

RELAZIONE**REGOLAMENTO N. 20 DEL 26 MARZO 2008 RECANTE DISPOSIZIONI IN MATERIA DI CONTROLLI INTERNI, GESTIONE DEI RISCHI, COMPLIANCE ED ESTERNALIZZAZIONE DELLE ATTIVITÀ DELLE IMPRESE DI ASSICURAZIONE, AI SENSI DEGLI ARTICOLI 87 E 191, COMMA 1, DEL DECRETO LEGISLATIVO 7 SETTEMBRE 2005, N. 209 – CODICE DELLE ASSICURAZIONI PRIVATE**

Il Regolamento dà attuazione degli articoli 87 e 191, comma 1, lettera c) del Codice delle Assicurazioni, che attribuiscono all'ISVAP il potere di dettare disposizioni in materia di adeguatezza del sistema dei controlli interni e di gestione dei rischi delle imprese e dei gruppi assicurativi.

Il Regolamento (in particolare i capi II, III e IV) riproduce in larga parte le disposizioni della circolare ISVAP n. 577/D del 30 dicembre 2005 (di seguito "577").

Le principali innovazioni apportate riguardano il capo V, concernente l'istituzione di una funzione di *compliance* nelle imprese di assicurazione, e il capo VIII, che introduce la disciplina dell'esternalizzazione delle attività delle imprese di assicurazione.

Con tali novità regolamentari si intendono rafforzare i requisiti qualitativi di gestione, che unitamente ai requisiti prudenziali di tipo quantitativo, rappresentano i presidi a salvaguardia della stabilità delle imprese e dei gruppi assicurativi.

La disciplina di tali aspetti si pone in linea con i più recenti orientamenti internazionali in materia di vigilanza prudenziale a fini di stabilità del settore assicurativo e consente di agevolare la graduale transizione del mercato e della Autorità di vigilanza verso il nuovo regime di Solvency II.

L'approccio regolamentare segue una impostazione *principle based*, attraverso l'individuazione di obiettivi e requisiti minimali, lasciando autonomia alle imprese nel definire i propri modelli gestionali. La regolamentazione è inoltre ispirata al principio di proporzionalità, per consentire implementazioni dei principi calibrate sulle dimensioni e sulla natura delle attività svolte dalle imprese di assicurazione.

Il Regolamento si compone di 41 articoli, suddivisi in nove capi.

Il capo I contiene le disposizioni di carattere generale, comprendenti il richiamo alle norme fondanti il potere regolamentare esercitato (articolo 1), la definizione delle espressioni usate nel testo (articolo 2) e l'ambito di applicazione del Regolamento (articolo 3).

Il capo II si compone di tre sezioni, dedicate rispettivamente ai principi generali in tema di controllo interno, al ruolo attribuito agli organi sociali nell'ambito del sistema dei controlli interni e gestione dei rischi, e alle singole componenti del sistema dei controlli interni.

La disciplina di tale aspetti si pone in linea di continuità rispetto alle previsioni della circolare 577, con limitate modifiche volte a introdurre specifici riferimenti alla adozione di politiche di gestione del rischio di non conformità da parte dell'organo amministrativo e delle conseguenti azioni a livello dell'alta direzione.

Si è inoltre previsto di specificare la periodicità – almeno annuale - con cui l'organo amministrativo deve valutare ai fini dell'eventuale revisione le direttive in materia di controlli interni, le strategie e le politiche di assunzione, valutazione e gestione dei rischi.

L'articolo 13 conferma l'obbligo, ai sensi dell'articolo 212 del Codice delle Assicurazioni, di individuare una funzione per la produzione di dati e di informazioni utili ai fini dell'esercizio della vigilanza supplementare, riprendendo sul punto le disposizioni della circolare ISVAP n. 456 del 6 novembre 2001.

I capi III e IV sono dedicati, rispettivamente, alla funzione di revisione interna, al sistema di gestione dei rischi e alla funzione di *risk management*, consolidando, anche in questo caso, le disposizioni della circolare 577.

