate come responsabili dei rispettivi compiti dovrebbero svolgere il processo di rating del credito, la convalida delle metodologie e la revisione dei risultati della convalida.

⁽¹¹⁾ Ciò comprende la convalida dei dati e i controlli dei dati inseriti, la revisione degli elenchi per l’accesso autorizzato alle informazioni riservate. Per le agenzie di rating del credito, tali controlli si applicano alle attività di rating del credito e ai processi alla base di tali attività, quali la convalida della metodologia/del modello di credito.

Le entità sottoposte a vigilanza dovrebbero assicurare di disporre di controlli sufficienti a garantire la qualità dei dati, in termini di disponibilità, riservatezza e integrità degli stessi, tra cui la convalida, i controlli sul trattamento e le procedure di controllo dei file di dati.

L'entità sottoposta a vigilanza dovrebbe istituire un opportuno sistema di gestione della sicurezza delle informazioni e le relative attività di controllo. In questo contesto, un'entità sottoposta a vigilanza dovrebbe stabilire i controlli necessari per garantire l'autenticità, la riservatezza, l'integrità e la disponibilità delle informazioni durante il loro trattamento dalla fonte all'utente finale.

L'entità sottoposta a vigilanza dovrebbe stabilire e documentare tutte le attività pertinenti di controllo dei processi di acquisizione, sviluppo e manutenzione delle TIC.

Componente 1.4 Informazione e comunicazione

20. Le entità sottoposte a vigilanza dovrebbero stabilire procedure per la condivisione discendente di informazioni accurate, complete e di buona qualità con il personale e le parti interessate esterne. Le entità sottoposte a vigilanza dovrebbero inoltre stabilire procedure per la comunicazione periodica di informazioni relative al sistema e alle attività di controllo interno all'organo di gestione e all'alta dirigenza esecutiva, comprese le informazioni relative al comportamento e al rispetto dei controlli interni.

Caratteristiche

- 1.4.1** L'entità sottoposta a vigilanza dovrebbe garantire una comunicazione interna ed esterna adeguata, condividendo tempestivamente informazioni accurate, complete e di buona qualità con il mercato, i clienti, gli utenti dei suoi prodotti e servizi e le autorità di regolamentazione.
- 1.4.2** L'entità sottoposta a vigilanza dovrebbe istituire canali di comunicazione ascendente, tra cui una procedura di segnalazione delle irregolarità, affinché le questioni rilevanti del controllo interno siano portate all'attenzione dell'organo di gestione e dell'alta dirigenza esecutiva. L'organo di gestione e l'alta dirigenza esecutiva dovrebbero inoltre ricevere aggiornamenti periodici sul sistema e sulle attività di controllo interno, anche per quanto riguarda la sicurezza delle informazioni. L'entità sottoposta a vigilanza dovrebbe disporre di procedure di attivazione di livelli successivi di intervento in caso di disaccordo sostanziale tra le funzioni CI e le unità operative.
- 1.4.3** L'entità sottoposta a vigilanza dovrebbe istituire canali di comunicazione discendente, dall'organo di gestione, dall'alta dirigenza esecutiva e dalle funzioni di controllo verso il personale. Ciò dovrebbe includere aggiornamenti

periodici sugli obiettivi e sulle responsabilità del controllo interno, la comunicazione in merito ai problemi individuati di conformità o di sicurezza delle informazioni, nonché presentazioni e attività di formazione in materia di politiche e procedure.

Componente 1.5 Attività di monitoraggio

21. Le entità sottoposte a vigilanza dovrebbero garantire di svolgere attività di monitoraggio che consentano di accertare se le componenti del sistema di controllo interno di un'entità sottoposta a vigilanza siano presenti e funzionino in modo efficace.

