Allegato A

Ruolo degli organi aziendali e sistema dei controlli interni

1. RUOLO DEGLI ORGANI AZIENDALI

Gli organi aziendali assumono un ruolo fondamentale per la definizione di un sistema organizzativo e dei controlli interni adeguato e efficace.

La composizione degli organi aziendali, per numero e professionalità, assicura l'efficace assolvimento dei loro compiti ed è calibrata in funzione delle caratteristiche operative e dimensionali dell'istituto. La ripartizione di competenze tra gli organi aziendali è definita in modo chiaro e garantisce una costante dialettica interna, evitando sovrapposizioni di competenze che possano incidere sulla funzionalità aziendale.

Il presidente dell'organo con funzione di supervisione strategica promuove la dialettica interna e l'effettivo funzionamento del sistema di governo societario; lo stesso non riveste un ruolo esecutivo né svolge, neppure di fatto, funzioni gestionali.

L'operato degli organi aziendali è documentato, per consentire un controllo sugli atti gestionali e sulle decisioni assunte; a questo fine, i verbali delle riunioni degli organi aziendali illustrano in modo dettagliato il processo di formazione delle decisioni e le loro motivazioni.

In questo ambito, l'organo con funzione di supervisione strategica:

a) definisce e approva gli obiettivi, le strategie, il profilo e i livelli di rischio dell'istituto, definendo le politiche aziendali e quelle del sistema dei controlli interni; ne verifica periodicamente la corretta attuazione e coerenza con l'evoluzione dell'attività aziendale;

b) approva le politiche di gestione dei rischi (operativi, di credito, di liquidità, ecc.), nonché le relative procedure e modalità di rilevazione e controllo;

c) approva e verifica periodicamente, con cadenza almeno annuale, la politica per il governo e la gestione dei rischi di sicurezza;

d) approva i criteri in base ai quali sono scelti gli strumenti finanziari in cui investire i fondi ricevuti dalla clientela;

e) approva i processi relativi alla prestazione dei servizi di pagamento e, per gli istituti di moneta elettronica, all'attività di emissione di moneta elettronica e ne verifica periodicamente l'adeguatezza;

f) verifica che l'assetto delle funzioni aziendali di controllo sia definito in coerenza con il principio di proporzionalità e con gli indirizzi strategici e che le funzioni medesime siano dotate di risorse qualitativamente e quantitativamente adeguate;

g) approva la struttura organizzativa e l'attribuzione di compiti e responsabilità e ne verifica, con cadenza almeno annuale, l'adeguatezza; in questo ambito, si assicura, tra l'altro, che:

   - i compiti e le responsabilità, formalizzati in un apposito regolamento interno, siano allocati in modo chiaro e appropriato e che siano separate le funzioni operative da quelle di controllo;
   - gli agenti e i soggetti convenzionati siano dotati di meccanismi di controllo interno adeguati al fine di conformarsi ai rispettivi obblighi in materia di lotta al riciclaggio e finanziamento al terrorismo;
   - l'esternalizzazione delle funzioni aziendali sia coerente con le strategie dell'istituto e i livelli di rischio definiti;
   - sia garantita la separatezza amministrativo-contabile tra l'attività di prestazione di servizi di pagamento e di emissione di moneta elettronica rispetto alle altre attività eventualmente svolte dall'istituto;

h) verifica che il sistema di flussi informativi sia adeguato, completo e tempestivo;

i) stabilisce i principi e gli obiettivi della gestione della continuità operativa.

L'organo con funzione di gestione:

a) attua le politiche aziendali e quelle del sistema dei controlli interni, definite dall'organo con funzione di supervisione strategica;

b) verifica nel continuo l'adeguatezza del sistema dei controlli interni, provvedendo al suo adeguamento alla luce dell'evoluzione dell'operatività;

c) definisce i flussi informativi volti ad assicurare agli organi aziendali la conoscenza dei fatti di gestione rilevanti;

d) definisce in modo chiaro i compiti e le responsabilità delle strutture e delle funzioni aziendali, in modo, tra l'altro, di prevenire potenziali conflitti di interesse e di assicurare che le strutture siano dirette da personale qualificato in relazione alle attività da svolgere;

e) in coerenza con le politiche di governo dei rischi, definisce e attua il processo di gestione dei rischi aziendali;

f) definisce e attua gli standard per la gestione dei dati sensibili relativi ai pagamenti e le procedure di gestione della sicurezza, assicurandone la coerenza con la politica di governo e gestione della sicurezza e la propensione al rischio dell'istituto;