Carattere innovativo, come accennato, riveste l'introduzione di un capo V, dedicato alla disciplina della *compliance*.

L'esistenza all'interno dell'impresa di adeguati presidi organizzativi e procedurali che assicurino il rispetto delle norme si configura come un importante strumento proattivo di prevenzione che consente non solo di circoscrivere e minimizzare i rischi legali e di reputazione, ma anche di garantire una adeguata protezione degli assicurati.

Il venire meno dell'incertezza su comportamenti richiesti in uno con la responsabilizzazione di tutto il personale facilita, infatti, la creazione di un patrimonio di regole e di valori condivisi, con conseguenze positive anche sui rapporti con la clientela.

In tale ottica, l'articolo 22 prevede che l'impresa si doti, ad ogni livello aziendale pertinente, di adeguati presidi volti a prevenire il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite patrimoniali o danni di reputazione, in conseguenza di violazioni di norme o di atti di autoregolamentazione.

Tali presidi devono essere idonei a garantire il rispetto delle norme e, in particolare, di quelle relative alla trasparenza e correttezza dei comportamenti nei confronti degli assicurati e danneggiati, all'informativa precontrattuale e contrattuale, alla gestione dei sinistri e, più in generale, alla tutela del consumatore.

Definiti gli obiettivi della verifica di conformità alle norme, l'articolo 23 introduce la costituzione di una specifica funzione di *compliance*, incaricata di verificare che l'organizzazione e le procedure aziendali siano adeguate a tali obiettivi, dettando alcuni principi per l'istituzione e l'operatività della funzione.

Si tratta di principi generali che lasciano le singole imprese libere di individuare le soluzioni organizzative più appropriate alla natura, dimensioni e complessità del proprio *business*, valutando in particolare se costituire una specifica unità organizzativa o avvalersi di risorse appartenenti ad altre strutture aziendali, ricondotte ad unitarietà attraverso l'individuazione di un unico responsabile della funzione.

Viene richiesto che l'organizzazione della funzione di *compliance* sia formalizzata in una specifica delibera dell'organo amministrativo che, nella sua autonomia, ne definisce compiti, responsabilità, modalità e frequenza di reportistica agli organi sociali e alle altre strutture interessate. Deve essere comunque assicurata l'indipendenza, professionalità e autorevolezza della funzione, nonché la separatezza dalle funzioni operative e dalle altre strutture cui sono attribuiti compiti di controllo. L'indipendenza va garantita attraverso la presenza di adeguati presidi per prevenire conflitti di interesse, nel caso in cui alla funzione lavorino risorse di altre aree operative.

Si prevede che l'attività della funzione di *compliance* sia sottoposta a verifiche di *audit* periodiche da parte della funzione di revisione interna, che ne valuta l'efficienza e l'efficacia.

In relazione, invece, ai collegamenti tra funzione di *compliance* e funzione di *risk management* – in linea con quanto previsto dalla circolare 577 relativamente ai rapporti tra funzione di revisione interna e funzione di *risk management* - si ritiene di lasciare all'autonomia dell'organo amministrativo la relativa definizione, che va adeguatamente formalizzata.

L'articolo 24 prevede che, indipendentemente dal modello organizzativo scelto dall'impresa, debba essere comunque nominato un responsabile della funzione di *compliance*, in possesso di

adeguati requisiti di professionalità, indipendenza ed autorevolezza, cui devono fare riferimento tutte le risorse investite a vario titolo di compiti di conformità.

In considerazione delle esigenze delle piccole imprese ed in applicazione del principio di proporzionalità, l'articolo 25 prevede una gamma di opzioni per l'organizzazione della funzione, che consente alle imprese di nominare quale responsabile anche un amministratore, purché privo di deleghe operative, ovvero di esternalizzare la funzione, nel rispetto delle condizioni già previste dalla circolare 577 per l'affidamento in *outsourcing* delle funzioni di revisione interna e di *risk management*.

