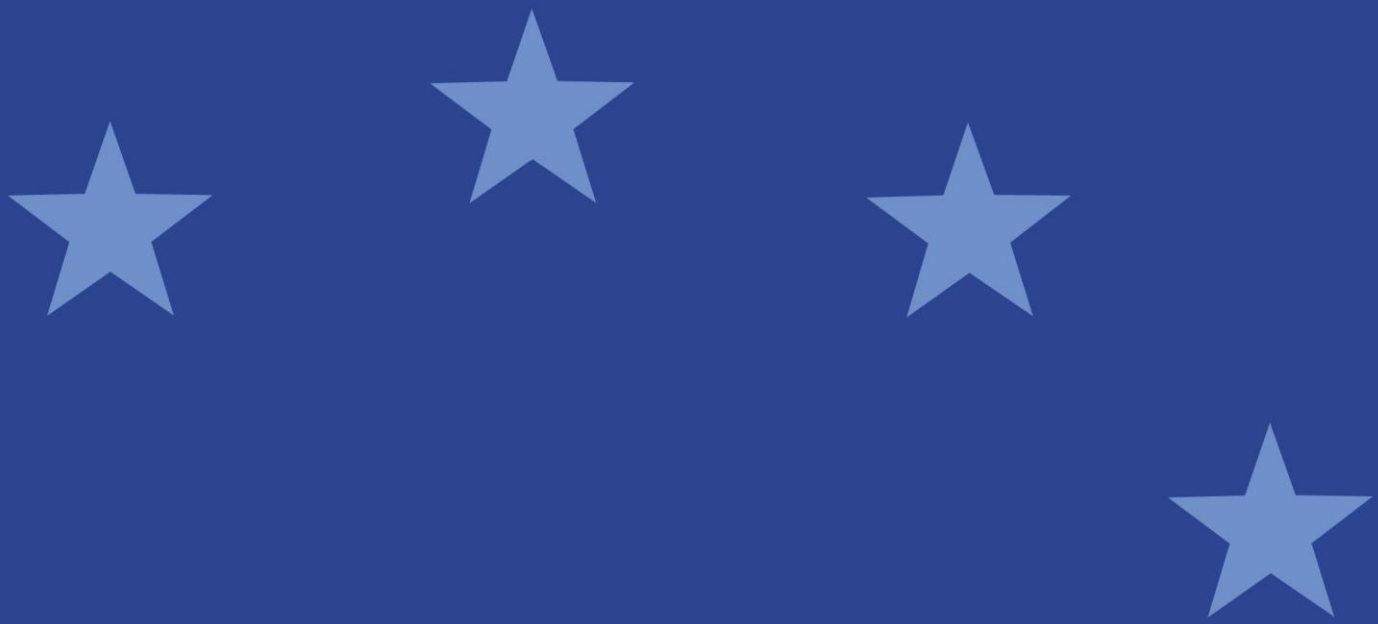
esma European Securities and Markets Authority

Orientamenti

sul controllo interno delle agenzie di rating del credito



10/03/2021 | ESMA33-9-371 IT

Indice

1 Ambito di applicazione

Destinatari

1. I presenti orientamenti si applicano alle agenzie di rating del credito stabilite nell'Unione e registrate presso l'Autorità europea degli strumenti finanziari e dei mercati ai sensi del regolamento (CE) n. 1060/2009 del Parlamento europeo e del Consiglio, del 16 settembre 2009, relativo alle agenzie di rating del credito ([1]).

Oggetto

2. I presenti orientamenti riguardano gli aspetti relativi alla struttura e ai meccanismi di controllo interno necessari per assicurare l'effettiva conformità da parte delle agenzie di rating del credito all'articolo 6, paragrafi 1, 2 e 4, e all'allegato I, sezione A, del regolamento relativo alle agenzie di rating del credito.

Tempistica

3. I presenti orientamenti si applicano a partire dal 1º luglio 2021.

([1]) GU L 302 del 17.11.2009, pag. 1.