Caratteristiche

- 1.5.1** L'entità sottoposta a vigilanza dovrebbe garantire l'esecuzione di valutazioni del sistema di controllo interno a diversi livelli aziendali di tale entità, quali le aree di attività, le funzioni di controllo e le funzioni di audit interno o di valutazione indipendente.
- 1.5.2** Le attività di monitoraggio dovrebbero essere definite e condotte in modo tale da consentire all'entità sottoposta a vigilanza di verificare se essa soddisfa i requisiti di natura legale e regolamentare, tra cui il rispetto delle politiche, delle procedure e dei codici di condotta interni. Ciò comprende le politiche e le procedure in materia di sicurezza delle informazioni dell'entità sottoposta a vigilanza.
- 1.5.3** Le valutazioni dei sistemi di controllo interno dovrebbero essere eseguite su base periodica o tematica, o mediante una combinazione di entrambe.
- 1.5.4** Le entità sottoposte a vigilanza dovrebbero integrare nei processi operativi valutazioni continue e adattarle al variare delle condizioni.
- 1.5.5** Le entità sottoposte a vigilanza dovrebbero segnalare le carenze individuate nell'ambito delle valutazioni di monitoraggio e i rimedi necessari all'organo di gestione e all'alta dirigenza esecutiva, che dovrebbero poi monitorare la tempestiva attuazione dell'azione correttiva o delle azioni correttive.
- 1.5.6** In caso di esternalizzazione, l'entità sottoposta a vigilanza dovrebbe assegnare il compito di monitorare i processi operativi esternalizzati a un membro del personale. Le entità sottoposte a vigilanza dovrebbero garantire che al fornitore di servizi siano fornite informazioni sufficienti sugli obiettivi e sulle aspettative di realizzazione e che prima della nomina del fornitore sia effettuata la dovuta diligenza.

5.2 Funzioni di controllo interno

22. Per garantire funzioni CI efficaci, le entità sottoposte a vigilanza dovrebbero includere le componenti e le caratteristiche indicate di seguito nelle loro politiche, procedure e prassi di lavoro.

Principi generali

23. L'ESMA ritiene che le funzioni CI delle entità sottoposte a vigilanza debbano disporre di risorse sufficienti e di personale dotato di competenze adeguate per poter svolgere i propri compiti. Il personale che lavora nelle funzioni CI dovrebbe avere una conoscenza tecnica sufficiente delle attività dell'entità sottoposta a vigilanza e dei rischi associati. Nel caso in cui un'entità sottoposta a vigilanza abbia assegnato i compiti operativi di una funzione CI al livello di gruppo o a una parte esterna, l'ESMA è dell'avviso che tale entità debba conservare la piena responsabilità delle attività della funzione CI esternalizzata. Le entità sottoposte a vigilanza dovrebbero assicurare che il personale incaricato delle funzioni CI dovrebbe essere di grado adeguato per avere l'autorità necessaria ad adempiere alle proprie responsabilità. Ad esempio, i membri del personale incaricati delle funzioni di conformità, gestione del rischio, audit interno, gestione della sicurezza delle informazioni, revisione (per le CRA) e sorveglianza (per i BMA) dovrebbero avere libero accesso e riferire periodicamente all'organo di gestione.

24. Le attività possono essere svolte a livello di gruppo o da altre entità giuridiche nell'ambito di una struttura societaria, purché la struttura del gruppo non ostacoli la capacità dell'organo di gestione di un'entità sottoposta a vigilanza di esercitare il proprio controllo e la capacità dell'alta dirigenza esecutiva di gestire i rischi in modo efficace, o la capacità dell'ESMA di vigilare in modo efficace sull'entità sottoposta a vigilanza. In tutti i casi si applica l'orientamento 1.1.4.

25. Per garantire l'indipendenza delle funzioni CI di un'entità sottoposta a vigilanza, l'ESMA si attende che le entità sottoposte a vigilanza tengano conto dei seguenti principi nello stabilire i ruoli e le responsabilità delle proprie funzioni CI:

- i. le funzioni CI, dal punto di vista organizzativo, dovrebbero essere separate dalle funzioni/attività che sono chiamate a monitorare o sottoporre ad audit o a controllo;
- ii. le funzioni CI non dovrebbero svolgere compiti operativi rientranti nell'ambito delle attività che sono tenute a monitorare o sottoporre ad audit o a controllo;
- iii. il membro del personale incaricato di una funzione CI non dovrebbe riferire a una persona avente la responsabilità di gestire le attività che la funzione CI monitora o sottopone ad audit o a controllo;

26. i membri del personale che adempiono a responsabilità relative alle funzioni CI dovrebbero avere accesso alle pertinenti attività di formazione interna o esterna per garantire che le loro competenze siano adeguate all'esecuzione dei compiti.