Al fine di consentire adeguate economie di scala, si è inoltre previsto che le attività relative alla funzione di *compliance* possano essere accentrate all'interno del gruppo assicurativo attraverso la costituzione di una unità specializzata; ciò a condizione che in ciascuna impresa sia individuato un referente che curi i rapporti con il responsabile della funzione di gruppo e che siano adottate procedure atte a garantire che le politiche di gestione del rischio di non conformità definite a livello di gruppo siano adeguatamente calibrate rispetto alle caratteristiche operative della singola impresa.

Nel Capo VI, in attuazione dell'articolo 87 del Codice delle Assicurazioni, è stata introdotta una serie di disposizioni in tema di gruppo assicurativo, in larga parte riprese dalla previgente circolare 577.

Fermo restando che ciascuna impresa appartenente al gruppo è, in ogni caso, tenuta a dotarsi di sistemi di controlli interni, sono previsti specifici doveri per la capogruppo, chiamata ad assicurare forme di controllo (strategico, gestionale e tecnico - operativo) sul gruppo unitariamente considerato (articolo 26) e di supervisione sul sistema di controlli interni delle società appartenenti al gruppo medesimo. La capogruppo è tenuta a formalizzare e rendere noti a tutte le società del gruppo i criteri di identificazione, misurazione, gestione e controllo dei rischi e a validare i sistemi e le procedure di controllo all'interno del gruppo (articolo 27).

In conformità con l'ammissibilità, per le singole imprese, della esternalizzazione di tali funzioni, lo svolgimento delle funzioni di revisione interna, di *risk management* e di *compliance* può essere accentrato presso una delle società che compongono il gruppo.

Il Capo VII, articolo 28, disciplina gli obblighi di comunicazione nei confronti dell'Autorità di vigilanza, in linea con quanto già previsto nella circolare 577.

Il Capo VIII assume particolare rilievo, in quanto disciplina, per la prima volta in modo organico, l'esternalizzazione di attività e funzioni delle imprese di assicurazione. Il mercato assicurativo nazionale ed internazionale sta mostrando una crescente tendenza verso l'adozione di nuovi modelli organizzativi che prevedono l'affidamento di attività o di alcune fasi di esse a soggetti terzi, giuridicamente autonomi, appartenenti o meno al medesimo gruppo dell'impresa. Tale tendenza necessita di un appropriato quadro regolamentare, come peraltro riconosciuto a livello internazionale; nel delineare i nuovi principi, si è tenuto conto in particolare delle linee guida definite dal *Joint Forum* nel documento "*Outsourcing in Financial Services*" del febbraio 2005.

La sezione I del Capo enuncia i presupposti formali e sostanziali cui è subordinata la possibilità di esternalizzazione e specifica la portata dei poteri di intervento dell'Autorità.

L'articolo 29 individua un duplice ordine di limiti alla facoltà di esternalizzazione:

- la natura e la quantità delle attività cedute all'esterno e le modalità della cessione non devono trasformare l'impresa cedente in una "scatola vuota";
- in conformità ai principi internazionali comunemente accettati che riconoscono l'esistenza di funzioni assolutamente non affidabili a soggetti esterni, è fatto divieto di esternalizzare l'attività di sottoscrizione dei rischi – che rappresenta il *core business* delle imprese di assicurazione.

Resta naturalmente fermo il principio che l'esternalizzazione di funzioni non può in alcun modo esonerare gli organi sociali e l'alta direzione dalle proprie responsabilità.

L'articolo 30 sottopone a particolari cautele l'esternalizzazione di attività essenziali o importanti, vale dire di quelle la cui mancata o anomala esecuzione comprometterebbe gravemente la capacità dell'impresa di continuare a conformarsi alle condizioni richieste per la conservazione dell'autorizzazione all'esercizio oppure comprometterebbe gravemente i suoi risultati finanziari, la sua stabilità o la continuità e qualità dei servizi verso gli assicurati (si pensi alla gestione degli investimenti e dei sinistri).