2 Riferimenti normativi, abbreviazioni e definizioni

Riferimenti normativi

Regolamento ESMA	Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione ([2])
Regolamento CRA	Regolamento (CE) n. 1060/2009 del Parlamento europeo e del Consiglio, del 16 settembre 2009, relativo alle agenzie di rating del credito

Abbreviazioni

ESMA	Autorità europea degli strumenti finanziari e dei mercati
CRA	Agenzia di rating del credito (*Credit Rating Agency*)
CRAR	*Regolamento CRA*
Quadro CI	Quadro di controllo interno
Funzioni CI	Funzioni di controllo interno
INED	Membri indipendenti del consiglio di amministrazione o di sorveglianza della CRA
Consiglio di amministrazione o di sorveglianza della CRA	Il consiglio

3 Finalità

4. I presenti orientamenti riguardano gli aspetti relativi alla struttura e ai meccanismi di controllo interno necessari per assicurare l'effettiva conformità da parte delle CRA all'articolo 6, paragrafi 1, 2 e 4, e all'allegato I, sezione A, del CRAR.

5. Gli orientamenti descrivono le aspettative dell'ESMA riguardo alle componenti e alle caratteristiche del quadro CI e delle funzioni CI di una CRA.

([2]) *GU L 331 del 15.12.2010, pag. 84.*

4 Conformità e obblighi di notifica

4.1 Status degli orientamenti

6. Il presente documento contiene orientamenti emanati ai sensi dell'articolo 16 del regolamento ESMA. Conformemente al regolamento, le CRA devono compiere ogni sforzo per conformarsi agli orientamenti.

4.2 Obblighi di notifica

7. L'ESMA valuterà l'applicazione dei presenti orientamenti da parte delle CRA tramite le sue costanti attività di vigilanza e monitoraggio delle loro attività.

8. Ai fini dell'applicazione dei presenti orientamenti, l'ESMA applicherà il principio di proporzionalità. Sebbene tutte le CRA debbano dimostrare di possedere le caratteristiche di un sistema di controllo interno efficace descritte nei presenti orientamenti, in alcuni casi l'ESMA può non aspettarsi che una CRA lo faccia mediante funzioni CI dedicate e distinte di cui alla sezione 5.2.

9. L'ESMA adeguerà le proprie aspettative di cui alla sezione 5.2 in funzione della natura, della portata e della complessità di una CRA. Per le CRA di dimensioni più grandi, l'ESMA si aspetta che queste rispondano a tutte le aspettative descritte negli orientamenti. Per le CRA di più piccole dimensioni, l'ESMA farà riferimento alle condizioni di registrazione dell'agenzia. Tuttavia, poiché la natura, la portata e la complessità di alcune CRA potrebbero essere cambiate dalla registrazione, l'ESMA comunicherà, nell'ambito della propria attività di vigilanza, se le aspettative di cui alla sezione 5.2 sono più elevate rispetto a quelle stabilite al momento della registrazione.

10. Sebbene l'ESMA comunicherà il tenore delle sue aspettative tramite le proprie attività di vigilanza, spetta comunque alla dirigenza della CRA, sotto la supervisione del consiglio, la responsabilità di valutare l'adeguatezza del proprio controllo interno alla luce dei presenti orientamenti

5 Orientamenti sui controlli interni delle CRA

Obblighi di cui all'articolo 6, paragrafi 1, 2 e 4, e all'allegato I, sezione A, del CRAR

11. Affinché una CRA soddisfi gli obiettivi di una struttura di controllo interno efficace conformemente all'articolo 6, paragrafi 1, 2 e 4, e all'allegato I, sezione A, del CRAR, l'ESMA si attende che una CRA dimostri che le sue 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.

12. In tale contesto, i termini «politiche e procedure» dovrebbero fare riferimento ai documenti interni che disciplinano o indirizzano il modo in cui la CRA o il suo personale dovrebbero svolgere le attività soggette agli obblighi derivanti dal CRAR.

5.1 Quadro di controllo interno

13. Affinché dimostri di avvalersi di un quadro di controllo interno (quadro CI) efficace, l'ESMA si aspetta che una CRA sia in grado di dare evidenza della presenza delle componenti e caratteristiche indicate di seguito nelle proprie politiche e procedure interne e prassi di lavoro.