g) definisce e attua la politica aziendale in materia di esternalizzazione di funzioni aziendali;

h) assicura che il personale e gli agenti utilizzati per la prestazione di servizi di pagamento, nonché il personale e i soggetti convenzionati utilizzati per la distribuzione e il rimborso della moneta elettronica, siano adeguatamente formati con riferimento ai prodotti commercializzati e ai servizi prestati, agli adempimenti in materia di prevenzione dei fenomeni di riciclaggio e di finanziamento al terrorismo, alla normativa in materia di trasparenza;

i) assicura che le politiche aziendali e le procedure siano tempestivamente comunicate a tutto il personale interessato;

j) adotta tempestivamente le misure necessarie nel caso in cui emergano carenze o anomalie dall'insieme delle verifiche svolte sul sistema dei controlli;

k) definisce il piano aziendale di emergenza e continuità operativa e ne promuove il controllo periodico (di norma annuale) e l'aggiornamento.

L'organo con funzione di controllo, nel rispetto delle attribuzioni degli altri organi e collaborando con essi:

a) vigila sull'osservanza delle norme di legge, regolamentari e statutarie, sulla corretta amministrazione, sull'adeguatezza degli assetti organizzativi e contabili dell'istituto;

b) vigila sulla funzionalità del complessivo sistema dei controlli interni e accerta l'efficacia delle strutture e funzioni coinvolte nel sistema dei controlli e l'adeguato coordinamento tra le stesse;

c) valuta il grado di adeguatezza e il regolare funzionamento delle principali aree organizzative;

d) promuove interventi correttivi delle carenze e delle irregolarità rilevate.

L'organo con funzione di controllo può avvalersi per lo svolgimento delle proprie funzioni di tutte le unità delle strutture organizzative che assolvono funzioni di controllo e, in particolare, della funzione di revisione interna. L'attività di controllo può determinare la formulazione di osservazioni e proposte di modifica volte alla rimozione di eventuali anomalie riscontrate. Di tali osservazioni e proposte, nonché della successiva attività di verifica dell'organo con funzione di controllo sull'attuazione di eventuali provvedimenti, è conservata adeguata evidenza.

L'organo con funzione di controllo mantiene il coordinamento con le funzioni di controllo interno e con il soggetto incaricato della revisione legale dei conti, al fine di incrementare il grado di conoscenza sull'andamento della gestione aziendale, avvalendosi anche delle risultanze degli accertamenti effettuati da tali unità operative.

L'interazione tra l'attività dell'organo con funzione di controllo e l'attività di vigilanza contribuisce al rafforzamento del complessivo sistema di supervisione sull'istituto.

2. SISTEMA DEI CONTROLLI INTERNI

Premessa

Il sistema dei controlli interni è costituito dall'insieme delle risorse, delle strutture organizzative, delle regole e delle procedure per assicurare il conseguimento delle strategie aziendali e dell'efficacia ed efficienza dei processi aziendali, della salvaguardia del valore delle attività e della protezione dalle perdite, dell'affidabilità e integrità delle informazioni contabili e gestionali, della conformità delle operazioni con la legge, la normativa di vigilanza e di sorveglianza sul sistema dei pagamenti e le disposizioni interne dell'istituto.

Nel sistema dei controlli interni rientrano le strategie, le politiche, i processi e i meccanismi riguardanti la gestione dei rischi a cui l'istituto è o potrebbe essere esposto e per determinare e controllare il livello di rischio tollerato. In questo contesto, la gestione dei rischi include le funzioni di individuazione, assunzione, misurazione, sorveglianza e attenuazione dei rischi.

Per gli istituti, in relazione alla prestazione dei servizi di pagamento e all'emissione di moneta elettronica, assumono particolare rilievo i rischi operativi, inclusi i rischi relativi alla sicurezza, e quelli di natura legale e reputazionale che possono discendere dai rapporti con la clientela. A tal fine, gli istituti sono tenuti, tra l'altro, ad approntare specifici presidi organizzativi per assicurare il rispetto delle prescrizioni normative e di autoregolamentazione, pianificando, in tale ambito, specifici controlli sulle succursali, sugli agenti e sui soggetti convenzionati.

Gli istituti valutano attentamente le implicazioni derivanti dai mutamenti dell'operatività aziendale (ingresso in nuovi mercati o in nuovi settori operativi, offerta di nuovi prodotti, utilizzo di canali distributivi innovativi, partecipazione a nuovi sistemi di pagamento), con preventiva individuazione dei rischi e definizione di procedure di controllo adeguate, approvate dagli organi aziendali competenti.

