



Istituto per la Vigilanza sulle Assicurazioni Private e di Interesse Collettivo

REGOLAMENTO N. 20 DEL 26 MARZO 2008

REGOLAMENTO 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

L'ISVAP

(Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo)

VISTA la legge 12 agosto 1982, n. 576 e successive modificazioni ed integrazioni, concernente la riforma della vigilanza sulle assicurazioni;

VISTO il decreto legislativo 7 settembre 2005, n. 209 e successive modificazioni ed integrazioni, recante il Codice delle Assicurazioni Private;

adotta il seguente:

REGOLAMENTO

INDICE

Capo I – Disposizioni di carattere generale

- Art. 1 (Fonti normative)
- Art. 2 (Definizioni)
- Art. 3 (Ambito di applicazione)

Capo II – Sistema dei controlli interni

Sezione I – Principi generali

- Art. 4 (Obiettivi del sistema dei controlli interni)

Sezione II – Ruolo degli organi sociali

- Art. 5 (Organo amministrativo)
- Art. 6 (Comitato per il controllo interno)
- Art. 7 (Alta direzione)
- Art. 8 (Organo di controllo)

Art. 9 (Formalizzazione degli atti)

Sezione III – Componenti del sistema dei controlli interni

Art. 10 (Cultura del controllo interno)

Art. 11 (Attività di controllo e separazione dei compiti)

Art. 12 (Flussi informativi e canali di comunicazione)

Art. 13 (Funzione per la produzione di dati e informazioni ai fini della vigilanza supplementare)

Art. 14 (Sistemi informatici)

Capo III – Revisione interna

Art. 15 (Funzione di revisione interna)

Art. 16 (Esternalizzazione della funzione di revisione interna)

Art. 17 (Collaborazione tra funzioni e organi deputati al controllo)

Capo IV – Gestione dei rischi

Art. 18 (Obiettivi del sistema di gestione dei rischi)

Art. 19 (Individuazione e valutazione dei rischi)

Art. 20 (*Stress test*)

Art. 21 (Funzione di *risk management*)

Capo V – Funzione di *compliance*

Art. 22 (Obiettivi della verifica di conformità alle norme)

Art. 23 (Funzione di *compliance*)

Art. 24 (Responsabile della funzione di *compliance*)

Art. 25 (Esternalizzazione della funzione di *compliance*)

Capo VI – Disposizioni in materia di gruppo assicurativo

Art. 26 (Ruolo della capogruppo)

Art. 27 (Controllo interno e gestione dei rischi nel gruppo)

Capo VII – Obblighi di comunicazione all'ISVAP

Art. 28 (Comunicazioni all'ISVAP)

Capo VIII – Disposizioni in materia di esternalizzazione

Sezione I – Condizioni per l'esternalizzazione di attività

Art. 29 (Esternalizzazione di attività)

Art. 30 (Esternalizzazione di attività essenziali o importanti)

Art. 31 (Politica di esternalizzazione e scelta dei fornitori)

Art. 32 (Contratto di esternalizzazione)

Art. 33 (Controllo sulle attività esternalizzate)

Art. 34 (Poteri di intervento dell'ISVAP)

Sezione II – Obblighi di comunicazione all'ISVAP

Art. 35 (Comunicazione in caso di esternalizzazione di attività essenziali o importanti)

Art.36 (Esternalizzazione della funzione di revisione interna, di *risk management* e di *compliance*)

Art. 37 (Comunicazioni in caso di esternalizzazione di altre attività)

Capo IX – Disposizioni transitorie e finali

Art. 38 (Disposizioni transitorie)

Art. 39 (Abrogazione di norme)

Art. 40 (Pubblicazione)

Art. 41 (Entrata in vigore)

Elenco degli Allegati

Allegato 1	Modello di comunicazione per la esternalizzazione di attività essenziali o importanti
Allegato 2	Prospetto di comunicazione per l'esternalizzazione di attività diverse da quelle essenziali o importanti
Allegato 3	Prospetto riepilogativo dei contratti di esternalizzazione in vigore

Capo I – Disposizioni di carattere generale

Art. 1 (Fonti normative)

1. Il presente Regolamento è adottato ai sensi degli articoli 5, comma 2, 87, comma 1, 190, comma 1 e 191, comma 1, lettera c) del decreto legislativo 7 settembre 2005, n. 209.