Principi generali

14. Il consiglio di una CRA dovrebbe essere responsabile del controllo e dell'approvazione di tutte le componenti del quadro CI elaborato dalla dirigenza, oltre ad assicurare che dette componenti siano oggetto di monitoraggio e aggiornamento periodico da parte da parte dirigenza. Dovrebbe spettare alla dirigenza della CRA creare, attuare e aggiornare le politiche e le procedure scritte riguardanti il controllo interno a sostegno delle componenti del quadro CI.

15. Al fine di porre in essere tali politiche e procedure, una CRA dovrebbe prevedere processi decisionali chiari, trasparenti e documentati nonché una chiara ripartizione dei ruoli e delle responsabilità nell'ambito del quadro CI, comprese le sue aree di attività e le sue funzioni di controllo interno.

Componente 1.1 Ambiente di controllo

16. Per ambiente di controllo l'ESMA intende l'insieme di norme, processi e strutture necessario a svolgere il controllo interno in seno a un'organizzazione. A parere dell'ESMA, l'ambiente di controllo è la base su cui si fonda un sistema efficace di controlli interni.

17. Il consiglio e la dirigenza di una CRA contribuiscono entrambi a dare il massimo risalto all'importanza del controllo interno. La dirigenza è responsabile della definizione e del funzionamento del controllo interno, nonché della valutazione dell'adeguatezza e dell'efficacia dell'ambiente di controllo.

Caratteristica

1.1.1 La dirigenza della CRA dovrebbe avere la responsabilità di creare una forte cultura di etica e di conformità all'interno dell'agenzia attuando politiche e procedure che disciplinano il comportamento del personale della CRA. In tali ambiti, il consiglio dovrebbe esercitare un controllo sulla dirigenza.

1.1.2 La dirigenza dovrebbe avere la responsabilità di assicurare che le politiche e le procedure della CRA:

i. richiamino la circostanza che le attività di rating del credito dovrebbero essere condotte in conformità del CRAR, delle leggi applicabili e dei valori aziendali della CRA;

ii. chiariscano che, oltre a ottemperare a prescrizioni di leggi e regolamenti 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;

iii. garantiscano che il personale sia consapevole delle potenziali azioni disciplinari interne ed esterne nonché delle azioni legali e delle sanzioni che possono scaturire da comportamenti scorretti o inaccettabili.

In tali ambiti, il consiglio dovrebbe esercitare un controllo sulla dirigenza.

1.1.3 La dirigenza della CRA dovrebbe avere la responsabilità di creare, mantenere e aggiornare periodicamente adeguate politiche e procedure scritte di controllo interno. In tali ambiti, il consiglio dovrebbe esercitare un controllo sulla dirigenza.

1.1.4 La dirigenza della CRA dovrebbe mantenere la responsabilità delle attività commissionate a prestatori di servizi esterni o a una funzione a livello del gruppo di cui fa parte la CRA. In tali ambiti, il consiglio dovrebbe esercitare un controllo sulla dirigenza.

Componente 1.2 Gestione del rischio

18. L'ESMA ritiene che la gestione del rischio comporti l'individuazione, la valutazione, il monitoraggio e l'attenuazione di tutti i rischi suscettibili di incidere in maniera rilevante sulla capacità della CRA di adempiere ai propri obblighi derivanti dal CRAR o di minacciarne la continuità operativa. In tal modo la CRA può allocare adeguatamente le proprie risorse di controllo interno. Un'efficace gestione del rischio dovrebbe prevedere un processo dinamico in continua evoluzione per l'individuazione, la valutazione e la gestione dei rischi ai fini del conseguimento dei principali obiettivi della CRA.

Caratteristica

1.2.1 La CRA dovrebbe svolgere le valutazioni interne del rischio conformemente a una metodologia di valutazione del rischio ben definita e completa.

1.2.2 La metodologia di valutazione del rischio della CRA dovrebbe comprendere tutte le aree di attività dell'agenzia.

1.2.3 La CRA dovrebbe stabilire la propria propensione al rischio e individuare i livelli di tolleranza al rischio nell'ambito del processo di valutazione del rischio.

1.2.4 Il processo di valutazione del rischio della CRA dovrebbe definire e individuare in anticipo i criteri e gli obiettivi rispetto ai quali saranno valutati i rischi dell'agenzia.

1.2.5 La metodologia di valutazione del rischio della CRA dovrebbe essere soggetta a evoluzione e miglioramento costanti.