Nella predisposizione dei presidi organizzativi, gli istituti tengono conto dell'esigenza di prevenire fenomeni di riciclaggio e di finanziamento al terrorismo.

Tipologie di controllo

Si descrivono di seguito alcune tipologie di controllo, indipendentemente dalle strutture organizzative in cui sono collocate:

1) *controlli di linea* (c.d. *controlli di primo livello*), diretti ad assicurare il corretto svolgimento delle operazioni connesse con la prestazione dei servizi di pagamento e con l'emissione di moneta elettronica. Essi

sono effettuati dalle stesse strutture operative (es. controlli di tipo gerarchico, sistematici e a campione), incorporati nelle procedure (anche automatizzate) ovvero eseguiti nell'ambito dell'attività di *back office*;

2) *controlli sulla gestione dei rischi e di conformità alle norme* (c.d. *controlli di secondo livello*), che hanno l'obiettivo di assicurare: (i) il rispetto dei limiti assegnati alle varie funzioni operative; e (ii) la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio-rendimento assegnati, nonché la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione. Essi sono affidati a strutture diverse da quelle produttive; le funzioni di controllo concorrono alla definizione delle politiche di governo e del processo di gestione dei rischi aziendali;

3) *revisione interna* (*internal audit,* c.d. *controlli di terzo livello*). In tale ambito rientra la valutazione periodica della completezza, della funzionalità e dell'adeguatezza del sistema dei controlli interni, inclusi quelli sul sistema informativo (*ITC audit*), con cadenza prefissata in relazione alla natura e all'intensità dei rischi. L'attività è condotta da funzioni diverse e indipendenti da quelle produttive, anche attraverso verifiche *in loco.*

Ferma l'esigenza di gestire tutti i rischi aziendali, gli istituti, in considerazione della natura dell'attività svolta, prestano particolare attenzione ai rischi operativi, inclusi quelli relativi alla sicurezza, e di reputazione ([1]).

Pertanto, gli istituti:

- prestano particolare attenzione agli eventi di maggiore gravità e scarsa frequenza e individuano le varie forme e modalità con cui possono manifestarsi i rischi operativi, inclusi quelli relativi alla sicurezza, in relazione alle specifiche caratteristiche organizzative ed operative;
- valutano i rischi operativi, inclusi quelli relativi alla sicurezza, e reputazionali connessi con l'introduzione di nuovi prodotti, attività, reti distributive, processi e sistemi rilevanti e con la partecipazione, anche indiretta, a nuovi sistemi di pagamento;
- si dotano di piani di emergenza e di continuità operativa che assicurano la propria capacità di operare su base continuativa e di limitare le perdite operative in caso di gravi interruzioni dell'operatività.

([1]) Il rischio di reputazione può scaturire direttamente da determinati eventi o comportamenti (ad es. politiche commerciali percepite dalla clientela come poco attente ai propri interessi) o indirettamente da altre tipologie di rischio (operativo, credito, liquidità) rispetto alle quali gli effetti reputazionali possono amplificare l'impatto economico. Il rischio di reputazione può pertanto conseguire sia da comportamenti irregolari sia da errate percezioni da parte della clientela o del mercato.

Nel caso in cui gli istituti, nella prestazione dei servizi di pagamento, eroghino finanziamenti ai clienti, essi definiscono adeguati processi decisionali e operativi connessi con la gestione del rischio di credito ([1]).

L'attività di concessione di finanziamenti ha natura accessoria ai servizi di pagamento prestati: gli istituti adottano sistemi e procedure per monitorare i finanziamenti e identificano criteri, di natura anche quantitativa, che tengano conto dei flussi di pagamento effettuati su base annuale.

Gli istituti hanno in ogni momento conoscenza della propria esposizione nei confronti di ogni cliente o gruppo di clienti connessi ([2]), anche al fine di procedere, se del caso, ad una tempestiva revisione delle linee di credito.

Poiché l'insolvenza di un grande prenditore può avere effetti di rilievo sulla solidità patrimoniale, gli istituti si dotano di regole volte ad assicurare la corretta rilevazione, valutazione della qualità e dell'andamento nel tempo delle esposizioni assunte nei confronti di un singolo cliente o gruppo di clienti connessi che siano di importo rilevante rispetto ai fondi propri. Gli istituti adottano misure adeguate a limitare o presidiare opportunamente i rischi derivanti dall'assunzione di esposizioni di importo rilevante nei confronti di singoli clienti o gruppi di clienti connessi.