Art. 2 (Definizioni)

1. Ai fini del presente Regolamento si intende per:
 - a) “alta direzione”: l'amministratore delegato, il direttore generale, nonché l'alta dirigenza che svolge compiti di sovrintendenza gestionale;
 - b) “attività essenziale o importante”: attività 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 risultati finanziari, la stabilità dell'impresa o la continuità e qualità dei servizi verso gli assicurati;
 - c) “attuario incaricato”: l'attuario incaricato dalle imprese di assicurazione ai sensi degli articoli 31, comma 1 e 34, comma 1, del decreto legislativo 7 settembre 2005, n. 209;
 - d) “capogruppo”: l'impresa di assicurazione o di riassicurazione o l'impresa di partecipazione assicurativa con sede legale in Italia come definita dall'articolo 83 del decreto legislativo 7 settembre 2005 n. 209 e dalle relative disposizioni di attuazione;
 - e) “decreto”: il decreto legislativo 7 settembre 2005, n. 209, recante il Codice delle assicurazioni private;
 - f) “esternalizzazione”: l'accordo tra un'impresa di assicurazione e un fornitore di servizi, anche se non autorizzato all'esercizio di attività assicurativa, in base al quale il fornitore realizza un processo, un servizio o un'attività che verrebbero altrimenti realizzati dalla stessa impresa di assicurazione;
 - g) “gruppo assicurativo”: gruppo di società di cui all'articolo 82 del decreto legislativo 7 settembre 2005, n. 209 e relative disposizioni di attuazione;
 - h) “ISVAP” o “Autorità”: l'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo;
 - i) “organo amministrativo”: il consiglio di amministrazione o, nelle imprese che hanno adottato il sistema di cui all'articolo 2409 *octies* del codice civile, il consiglio di gestione;
 - j) “organo di controllo”: il collegio sindacale o, nelle imprese che hanno adottato un sistema diverso da quello di cui all'articolo 2380, comma 1, del codice civile, il consiglio di sorveglianza o il comitato per il controllo sulla gestione;
 - k) “sede secondaria”: una sede che costituisce parte, sprovvista di personalità giuridica, di un'impresa di assicurazione o di riassicurazione e che effettua direttamente, in tutto o in parte, l'attività assicurativa o riassicurativa;
 - l) “S.E.E.”: lo Spazio Economico Europeo di cui all'accordo di estensione della normativa dell'Unione europea agli Stati appartenenti all'Associazione europea di libero scambio, firmato ad Oporto il 2 maggio 1992 e ratificato con legge 28 luglio 1993, n. 300;
 - m) “società di revisione”: la società di revisione contabile di cui all'articolo 102 del decreto legislativo 7 settembre 2005, n. 209;
 - n) “Stato membro”: uno Stato membro dell'Unione europea o uno Stato aderente allo Spazio economico europeo, come tale equiparato allo Stato membro dell'Unione europea;

- o) “Stato terzo”: uno Stato che non è membro dell’Unione Europea o non è aderente allo Spazio economico europeo;
- p) “*stress test*”: analisi qualitativa o quantitativa finalizzata a valutare l’impatto sulla situazione finanziaria delle imprese di andamenti sfavorevoli dei fattori di rischio, singolarmente considerati o combinati in un unico scenario.

Art. 3
(Ambito di applicazione)

1. Le disposizioni del presente Regolamento si applicano:
 - a) alle imprese di assicurazione e di riassicurazione con sede legale in Italia;
 - b) alle sedi secondarie in Italia di imprese di assicurazione con sede legale in uno Stato terzo;
 - c) alle sedi secondarie in Italia di imprese di riassicurazione con sede legale in uno Stato terzo;
 - d) alle capogruppo, limitatamente alle disposizioni di cui al Capo VI.