Componente 1.3 Attività di controllo

19. L'ESMA ritiene che le attività di controllo che regolano l'attività della CRA contribuiscano ad attenuare l'impatto dei rischi all'interno di un'organizzazione. Tali azioni sono definite mediante politiche, procedure, sistemi, meccanismi e altre misure. Le attività di controllo dovrebbero avere natura preventiva, investigativa, correttiva o dissuasiva.

Caratteristiche

1.3.1 Documentazione: la CRA dovrebbe documentare le proprie politiche e procedure riguardanti tutte le attività soggette alle disposizioni del CRAR.

1.3.2 *Controlli documentati e verifica dei controlli*: la CRA dovrebbe documentare i controlli essenziali posti in essere per assicurare l'osservanza delle politiche e delle procedure pertinenti ai fini del CRAR. La documentazione della verifica dei controlli dovrebbe contenere:

i. una descrizione del controllo;

ii. il rischio o i rischi rilevanti associati;

iii. il ruolo o la funzione (o i ruoli e le funzioni) responsabili di eseguire il controllo;

iv. il ruolo o la funzione (o i ruoli e le funzioni) responsabili di riesaminare il controllo;

v. la prova che il controllo è stato eseguito;

vi. la frequenza di esecuzione del controllo;

vii. una descrizione della procedura di verifica.

1.3.3 *Separazione delle funzioni*: la CRA dovrebbe garantire un'adeguata separazione delle funzioni per gestire i rischi di conflitti di interesse, frode ed errore umano. La separazione delle funzioni dovrebbe garantire che le persone:

i. addette all'analisi di un rating del credito non siano esclusivamente responsabili dell'approvazione del rating;

ii. addette allo sviluppo di metodologie, modelli o ipotesi fondamentali di rating alla base del rating del credito non siano le sole responsabili dell'approvazione di tali metodologie, modelli o ipotesi fondamentali di rating;

iii. addette alla convalida o al riesame di una metodologia, di un modello o di un'ipotesi fondamentale di rating non siano esclusivamente responsabili dell'approvazione di tale convalida o riesame.

1.3.4 *Designazione delle responsabilità*: la CRA dovrebbe designare in modo chiaro e ben definito i ruoli o le funzioni responsabili di effettuare i controlli relativi agli obblighi derivanti dal CRAR e specificarne i rispettivi compiti e responsabilità. A tal fine, la CRA 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*: la CRA dovrebbe documentare e descrivere i processi relativi a metodologie, modelli o ipotesi fondamentali alla base del rating del credito, ivi compresi i membri del personale responsabili della loro convalida o del loro riesame e l'analisi dei risultati di tali processi.

1.3.6 *Verifiche, convalide, riconciliazioni e riesami*: la CRA dovrebbe adottare misure atte a individuare e contrastare i comportamenti inopportuni, non autorizzati, erronei o fraudolenti nelle proprie attività di rating del credito e nei processi sottostanti, quali la convalida della metodologia di rating o dei modelli, la convalida e l'immissione dei dati.

1.3.7 *Controlli informatici generali*: la CRA dovrebbe porre in essere controlli atti a garantire l'efficacia del proprio ambiente informatico nel sostenere i processi operativi.

Componente 1.4 Informazione e comunicazione

20. L'ESMA ritiene che un'adeguata comunicazione interna ed esterna sia fondamentale affinché una CRA adempia agli obblighi normativi nei confronti del mercato, dei clienti e del personale. La CRA dovrebbe stabilire procedure per la condivisione a valle di informazioni accurate, complete e di buona qualità con il personale e le parti interessate esterne nonché procedure per la condivisione a monte di informazioni riservate relative al comportamento e all'osservanza dei controlli interni.

Caratteristiche

1.4.1 La CRA dovrebbe garantire una comunicazione interna ed esterna adeguata, condividendo tempestivamente informazioni accurate, complete e di buona qualità con il mercato, gli investitori, i clienti e le autorità di regolamentazione.

1.4.2 La CRA dovrebbe istituire canali di comunicazione a monte, tra cui una procedura di segnalazione delle irregolarità, affinché le questioni rilevanti di controllo interno siano portate a conoscenza del consiglio e della dirigenza.