Il processo riguardante l'erogazione del credito comprende le seguenti fasi: 1) istruttoria; 2) erogazione; 3) monitoraggio delle posizioni; 4) interventi in caso di anomalia; 5) revisione delle linee di credito. Il processo risulta dal regolamento interno ed è periodicamente

---

([1]) Tale obbligo è previsto anche con riferimento all'attività di emissione e gestione di carte di credito con saldo mensile.

([2]) A tali fini si identificano due tipologie di connessioni tra uno o più soggetti:

a) giuridica - se uno dei soggetti in esame ha, direttamente o indirettamente, un potere di controllo sull'altro o sugli altri;
b) economica - quando, indipendentemente dall'esistenza dei rapporti di controllo di cui alla lettera a), esistono, tra i soggetti considerati, legami tali che, con tutta probabilità, se uno di essi si trova in difficoltà finanziarie, in particolare difficoltà di raccolta di fondi o rimborso dei debiti, l'altro, o tutti gli altri, potrebbero incontrare analoghe difficoltà.

Con riferimento alla lettera a) il controllo sussiste – salvo che l'istituto dimostri il contrario – quando ricorre anche una sola delle seguenti circostanze:

1) uno dei soggetti in esame possiede - direttamente o indirettamente - più del 50% del capitale o delle azioni con diritto di voto di un altro dei soggetti in esame;
2) uno dei soggetti in esame possiede il 50% o meno del 50% del capitale o dei diritti di voto in un altro dei soggetti in esame ed è in grado di esercitare il controllo congiunto su di esso in virtù delle azioni e dei diritti posseduti, di clausole statutarie e di accordi con gli altri partecipanti.

Nell'ipotesi di cui al punto 2, ovvero indipendentemente da possessi azionari, costituisce indice di controllo la disponibilità di uno o più dei seguenti poteri: i) indirizzare l'attività di un'impresa in modo da trarne benefici; ii) decidere operazioni significative, quali ad esempio il trasferimento dei profitti e delle perdite; iii) nominare o rimuovere la maggioranza dei componenti degli organi amministrativi; iv) disporre della maggioranza dei voti negli organi amministrativi o della maggioranza dei voti nell'assemblea dei soci o in altro organo equivalente; v) coordinare la gestione di un'impresa con quella di altre imprese ai fini del perseguimento di uno scopo comune.

sottoposto a verifica. Il regolamento, approvato dall'organo con funzione di gestione, definisce, tra l'altro: la documentazione minimale da acquisire per effettuare una adeguata valutazione del merito creditizio del prenditore; le eventuali deleghe in materia di erogazione del credito; le modalità di rinnovo degli affidamenti; le procedure e gli adempimenti riferiti alla fase di monitoraggio del credito nonché le modalità e i tempi di attivazione in caso di rilevazione di crediti anomali; criteri di classificazione, gestione e valutazione dei crediti anomali.

Tutti gli affidamenti sono concessi al termine di un procedimento istruttorio documentato, ancorché basato su procedure automatizzate.

In caso di ricorso ad agenti per la prestazione di servizi di pagamento o, per i soli IMEL, a soggetti convenzionati per la distribuzione e il rimborso della moneta elettronica, gli istituti assicurano il rispetto delle proprie disposizioni interne da parte di questi soggetti, nonché delle disposizioni ad essi applicabili (ad esempio trasparenza, usura, antiriciclaggio, diritti e obblighi delle parti). Gli istituti effettuano controlli, *in loco* o a distanza, sulla rete con cadenza almeno annuale. Gli istituti assicurano altresì che siano resi riconoscibili all'utenza i soggetti di cui si avvalgono (agenti, soggetti convenzionati, punti operativi abilitati all'incasso ai sensi dell'art. 12, comma 4, del d.lgs. 141/2010).

Gli istituti controllano e gestiscono i rischi connessi con gli investimenti dei fondi ricevuti dai clienti in modo da assicurare la pronta disponibilità delle somme per l'esecuzione delle operazioni di pagamento. Essi approntano procedure operative volte ad assicurare il rispetto dei termini fissati dalla normativa per il deposito o l'investimento dei fondi e per la sistemazione di eventuali sbilanci tra valore di tali attività e fondi ricevuti ([1]).

Funzioni aziendali di controllo

Gli istituti istituiscono funzioni indipendenti di controllo di conformità alle norme, di gestione del rischio e di revisione interna, in modo proporzionato alla dimensione e alla complessità dell'attività svolta nonché alla tipologia e alla gamma dei servizi di pagamento prestati.