Capo II – Sistema dei controlli interni

Sezione I – Principi generali

Art. 4
(Obiettivi del sistema dei controlli interni)

1. Le imprese di assicurazione si dotano di un’idonea organizzazione amministrativa e contabile e di un adeguato sistema dei controlli interni, proporzionati alle dimensioni e alla caratteristiche operative dell’impresa e alla natura e alla intensità dei rischi aziendali.
2. Il sistema dei controlli interni è costituito dall’insieme delle regole, delle procedure e delle strutture organizzative volte ad assicurare il corretto funzionamento ed il buon andamento dell’impresa e a garantire, con un ragionevole margine di sicurezza:
 - a) l’efficienza e l’efficacia dei processi aziendali;
 - b) l’adeguato controllo dei rischi;
 - c) l’attendibilità e l’integrità delle informazioni contabili e gestionali;
 - d) la salvaguardia del patrimonio;
 - e) la conformità dell’attività dell’impresa alla normativa vigente, alle direttive e alle procedure aziendali.

Sezione II – Ruolo degli organi sociali

Art. 5
(Organo amministrativo)

1. L’organo amministrativo ha la responsabilità ultima del sistema dei controlli interni del quale deve assicurare la costante completezza, funzionalità ed efficacia, anche con riferimento alle attività esternalizzate. L’organo amministrativo assicura che il sistema di gestione dei rischi

consenta la identificazione, la valutazione e il controllo dei rischi maggiormente significativi, ivi compresi i rischi derivanti dalla non conformità alle norme.

2. Ai fini di cui al comma 1, l'organo amministrativo nell'ambito dei compiti di indirizzo strategico e organizzativo di cui all'articolo 2381 del codice civile:

- a) approva l'assetto organizzativo dell'impresa nonché l'attribuzione di compiti e responsabilità alle unità operative, curandone l'adeguatezza nel tempo;
- b) assicura che siano adottati e formalizzati adeguati processi decisionali e che sia attuata una appropriata separazione di funzioni;
- c) approva, curandone l'adeguatezza nel tempo, il sistema delle deleghe di poteri e responsabilità, avendo cura di evitare l'eccessiva concentrazione di poteri in un singolo soggetto e ponendo in essere strumenti di verifica sull'esercizio dei poteri delegati;
- d) definisce le direttive in materia di sistema dei controlli interni, rivedendole almeno una volta l'anno e curandone l'adeguamento alla evoluzione dell'operatività aziendale e delle condizioni esterne;
- e) definisce e, almeno una volta l'anno, valuta ai fini dell'eventuale revisione le strategie e le politiche di assunzione, valutazione e gestione dei rischi maggiormente significativi, in coerenza con il livello di adeguatezza patrimoniale dell'impresa; sulla base dei risultati dei processi di individuazione e valutazione dei rischi, fissa i livelli di tolleranza al rischio e li rivede almeno una volta l'anno;
- f) definisce, ove ne ricorrano i presupposti, le direttive e i criteri per la circolazione e la raccolta dei dati e delle informazioni utili a fini dell'esercizio della vigilanza supplementare di cui al Titolo XV del decreto, nonché le direttive in materia di controllo interno per la verifica della completezza e tempestività dei relativi flussi informativi;
- g) verifica che l'alta direzione implementi correttamente il sistema dei controlli interni e di gestione dei rischi secondo le direttive impartite e che ne valuti la funzionalità e l'adeguatezza;
- h) richiede di essere periodicamente informato sulla efficacia e adeguatezza del sistema di controllo interno e di gestione dei rischi e che gli siano riferite con tempestività le criticità più significative, siano esse individuate dall'alta direzione, dalla funzione di revisione interna, dal personale, impartendo con tempestività le direttive per l'adozione di misure correttive;
- i) individua particolari eventi o circostanze che richiedono un immediato intervento da parte dell'alta direzione.