In tali casi le imprese devono garantire che l'esternalizzazione non pregiudichi il proprio sistema di *governance*, né la stabilità finanziaria o la capacità di prestare adeguatamente i propri servizi agli assicurati e ai danneggiati, né determini un ingiustificato incremento del rischio operativo.

E' richiesto, poi, dall'articolo 31, che la politica di esternalizzazione sia previamente definita da una delibera dell'organo amministrativo che deve includere almeno i criteri di selezione dei fornitori sotto il profilo della professionalità, onorabilità e capacità finanziaria, nonché l'adozione di metodi che consentano di verificare il rispetto di livelli minimi di servizio ovvero il raggiungimento di risultati prestabiliti da parte del fornitore.

L'articolo 32 indica le condizioni necessarie da soddisfare nella stipulazione degli accordi di esternalizzazione in un'ottica di salvaguardia delle qualità del servizio e di agevolazione dell'attività di vigilanza dell'Autorità.

L'articolo 33 indica gli obiettivi a cui devono tendere i controlli dell'impresa sul fornitore e sulla esecuzione delle attività esternalizzate: in generale va garantito il rispetto di standard di controllo almeno pari a quelli che sarebbero previsti se le attività fossero svolte direttamente dall'impresa. A tal fine le imprese sono tenute ad individuare idonei presidi organizzativi e contrattuali che consentano di controllare costantemente le attività esternalizzate al fine di verificare la loro conformità a norme di legge e alle direttive aziendali, nonché alle soglie di tolleranza al rischio predefinite dall'impresa. I meccanismi adottati devono garantire alle imprese di intervenire tempestivamente ogniqualvolta i soggetti affidatari non rispettino gli impegni o la qualità dei servizi resi sia inferiore ai livelli e agli obiettivi predefiniti.

Le imprese devono inoltre prevedere appositi piani di emergenza e di reinternalizzazione delle attività cedute.

L'articolo 34 individua i poteri attribuiti all'ISVAP nelle ipotesi esternalizzazione.

E' previsto che all'Autorità sia consentito richiedere modifiche al contratto ovvero, nei casi più gravi, il recesso dallo stesso, qualora tale intervento sia reso necessario per garantire la sana e prudente gestione dell'impresa assicurativa o la tutela degli assicurati.

La sezione II definisce gli obblighi di comunicazione nei confronti dell'ISVAP, alcuni dei quali già previsti nel vigente assetto normativo. Tali adempimenti sono diversificati a seconda che l'esternalizzazione riguardi:

- funzioni essenziali o importanti (art. 35);
- le funzioni di revisione interna, di *risk management* e di *compliance* (art. 36);
- altre attività (art. 37).

Nel primo caso, in ragione della rilevanza delle attività cedute, è richiesta una comunicazione preventiva al fine di consentire alla Vigilanza la tempestiva conoscenza delle scelte organizzative dell'impresa; analoga informativa deve essere resa nelle ipotesi di cessazione del rapporto.

Nella seconda ipotesi, in considerazione del fatto che le funzioni interessate al processo di esternalizzazione sono coinvolte in delicate funzioni di controllo, è richiesta la comunicazione preventiva della bozza del contratto, finalizzata a consentire all'Autorità di effettuare, prima della sua esecuzione, una verifica più stringente circa la conformità alle disposizioni del Regolamento. La comunicazione dà avvio ad un procedimento che prevede un meccanismo di silenzio assenso, decorsi sessanta giorni senza rilievi da parte dell'Autorità.

In tutti gli altri casi di esternalizzazione di funzioni non rilevanti (quali ad es. l'affidamento a terzi dei servizi di sicurezza dei locali, di formazione del personale, di manutenzione...) è, invece, richiesta una comunicazione *ex post*, da effettuarsi in occasione della trasmissione del bilancio di esercizio.

Infine, il Capo IX reca le disposizioni transitorie e finali.