1.4.3 La CRA dovrebbe istituire canali di comunicazione a valle, dalla dirigenza e dalle funzioni di controllo al personale. La comunicazione dovrebbe prevedere aggiornamenti periodici sugli obiettivi e sulle responsabilità del controllo interno, i problemi di conformità individuati, le presentazioni e le attività di formazione in materia di politiche e procedure.

Componente 1.5 Attività di monitoraggio

21. L'ESMA è del parere che il monitoraggio continuo e le analisi tematiche delle attività di una CRA siano necessari per assicurare l'adeguatezza e l'efficacia costanti del sistema di controllo interno. Tale monitoraggio contribuirà ad accertare la presenza e il funzionamento efficace delle componenti del sistema di controllo interno della CRA.

Caratteristiche

1.5.1 La CRA dovrebbe garantire l'esecuzione di valutazioni del sistema di controllo interno a diversi livelli, quali le aree di attività, le funzioni di controllo e le funzioni di audit interno o di valutazione indipendente.

1.5.2 Le valutazioni del sistema di controllo interno della CRA dovrebbero essere eseguite su base periodica o tematica, o una combinazione di entrambe.

1.5.3 La CRA dovrebbe integrare nei processi utilizzati per la propria attività valutazioni continue, quali il monitoraggio tempestivo delle interazioni per posta elettronica fra analisti ed emittenti, e adattarle al variare delle condizioni, ivi compresa la partecipazione periodica ai comitati di rating o la relativa revisione ex post.

1.5.4 La CRA dovrebbe segnalare le carenze individuate nell'ambito delle valutazioni di monitoraggio e i rimedi necessari al consiglio e alla dirigenza, i quali dovrebbero poi monitorare la tempestiva attuazione dell'azione o delle azioni correttive.

1.5.5 In caso di esternalizzazione di importanti funzioni operative, la CRA dovrebbe garantire che il personale sia direttamente responsabile del monitoraggio dei processi esternalizzati. La CRA dovrebbe assicurare che i prestatori di servizi esterni ricevano chiare indicazioni riguardo ai propri obiettivi e ai risultati attesi e che venga svolta la procedura di due diligence prima che venga designato il prestatore.

5.2 Funzioni di controllo interno

22. Al fine di garantire che una CRA si avvalga di funzioni di controllo interno (funzioni CI) efficaci, l'ESMA si aspetta che una CRA sia in grado di fornire prova che le componenti e le caratteristiche indicate di seguito siano contenute nelle proprie politiche e procedure interne e prassi di lavoro.

Principi generali

23. L'ESMA ritiene che le funzioni CI di una CRA debbano disporre di risorse sufficienti e di personale dotato di competenze adeguate per poter svolgere i propri compiti. Nel caso in cui la CRA abbia assegnato i compiti operativi importanti di una funzione CI a un gruppo o a una parte esterna, l'ESMA è dell'avviso che la CRA debba conservare la piena responsabilità delle attività della funzione CI esternalizzata. Secondo l'ESMA il personale incaricato delle funzioni CI della CRA dovrebbe essere di grado adeguato per avere l'autorità necessaria ad adempiere alle proprie responsabilità. Alcune funzioni 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 del consiglio della CRA di esercitare il proprio controllo e la capacità della dirigenza di gestire i rischi in modo efficace, o la capacità dell'ESMA di vigilare in modo efficace sulla CRA.

24. Per garantire l'indipendenza delle funzioni CI, l'ESMA auspica che la CRA tenga conto dei seguenti principi nello stabilire i ruoli e le responsabilità delle proprie funzioni CI:

    i. le funzioni CI dovrebbero essere divise, dal punto di vista funzionale, dalle funzioni/attività che sono chiamate a monitorare o sottoporre ad audit o 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 controllo;

    iii. il capo di una funzione CI non dovrebbe riferire a una persona avente la responsabilità diretta di gestire le attività che la funzione CI monitora o sottopone ad audit o controllo;

    iv. 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 ai compiti svolti.

Proporzionalità

25. Le condizioni di registrazione di una CRA stabiliscono le aspettative minime dell'ESMA nei confronti dell'agenzia di rating in tema di controllo interno, funzioni di controllo interno e governance. In alcuni casi, l'inclusione nella struttura organizzativa di una CRA di tutte le funzioni CI previste in questa sezione può non essere proporzionata. Ciononostante, le caratteristiche di tutte le funzioni CI descritte in questa sezione degli orientamenti dovrebbero essere previste e assegnate a un responsabile idoneo.