Art. 6

(Comitato per il controllo interno)

1. Per l'espletamento dei compiti relativi al sistema dei controlli interni, l'organo amministrativo può costituire un Comitato di controllo interno, composto da amministratori non esecutivi, preferibilmente indipendenti ai sensi dell'articolo 2387 codice civile, al quale affidare funzioni consultive e propositive.
2. In particolare il Comitato di controllo interno assiste l'organo amministrativo nella determinazione delle linee di indirizzo del sistema dei controlli interni, nella verifica periodica della sua adeguatezza e del suo effettivo funzionamento, nell'identificazione e gestione dei principali rischi aziendali.
3. L'organo amministrativo definisce la composizione, i compiti e le modalità di funzionamento del Comitato. L'istituzione del Comitato di controllo interno non solleva l'organo amministrativo dalle proprie responsabilità.

Art. 7
(Alta direzione)

1. L'alta direzione è responsabile dell'attuazione, del mantenimento e del monitoraggio del sistema dei controlli interni e di gestione dei rischi, ivi compresi quelli derivanti dalla non conformità alle norme, coerentemente con le direttive dell'organo amministrativo.
2. L'alta direzione:
 - a) definisce in dettaglio l'assetto organizzativo dell'impresa, i compiti e le responsabilità delle unità operative e dei relativi addetti, nonché i processi decisionali in coerenza con le direttive impartite dall'organo amministrativo; in tale ambito attua l'appropriata separazione di compiti sia tra singoli soggetti che tra funzioni in modo da evitare, per quanto possibile, l'insorgere di conflitti di interesse;
 - b) attua le politiche di assunzione, valutazione e gestione dei rischi fissate dall'organo amministrativo, assicurando la definizione di limiti operativi e la tempestiva verifica dei limiti medesimi, nonché il monitoraggio delle esposizioni ai rischi e il rispetto dei livelli di tolleranza;
 - c) cura il mantenimento della funzionalità e dell'adeguatezza complessiva dell'assetto organizzativo, del sistema dei controlli interni e di gestione dei rischi, incluso il rischio di non conformità alle norme;
 - d) verifica che l'organo amministrativo sia periodicamente informato sull'efficacia e sull'adeguatezza del sistema dei controlli interni e di gestione dei rischi e della funzione di *compliance* e comunque tempestivamente ogni qualvolta siano riscontrate criticità significative;
 - e) dà attuazione alle indicazioni dell'organo amministrativo in ordine alle misure da adottare per correggere le anomalie riscontrate e apportare miglioramenti;
 - f) propone all'organo amministrativo iniziative volte all'adeguamento ed al rafforzamento del sistema dei controlli interni e di gestione dei rischi.

Art. 8
(Organo di controllo)

1. L'organo di controllo verifica l'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dall'impresa e il suo concreto funzionamento.
2. Per l'espletamento dei compiti di cui al comma 1 l'organo di controllo può richiedere la collaborazione di tutte le strutture che svolgono funzioni di controllo.
3. L'organo di controllo:
 - a) acquisisce, all'inizio del mandato, conoscenze sull'assetto organizzativo aziendale ed esamina i risultati del lavoro della società di revisione per la valutazione del sistema di controllo interno e del sistema amministrativo contabile;
 - b) verifica l'idoneità della definizione delle deleghe, nonché l'adeguatezza dell'assetto organizzativo prestando particolare attenzione alla separazione di responsabilità nei compiti e nelle funzioni;
 - c) valuta l'efficienza e l'efficacia del sistema dei controlli interni, con particolare riguardo all'operato della funzione di revisione interna della quale deve verificare la sussistenza della necessaria autonomia, indipendenza e funzionalità; nell'ipotesi in cui tale funzione sia stata esternalizzata valuta il contenuto dell'incarico sulla base del relativo contratto;
 - d) mantiene un adeguato collegamento con la funzione di revisione interna;