Proporzionalità – Funzioni di controllo interno

27. Sebbene tutte le entità sottoposte a vigilanza siano tenute a dimostrare le caratteristiche delle funzioni CI efficaci delineate nei presenti orientamenti, l'ESMA calibra le proprie aspettative in base alla natura, alla dimensione e alla complessità di un'entità sottoposta a vigilanza, come descritto nella sezione 3.4 dei presenti orientamenti.
28. Questa sezione spiega in modo più dettagliato in che modo l'ESMA tiene conto della proporzionalità nella sua attività di vigilanza sulle funzioni CI.

Separazione delle funzioni

29. La separazione delle funzioni dovrebbe essere integrata nello sviluppo delle attività di controllo. Potrebbero tuttavia esservi alcuni casi in cui il diritto dell'Unione non richiede la separazione dei compiti e tale separazione non è praticabile tenuto conto della natura, della dimensione e della complessità dell'entità sottoposta a vigilanza. In questo caso, potrebbero essere più adeguati controlli alternativi. Qualora vengano utilizzati altri controlli, le entità sottoposte a vigilanza dovrebbero documentare la logica alla base della disposizione, individuare i possibili rischi, attuare controlli compensativi per affrontarli e dimostrare che la disposizione non compromette l'ambiente di controllo.

Risorse

30. Per alcune entità sottoposte a vigilanza, potrebbe non essere proporzionato disporre di personale a tempo pieno in tutte le funzioni, per loro natura, dimensione e complessità. In questi casi, un'entità sottoposta a vigilanza può scegliere di adeguare il numero di ore delle risorse alle attività di controllo o di esternalizzare l'attività.

Specializzazione all'interno delle funzioni

31. Man mano che un'entità sottoposta a vigilanza cresce e il suo ambiente di controllo matura, dovrebbe avvalersi della specializzazione del personale per trarre vantaggio dalle competenze dei dipendenti nei processi chiave o nelle aree di rischio. Le entità sottoposte a vigilanza di una determinata natura, portata e complessità dovrebbero disporre di squadre dedicate di monitoraggio o d'inchiesta nell'ambito della funzione di controllo della conformità.

Maturità delle attività di controllo

32. La maturità delle attività di controllo (cioè manuali, ibride, automatizzate e, in alcuni casi, che incorporano strumenti di intelligenza artificiale) dovrebbe riflettere la natura, la dimensione, la complessità e il profilo di rischio complessivo di un'entità sottoposta a vigilanza. Per le entità sottoposte a vigilanza di una certa natura, dimensione e complessità, dovrebbero esserci un livello più elevato di controlli automatizzati e una maggiore integrazione tra i sistemi delle funzioni di controllo, al fine di ottimizzare le attività di monitoraggio e la comunicazione, da parte di un'entità sottoposta a vigilanza, delle informazioni sulla gestione all'alta dirigenza esecutiva e all'organo di gestione.

Componente 2.1 Funzione di controllo della conformità

33. La funzione di controllo della conformità di un'entità sottoposta a vigilanza è responsabile del monitoraggio e della rendicontazione in merito all'adempimento, da parte dell'entità sottoposta a vigilanza e dei suoi dipendenti, degli obblighi derivanti dal regolamento pertinente. Spetta alla funzione di controllo della conformità tenersi aggiornata sulle modifiche introdotte nelle disposizioni legislative e regolamentari applicabili alle proprie attività. La funzione di controllo della conformità è altresì responsabile di fornire consulenza all'organo di gestione in merito a leggi, norme, regolamenti e standard cui l'entità sottoposta a vigilanza deve conformarsi e di valutare, insieme ad altre funzioni competenti, l'eventuale impatto delle modifiche del contesto giuridico o normativo sulle attività dell'entità sottoposta a vigilanza.