Per assicurare la correttezza e l'indipendenza delle funzioni aziendali di controllo è necessario che:

a) tali funzioni dispongano dell'autorità, delle risorse e delle competenze necessarie per lo svolgimento dei loro compiti;

b) i responsabili non siano gerarchicamente subordinati ai responsabili delle funzioni sottoposte a controllo e siano nominati dall'organo con funzione di supervisione strategica, sentito l'organo con

([1]) Gli istituti adottato, tra l'altro, presidi idonei a fronteggiare il rischio di disconoscimenti in relazione a operazioni di accreditamento della moneta elettronica o dei conti di pagamento via web, ad es. con addebito di carte di credito (fenomeni di phishing, ecc.).

funzione di controllo. Essi riferiscono direttamente agli organi aziendali;

c) coloro che partecipano alle funzioni aziendali di controllo non partecipino direttamente alla prestazione dei servizi che essi sono chiamati a controllare. Ferma restando tale previsione, in applicazione del principio di proporzionalità, i responsabili delle funzioni di controllo possono avvalersi di soggetti aventi anche funzioni operative, incardinati in strutture aziendali diverse da quelle di controllo, a condizione che l'affidamento a tali soggetti di altri compiti oltre a quelli di controllo non impedisca loro di svolgere in modo adeguato e professionale i compiti di controllo;

d) le funzioni aziendali di controllo siano tra loro separate sotto un profilo organizzativo;

e) il metodo per la determinazione della remunerazione di coloro che partecipano alle funzioni aziendali di controllo non ne comprometta l'obiettività.

Gli istituti possono non applicare i requisiti di cui alla lett. d) del precedente capoverso, qualora dimostrino che, in applicazione del principio di proporzionalità, gli obblighi in questione non sono proporzionati ai rischi da essi assunti e che le funzioni di controllo continuano ad essere efficaci.

Le funzioni aziendali di controllo, svolgono i compiti di seguito indicati.

La funzione di gestione del rischio:

a) collabora alla definizione delle politiche di governo e del processo di gestione del rischio e delle relative procedure e modalità di rilevazione e controllo, verificandone l'adeguatezza nel continuo;

b) verifica nel continuo l'adeguatezza del sistema di controllo dei rischi e ne verifica il rispetto da parte dell'istituto;

c) verifica l'adeguatezza e l'efficacia delle misure prese per rimediare alle carenze riscontrate nel sistema di controllo dei rischi.

La funzione di controllo di conformità (*compliance*) valuta l'adeguatezza delle procedure interne rispetto all'obiettivo di prevenire la violazione di leggi, regolamenti e norme di autoregolamentazione applicabili all'istituto; a questo fine:

a) identifica le norme applicabili all'istituto e ai servizi da esso prestati e ne misura/valuta l'impatto sui processi e procedure aziendali;

b) propone modifiche organizzative e procedurali volte ad assicurare adeguato presidio dei rischi di non conformità alle norme;

c) predispone flussi informativi diretti agli organi aziendali e alle altre funzioni aziendali di controllo;

d) verifica l'efficacia degli adeguamenti organizzativi suggeriti per la prevenzione del rischio di non conformità.

La funzione di revisione interna:

a) definisce e applica un piano di *audit*, approvato dall'organo con funzione di supervisione strategica, per l'esame e la valutazione dell'adeguatezza e dell'efficacia del sistema dei controlli interni, incluso il sistema per la gestione del rischio di sicurezza, e dei meccanismi adottati dagli agenti utilizzati per la prestazione dei servizi di pagamento e dai soggetti convenzionati per la distribuzione e il rimborso della moneta elettronica per conformarsi agli obblighi in materia di lotta al riciclaggio e finanziamento al terrorismo. Il piano di *audit* prevede, tra l'altro, specifici controlli sull'intera rete di succursali, agenti utilizzati per la promozione e conclusione dei contratti relativi alla prestazione dei servizi di pagamento e soggetti convenzionati per la distribuzione e il rimborso di moneta elettronica;
b) formula raccomandazioni agli organi aziendali basate sui risultati delle verifiche effettuate in base al piano di *audit* e ne verifica l'osservanza.

Le funzioni aziendali di controllo presentano agli organi aziendali, almeno una volta all'anno, relazioni sull'attività svolta e forniscono agli stessi organi consulenza per i profili che attengono ai compiti di controllo svolti.