- e) cura il tempestivo scambio con la società di revisione dei dati e delle informazioni rilevanti per l'espletamento dei propri compiti, esaminando anche le periodiche relazioni della società di revisione;
- f) segnala all'organo amministrativo le eventuali anomalie o debolezze dell'assetto organizzativo e del sistema dei controlli interni indicando e sollecitando idonee misure correttive; nel corso del mandato pianifica e svolge, anche coordinandosi con la società di revisione, periodici interventi di vigilanza volti ad accertare se le carenze o anomalie segnalate siano state superate e se, rispetto a quanto verificato all'inizio del mandato, siano intervenute significative modifiche dell'operatività della società che impongano un adeguamento dell'assetto organizzativo e del sistema dei controlli interni;
- g) in caso di società appartenenti al medesimo gruppo assicurativo assicura i collegamenti funzionali ed informativi con gli organi di controllo delle altre imprese;
- h) conserva una adeguata evidenza delle osservazioni e delle proposte formulate e della successiva attività di verifica dell'attuazione delle eventuali misure correttive.

Art. 9
(Formalizzazione degli atti)

1. L'operato dell'organo amministrativo, direttivo e di controllo è adeguatamente documentato, al fine di consentire il controllo sugli atti gestionali e sulle decisioni assunte.

Sezione III - Componenti del sistema dei controlli interni

Art. 10
(Cultura del controllo interno)

1. L'organo amministrativo promuove un alto livello di integrità e una cultura del controllo interno tale da sensibilizzare l'intero personale sull'importanza e utilità dei controlli interni.
2. L'alta direzione è responsabile della promozione della cultura del controllo interno e assicura che il personale sia messo a conoscenza del proprio ruolo e delle proprie responsabilità, in modo da essere effettivamente impegnato nello svolgimento dei controlli, intesi quale parte integrante della propria attività. A tal fine assicura la formalizzazione e l'adeguata diffusione tra il personale del sistema delle deleghe e delle procedure che regolano l'attribuzione di compiti, i processi operativi e i canali di reportistica.
3. L'alta direzione promuove continue iniziative formative e di comunicazione volte a favorire l'effettiva adesione di tutto il personale ai principi di integrità morale ed ai valori etici.
4. Al fine di promuovere la correttezza operativa ed il rispetto dell'integrità e dei valori etici da parte di tutto il personale, nonché per prevenire condotte devianti di cui possono essere chiamate a rispondere ai sensi del decreto legislativo 8 giugno 2001, n. 231, nonché ai sensi dell'articolo 325 del decreto legislativo 7 settembre 2005, n. 209, le imprese adottano un codice etico che definisca le regole comportamentali, disciplini le situazioni di potenziale conflitto di interesse e preveda azioni correttive adeguate, nel caso di deviazione dalle direttive e dalle procedure approvate dal vertice o di infrazione della normativa vigente e dello stesso codice etico.
5. Le imprese evitano, ad ogni livello aziendale, politiche e pratiche di remunerazione che possano essere di incentivo ad attività illegali o devianti rispetto agli standard etico-legali ovvero indurre propensioni al rischio contrastanti con l'interesse della società.

Art. 11

(Attività di controllo e separazione dei compiti)

1. Il sistema dei controlli interni prevede l'esecuzione, a tutti i livelli dell'impresa, di attività di controllo proporzionate alle dimensioni, natura e complessità degli affari, che contribuiscono a garantire l'attuazione delle direttive aziendali e a verificarne il rispetto.
2. Le attività di controllo di cui al comma 1 sono formalizzate e riviste su base periodica e coinvolgono tutto il personale. Tali attività comprendono meccanismi di doppie firme, autorizzazioni, verifiche e raffronti, liste di controllo e riconciliazione dei conti, nonché la limitazione dell'accesso alle operazioni ai soli soggetti incaricati e la registrazione e la verifica periodica delle operazioni effettuate.
3. Compatibilmente con le dimensioni aziendali, le imprese assicurano, nell'ambito delle funzioni aziendali, un adeguato livello di indipendenza del personale incaricato del controllo rispetto a quello con compiti operativi.