26. L'ESMA è del parere che il consiglio della CRA dovrebbe mantenere il controllo sullo svolgimento di questi compiti e sulla continua adeguatezza del personale e delle risorse delle funzioni CI alla luce della natura, della portata e della complessità delle sue attività operative.

Componente 2.1 Funzione di controllo della conformità

27. L'ESMA ritiene che sia la funzione di controllo della conformità di una CRA ad avere la responsabilità di monitorare e riferire in merito all'adempimento, da parte della CRA e dei suoi impiegati, degli obblighi derivanti dal CRAR. Spetta alla funzione di controllo della conformità tenersi aggiornata sulle modifiche introdotte nella legislazione e nella normativa applicabile alle proprie attività. La funzione di controllo della conformità è altresì responsabile di fornire consulenza al consiglio di amministrazione o di sorveglianza in merito a leggi, norme, regolamenti e standard cui la CRA deve conformarsi e di valutare insieme ad altre funzioni competenti l'eventuale impatto delle modifiche del quadro giuridico o normativo sulle attività della CRA.

Caratteristiche

2.1.1 La funzione di controllo della conformità 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.

2.1.2 La funzione di controllo della conformità dovrebbe fornire consulenza e assistenza ai membri del personale che svolgono attività di rating del credito ai fini dell'adempimento degli obblighi derivanti dal CRAR. 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 strutturato e ben definito.

2.1.4 La funzione di controllo della conformità, opportunamente assieme ad altre funzioni competenti, dovrebbe valutare il possibile impatto delle modifiche del contesto giuridico o normativo sulle attività della CRA e comunicare, ove opportuno, con la funzione di gestione dei rischi riguardo al rischio di conformità dell'agenzia.

2.1.5 La funzione di controllo della conformità dovrebbe assicurare l'osservanza delle politiche in materia di conformità e informare il consiglio e la dirigenza circa la gestione del rischio di conformità della CRA.

2.1.6 La funzione di controllo della conformità dovrebbe cooperare con la funzione di gestione dei rischi al fine di 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 dal consiglio e dalla funzione di gestione dei rischi nell'ambito dei rispettivi processi di valutazione del rischio.

Componente 2.2 Funzione di revisione

28. Secondo l'ESMA, la funzione di revisione di una CRA ha la responsabilità di rivedere le metodologie, i modelli e le ipotesi principali alla base del rating del credito su base continuativa e almeno una volta l'anno. La funzione di revisione della CRA è inoltre responsabile di convalidare e rivedere le nuove metodologie, i nuovi modelli e le nuove ipotesi principali alla base del rating del credito e ogni loro modifica.

Caratteristiche

2.2.1 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.

2.2.2 Gli azionisti della CRA o il personale che partecipa allo sviluppo dell'attività non dovrebbero svolgere i compiti della funzione di revisione.

2.2.3 Gli analisti non dovrebbero partecipare all'approvazione di nuove metodologie, nuovi modelli e nuove ipotesi principali alla base del rating, o alla convalida e revisione di metodologie, modelli ed ipotesi esistenti, nel caso in cui abbiano sviluppato loro stessi tali elementi.

2.2.4 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 alla base del rating.

Componente 2.3 Funzione di gestione dei rischi

29. L'ESMA ritiene che la funzione di gestione dei rischi di una CRA sia responsabile dello sviluppo e dell'attuazione del quadro di gestione dei rischi. Tale funzione dovrebbe garantire che i rischi attinenti ai propri obblighi derivanti dal CRAR siano individuati, valutati, misurati, monitorati, gestiti e adeguatamente segnalati dai dipartimenti/dalle funzioni pertinenti della CRA.

Caratteristiche

2.3.1 La funzione di gestione dei rischi dovrebbe svolgere le proprie funzioni in modo indipendente dalle aree e unità di attività di cui controlla i rischi, ma non le dovrebbe essere impedito di interagire con loro.