Caratteristiche

- 2.1.1** La funzione di controllo della conformità dovrebbe svolgere le proprie funzioni in modo indipendente dalle aree di attività e trasmettere relazioni periodiche all'organo di gestione dell'entità sottoposta a vigilanza e, se del caso, direttamente agli INED.
- 2.1.2** La funzione di controllo della conformità dovrebbe fornire consulenza e assistenza al personale ai fini dell'adempimento degli obblighi previsti dal regolamento pertinente. La funzione di controllo della conformità dovrebbe essere proattiva nell'individuare i rischi e le eventuali inadempienze tramite il tempestivo monitoraggio e la valutazione delle attività nonché nel dare seguito alle azioni correttive.
- 2.1.3** La funzione di controllo della conformità dovrebbe garantire che il monitoraggio della conformità sia effettuato sulla base di un programma di monitoraggio strutturato e ben definito. L'ambito delle attività di controllo della conformità dovrebbe comprendere tutti i processi e i sistemi operativi e informatici che potrebbero incidere sulla conformità dell'entità sottoposta a vigilanza al regolamento pertinente.

- 2.1.4** La funzione di controllo della conformità, eventualmente d'intesa con altre funzioni competenti, dovrebbe valutare il possibile impatto delle modifiche intervenute nel contesto giuridico o normativo sulle attività dell'entità sottoposta a vigilanza e, ove necessario, comunicare tempestivamente con la funzione di gestione dei rischi riguardo al rischio di conformità dell'entità sottoposta a vigilanza.
- 2.1.5** La funzione di controllo della conformità dovrebbe garantire il rispetto delle politiche di conformità e riferire all'organo di gestione e all'alta dirigenza esecutiva in merito al rischio di conformità dell'entità sottoposta a vigilanza.
- 2.1.6** La funzione di controllo della conformità dovrebbe cooperare con la funzione di gestione dei rischi e scambiare le informazioni necessarie per lo svolgimento dei rispettivi compiti.
- 2.1.7** Le conclusioni tratte dalla funzione di controllo della conformità dovrebbero essere tenute in considerazione dall'organo di gestione e dall'alta dirigenza esecutiva nonché dalla funzione di gestione dei rischi nell'ambito dei rispettivi processi di valutazione del rischio.

Componente 2.2 Funzione di gestione dei rischi

- 34. La funzione di gestione dei rischi di un'entità sottoposta a vigilanza è responsabile dello sviluppo e dell'attuazione del quadro di gestione dei rischi.

Caratteristiche

- 2.2.1** La funzione di gestione dei rischi dovrebbe svolgere le proprie funzioni in modo indipendente dalle aree di attività e unità di cui controlla i rischi, ma non le dovrebbe essere impedito di interagire con loro.
- 2.2.2** La funzione di gestione dei rischi dovrebbe garantire che tutti i rischi suscettibili di incidere sulla capacità di un'entità sottoposta a vigilanza di adempiere ai propri obblighi derivanti dai regolamenti pertinenti, o sulla sua continuità operativa, siano individuati, valutati e misurati. I rischi rilevanti per il conseguimento di tali obiettivi dovrebbero quindi essere monitorati, gestiti, attenuati e adeguatamente segnalati dalle e alle unità pertinenti all'interno dell'entità sottoposta a vigilanza in modo tempestivo.
- 2.2.3** La funzione di gestione dei rischi dovrebbe monitorare il profilo di rischio dell'entità sottoposta a vigilanza rispetto alla sua propensione al rischio per consentire la presa di decisioni.

- 2.2.4** La funzione di gestione dei rischi dovrebbe fornire consulenza sulle proposte e sulle decisioni in materia di rischio adottate dalle aree di attività e indicare all'organo di gestione se tali decisioni sono coerenti con la propensione al rischio e gli obiettivi dell'entità sottoposta a vigilanza.
- 2.2.5** La funzione di gestione dei rischi dovrebbe raccomandare miglioramenti al quadro di gestione dei rischi e, se necessario, modifiche delle politiche e delle procedure in materia di rischi. La funzione di gestione dei rischi dovrebbe rivedere le soglie di rischio in funzione di eventuali variazioni nella propensione al rischio dell'organizzazione.