2.3.2 La funzione di gestione dei rischi dovrebbe garantire che tutti i rischi suscettibili di incidere in maniera rilevante sulla capacità della CRA di adempiere ai propri obblighi derivanti dal CRAR, o sulla sua continuità operativa, siano individuati, valutati, misurati, monitorati, gestiti, attenuati e adeguatamente segnalati dalle e alle unità pertinenti della CRA.

2.3.3 La funzione di gestione dei rischi dovrebbe monitorare il profilo di rischio della CRA rispetto alla sua propensione al rischio per consentire la presa di decisioni.

2.3.4 La funzione di gestione dei rischi dovrebbe fornire consulenza sulle proposte e sulle decisioni in materia di rischio adottate dalle aree di attività e informare il consiglio in merito alla circostanza se tali decisioni sono coerenti con la propensione al rischio e gli obiettivi della CRA.

2.3.5 La funzione di gestione dei rischi dovrebbe raccomandare miglioramenti al quadro di gestione dei rischi e misure correttive per le politiche e le procedure in materia di rischio nonché rivedere le soglie di rischio, in funzione di eventuali variazioni nella propensione al rischio dell'organizzazione.

Componente 2.4 Funzione di sicurezza informatica

30. L'ESMA ritiene che la funzione di sicurezza informatica di una CRA sia responsabile dello sviluppo e dell'attuazione della sicurezza delle informazioni all'interno dell'agenzia. Una CRA dovrebbe istituire una funzione di sicurezza informatica che promuova una cultura della sicurezza delle informazioni al suo interno.

Caratteristiche

2.4.1 La funzione di sicurezza informatica dovrebbe svolgere le proprie funzioni in modo indipendente dalle aree di attività ed essere responsabile del monitoraggio della conformità della CRA alle politiche e procedure in materia di sicurezza delle informazioni.

2.4.2 La funzione di sicurezza informatica dovrebbe gestire le attività della CRA relative alla sicurezza delle informazioni.

2.4.3 La funzione di sicurezza informatica dovrebbe predisporre un programma di sensibilizzazione riguardo alla sicurezza delle informazioni rivolto al personale della CRA al fine di migliorare la cultura della sicurezza e favorire un'ampia comprensione dei requisiti in materia di sicurezza delle informazioni.

2.4.4 La funzione di sicurezza informatica dovrebbe presentare aggiornamenti periodici e fornire consulenza al consiglio e alla dirigenza in materia di sicurezza delle informazioni per quanto concerne i sistemi e le attività della CRA.

Componente 2.5 Funzione di audit interno

31. L'ESMA è del parere che la funzione di audit interno di una CRA sia responsabile di svolgere un'attività indipendente e obiettiva di garanzia e di consulenza intesa a migliorare le attività operative dell'organizzazione. La 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

2.5.1 La funzione di audit interno dovrebbe svolgere le sue funzioni in modo indipendente dalle aree di attività e attenersi a una carta di audit interno che definisce il suo ruolo e le sue responsabilità ed è soggetta al controllo del consiglio.

2.5.2 La funzione di audit interno dovrebbe seguire un approccio basato sui rischi.

2.5.3 La funzione di audit interno dovrebbe svolgere un riesame indipendente e fornire la garanzia obiettiva che le attività della CRA, comprese le importanti funzioni operative esternalizzate ([3]), siano conformi alle politiche e procedure della CRA stessa e alle disposizioni giuridiche e normative applicabili.

2.5.4 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 e un programma di audit dettagliato soggetto al controllo del consiglio.

2.5.5 La funzione di audit interno dovrebbe presentare relazioni regolari agli INED della CRA o al comitato di audit, se presente.

2.5.6 La funzione di audit interno dovrebbe comunicare le proprie raccomandazioni in una forma chiara e coerente che permetta al consiglio e alla dirigenza di comprenderne il grado di rilevanza e definirne conseguentemente le priorità.

2.5.7 Le raccomandazioni in materia di audit interno dovrebbero essere soggette a una procedura formale di follow-up da parte dei livelli adeguati della dirigenza, al fine di riferire e garantire in merito alla loro attuazione efficace e tempestiva.

([3]) Per importanti funzioni operative si intendono quelle elencate all'articolo 25, paragrafo 2, del regolamento delegato (UE) n. 449/2012 della Commissione sulle informazioni per la registrazione e la certificazione delle agenzie di rating del credito.