Componente 2.3 Funzione di gestione della sicurezza delle informazioni (solo per le entità sottoposte a vigilanza non soggette a DORA)

35. La funzione di gestione della sicurezza delle informazioni di un'entità sottoposta a vigilanza è responsabile dello sviluppo e dell'attuazione della sicurezza delle informazioni all'interno dell'entità stessa. Un'entità sottoposta a vigilanza dovrebbe istituire una funzione che promuova una cultura della sicurezza delle informazioni al suo interno.

Caratteristiche

- 2.3.1** La funzione di gestione della sicurezza delle informazioni dovrebbe essere responsabile della revisione e del monitoraggio della conformità dell'entità sottoposta a vigilanza alle politiche e alle procedure di sicurezza delle informazioni dell'entità stessa.
- 2.3.2** La funzione di gestione della sicurezza delle informazioni dovrebbe gestire le attività dell'entità sottoposta a vigilanza relative alla sicurezza delle informazioni.
- 2.3.3** La funzione di gestione della sicurezza delle informazioni dovrebbe sviluppare e predisporre un programma di sensibilizzazione riguardo alla sicurezza delle informazioni rivolto al personale al fine di migliorare la cultura della sicurezza e favorire un'ampia comprensione del quadro relativo alla sicurezza delle informazioni dell'entità sottoposta a vigilanza.
- 2.3.4** La funzione di gestione della sicurezza delle informazioni dovrebbe riferire all'organo di gestione e all'alta dirigenza esecutiva e fornire loro consulenza in merito allo stato del sistema di gestione della sicurezza delle informazioni e ai relativi rischi (ad esempio, informazioni sui progetti di sicurezza delle informazioni, incidenti relativi alla sicurezza delle informazioni e risultati delle analisi della sicurezza delle informazioni).

Componente 2.4 Funzione di audit interno

36. Una funzione di audit interno di un'entità sottoposta a vigilanza è responsabile di svolgere un'attività indipendente e obiettiva di garanzia e di consulenza intesa a migliorare le attività operative dell'organizzazione. Tale funzione aiuta l'organizzazione a conseguire i suoi obiettivi proponendo un approccio sistematico e disciplinato per valutare e migliorare l'efficacia del sistema di controllo interno.

Caratteristiche

- 2.4.1** La funzione di audit interno dovrebbe svolgere le proprie funzioni in modo indipendente dalle aree di attività e da altre funzioni CI. Dovrebbe essere disciplinata da una carta dell'audit interno che ne definisce il ruolo e le responsabilità ed è soggetta alla sorveglianza dell'organo di gestione.
- 2.4.2** La funzione di audit interno dovrebbe seguire un approccio basato sul rischio e aderire alle norme internazionali in materia di audit interno.
- 2.4.3** La funzione di audit interno dovrebbe svolgere un riesame indipendente e fornire la garanzia obiettiva che le attività dell'entità sottoposta a vigilanza, comprese le attività esternalizzate, siano conformi alle politiche e alle procedure della stessa nonché ai requisiti di natura legale e regolamentare applicabili.
- 2.4.4** La funzione di audit interno dovrebbe definire almeno una volta l'anno, sulla base degli obiettivi di controllo annuali di audit interno, un piano di audit soggetto al controllo dell'organo di gestione.
- 2.4.5** La funzione di audit interno dovrebbe presentare relazioni periodiche ai membri indipendenti dell'organo di gestione o al comitato di audit, se presente.
- 2.4.6** La funzione di audit interno dovrebbe comunicare le proprie raccomandazioni in una forma chiara e coerente che permetta all'organo di gestione e all'alta dirigenza esecutiva di comprenderne il grado di rilevanza e definire le priorità di conseguenza.
- 2.4.7** Le raccomandazioni in materia di audit interno dovrebbero essere soggette a una procedura formale di follow-up ai livelli adeguati della dirigenza, al fine di garantire e riferire in merito alla loro attuazione efficace e tempestiva.

Componente 2.5 Funzione di revisione (solo per le CRA)

37. La funzione di revisione di una CRA ha la responsabilità di rivedere le metodologie di rating del credito almeno una volta all'anno. La funzione di revisione della CRA è inoltre responsabile della convalida e del riesame delle nuove metodologie e di eventuali modifiche apportate alle metodologie esistenti.

Caratteristiche

- 2.5.1** La funzione di revisione dovrebbe svolgere le sue funzioni in modo indipendente dalle aree di attività responsabili delle attività di rating del credito e presentare relazioni periodiche agli INED della CRA.
- 2.5.2** Gli azionisti della CRA o il personale che partecipa allo sviluppo dell'attività non dovrebbero svolgere i compiti della funzione di revisione.
- 2.5.3** Gli analisti non dovrebbero partecipare all'approvazione di nuove metodologie, nuovi modelli e nuove ipotesi principali di rating o alla convalida e revisione di quelli esistenti che abbiano sviluppato loro stessi.
- 2.5.4** Il personale della funzione di revisione dovrebbe avere la responsabilità esclusiva o detenere la maggioranza dei diritti di voto in seno ai comitati responsabili di approvare le metodologie, i modelli e le ipotesi principali di rating.
- 2.5.5** Il personale della funzione di revisione responsabile della convalida e/o della revisione di una metodologia e che partecipa anche alla sua fase di sviluppo non dovrebbe avere la responsabilità esclusiva o detenere la maggioranza dei diritti di voto in seno ai comitati responsabili di approvare le metodologie.
- 2.5.6** In caso di esternalizzazione della funzione di revisione, l'agenzia di rating del credito dovrebbe tenere conto dell'orientamento 1.5.6. Inoltre, la CRA dovrebbe disporre di adeguati meccanismi di controllo interno per garantire il costante rispetto dei requisiti normativi e il mantenimento di standard di qualità analitica adeguati.

Componente 2.6 Funzione di sorveglianza (solo per i BMA) ⁽¹²⁾

38. La funzione di sorveglianza sovrintende ai principali aspetti della fornitura dei parametri di riferimento. Ciò include, a titolo esemplificativo ma non esaustivo, la revisione della definizione e della metodologia dell'indice di riferimento, la gestione dei soggetti terzi coinvolti nella fornitura dell'indice di riferimento, la valutazione delle revisioni o degli audit

⁽¹²⁾ I BMA non significativi che applicano l'articolo 26 del BMR sono tenuti ad applicare i presenti orientamenti in proporzione ai requisiti di cui all'articolo 26.

interni ed esterni del quadro di controllo dell'amministratore e la segnalazione alle autorità competenti di eventuali condotte illecite.

Caratteristiche

- 2.6.1** La funzione di sorveglianza dei BMA mantiene la sua indipendenza da qualsiasi organo di gestione o funzione dei BMA e da qualsiasi soggetto esterno a essi. L'indipendenza presuppone che i membri della funzione di sorveglianza non siano soggetti a conflitti di interessi tra le loro attività in qualità di membri di tale funzione e le loro altre attività. I BMA dovrebbero implementare un quadro operativo di controllo interno per prevenire e mitigare qualsiasi potenziale conflitto di interessi.
- 2.6.2** I BMA dovrebbero avere politiche e procedure chiare per quanto riguarda l'istituzione e le responsabilità della funzione di sorveglianza e dei suoi membri, comprese politiche e procedure per gli aggiornamenti della metodologia degli indici di riferimento e le revisioni dell'integrità dei dati.
- 2.6.3** La funzione di sorveglianza dei BMA dovrebbe svolgere regolarmente un'autovalutazione per valutare la propria efficacia e l'idoneità dei membri ai fini della funzione, nonché individuare potenziali conflitti di interessi e proporre aree di miglioramento, se necessario.
- 2.6.4** La funzione di sorveglianza dei BMA dovrebbe mantenere un canale di comunicazione definito e regolare con l'organo di gestione, l'alta dirigenza esecutiva e altre funzioni fondamentali. La funzione di sorveglianza dei BMA dovrebbe inoltre poter accedere alle informazioni sulla gestione e contestarle e ricevere aggiornamenti sullo stato delle azioni correttive a seguito di audit interni ed esterni, relazioni sui rischi e sulla conformità.
- 2.6.5** La funzione di sorveglianza dei BMA dovrebbe mantenere un canale di comunicazione definito con le autorità competenti interessate, anche per la segnalazione di condotte illecite o violazioni da parte degli amministratori o dei contributori.