Art. 12

(Flussi informativi e canali di comunicazione)

1. Le imprese devono possedere informazioni contabili e gestionali che garantiscano adeguati processi decisionali e consentano di definire e valutare se siano stati raggiunti gli obiettivi strategici fissati dall'organo amministrativo in modo da sottoporli ad eventuale revisione. A tal fine, l'alta direzione assicura che l'organo amministrativo abbia una conoscenza completa dei fatti aziendali rilevanti, anche attraverso la predisposizione di un'adeguata reportistica.
2. Il sistema dei controlli interni garantisce che le informazioni rispettino i principi di accuratezza, completezza, tempestività, coerenza, trasparenza e pertinenza così definiti:
 - a) *accuratezza*: le informazioni devono essere verificate al momento della ricezione e anteriormente rispetto al loro uso;
 - b) *completezza*: le informazioni devono coprire tutti gli aspetti rilevanti dell'impresa in termini di quantità e qualità, inclusi gli indicatori che possono avere conseguenze dirette o indirette sulla pianificazione strategica dell'attività;
 - c) *tempestività*: le informazioni devono essere puntualmente disponibili, in modo da favorire processi decisionali efficaci e consentire all'impresa di prevedere e reagire con prontezza agli eventi futuri;
 - d) *coerenza*: le informazioni devono essere registrate secondo metodologie che le rendano confrontabili;
 - e) *trasparenza*: le informazioni devono essere presentate in maniera facile da interpretare, garantendo la chiarezza delle componenti essenziali;
 - f) *pertinenza*: le informazioni utilizzate devono essere in relazione diretta con la finalità per cui vengono richieste ed essere continuamente rivedute e ampliate per garantirne la rispondenza alle necessità dell'impresa.
3. Le informazioni dirette a terzi, quali l'Autorità, gli assicurati, il mercato, devono essere attendibili, tempestive, pertinenti e devono essere comunicate in maniera chiara ed efficace.
4. Il sistema delle rilevazioni contabili e gestionali interne registra correttamente i fatti di gestione e fornisce una rappresentazione corretta e veritiera della situazione patrimoniale, finanziaria ed economica dell'impresa e in conformità con le leggi e la normativa secondaria.

5. Le imprese istituiscono e mantengono canali di comunicazione efficaci sia all'interno, in ogni direzione, sia all'esterno.
6. Il sistema deve favorire le segnalazioni di criticità anche attraverso la previsione di modalità che consentano al personale di portare direttamente all'attenzione dei livelli gerarchici più elevati le situazioni di particolare gravità.

Art. 13

(Produzione di dati e informazioni ai fini della vigilanza supplementare)

1. Le imprese istituiscono efficaci flussi informativi per la produzione di dati e di informazioni utili ai fini dell'esercizio della vigilanza supplementare, ove applicabile, adottando idonee procedure di controllo interno ed individuando una funzione specifica per la produzione di tali dati e informazioni.
2. Le imprese conservano i dati e le informazioni di cui al comma 1 presso la propria sede, per eventuali verifiche da parte dell'ISVAP.

Art. 14

(Sistemi informatici)

1. I sistemi informatici devono essere appropriati rispetto alle dimensioni e all'attività dell'impresa e devono fornire informazioni, sia all'interno che all'esterno, rispondenti ai principi di cui all'articolo 12, comma 2.
2. Ai fini di cui al comma 1:
 - a) l'organo amministrativo approva un piano strategico sulla tecnologia della informazione e comunicazione (ICT), volto ad assicurare l'esistenza e il mantenimento di una architettura complessiva dei sistemi altamente integrata sia dal punto di vista applicativo che tecnologico e adeguata ai bisogni dell'impresa;
 - b) gli ambienti di sviluppo e di produzione sono separati. Gli accessi ai diversi ambienti sono regolamentati e controllati attraverso procedure disegnate tenendo conto dell'esigenza di limitare i rischi di frode derivanti da intrusioni esterne o da infedeltà del personale. A tal fine le procedure garantiscono la sicurezza logica dei dati trattati, restringendo, in particolare per l'ambiente di produzione, l'accesso ai dati stessi a soggetti autorizzati e prevedono che tutte le violazioni vengano evidenziate; le procedure sono soggette a verifiche da parte della funzione di revisione interna;
 - c) le procedure per l'approvazione e l'acquisizione dell'*hardware* e del *software*, nonché per la cessione all'esterno di determinati servizi, sono formalizzate;
 - d) sono adottate procedure che assicurino la sicurezza fisica dell'*hardware*, del *software* e delle banche dati, anche attraverso procedure di *disaster recovery* e *back up*;
 - e) al fine di garantire la continuità dei processi dell'organizzazione, sono adottate e documentate procedure e standard operativi orientati alla individuazione e gestione degli eventi che possono pregiudicare la continuità del *business*, quali, in via esemplificativa, eventi imprevisti, *black-out*, incendi, allagamenti, malfunzionamenti dei componenti *hardware* e *software*, errori operativi da parte del personale incaricato della gestione dei sistemi o da parte degli utenti, introduzione involontaria di componenti dannosi per il sistema informativo e di rete, atti dolosi miranti a ridurre la disponibilità delle informazioni.
3. In caso di operazioni straordinarie quali fusioni o acquisizioni di portafoglio, l'impresa predisponde un piano di integrazione dei sistemi informatici nel quale sono specificati:

- a) ambiti, funzioni, procedure, applicazioni e basi dati interessate dal processo di integrazione;
- b) la tempistica associata a ciascuna fase dell'integrazione con particolare riguardo alla migrazione delle basi dati e alle date a partire dalle quali l'integrazione dei portafogli (premi, sinistri etc.) sarà completata;
- c) le unità e i presidi organizzativi ai quali sono affidati i controlli ed il monitoraggio dell'intero processo di integrazione.

Capo III – Revisione interna

Art. 15

(Funzione di revisione interna)

1. Le imprese istituiscono una funzione di revisione interna, incaricata di monitorare e valutare l'efficacia e l'efficienza del sistema di controllo interno e le necessità di adeguamento, anche attraverso attività di supporto e di consulenza alle altre funzioni aziendali.
2. La funzione di revisione interna deve presentare le seguenti caratteristiche:
 - a) la collocazione della funzione nell'ambito della struttura organizzativa deve essere tale da garantirne l'indipendenza e l'autonomia, affinché non ne sia compromessa l'obiettività di giudizio; la funzione di revisione interna non dipende gerarchicamente da alcun responsabile di aree operative; ai soggetti preposti alla funzione di revisione interna non devono essere affidate responsabilità operative o incarichi di verifica di attività per le quali abbiano avuto in precedenza autorità o responsabilità se non sia trascorso un ragionevole periodo di tempo;
 - b) il responsabile della funzione è nominato dall'organo amministrativo: egli deve avere specifica competenza e professionalità per lo svolgimento dell'attività; i compiti attribuiti al responsabile della funzione sono chiaramente definiti ed approvati con delibera del consiglio, che ne fissa anche poteri, responsabilità e modalità di reportistica all'organo amministrativo stesso;
 - c) agli incaricati della funzione deve essere consentita libertà di accesso a tutte le strutture aziendali e alla documentazione relativa all'area aziendale oggetto di verifica, incluse le informazioni utili per la verifica dell'adeguatezza dei controlli svolti sulle funzioni aziendali esternalizzate;
 - d) la funzione deve avere collegamenti organici con tutti i centri titolari di funzioni di controllo interno; il responsabile della funzione è dotato dell'autorità necessaria a garantire l'indipendenza della stessa;
 - e) la struttura dedicata deve essere adeguata in termini di risorse umane e tecnologiche alle dimensioni dell'impresa ed agli obiettivi di sviluppo che la stessa intende perseguire. Gli addetti alla struttura devono possedere competenze specialistiche e deve essere curato l'aggiornamento professionale.
3. La funzione di revisione interna uniforma la propria attività agli standard professionali comunemente accettati a livello nazionale ed internazionale e verifica:
 - a) i processi gestionali e le procedure organizzative;
 - b) la regolarità e la funzionalità dei flussi informativi tra settori aziendali;
 - c) l'adeguatezza dei sistemi informativi e la loro affidabilità affinché non sia inficiata la qualità delle informazioni sulle quali il vertice aziendale basa le proprie decisioni;
 - d) la rispondenza dei processi amministrativo contabili a criteri di correttezza e di regolare tenuta della contabilità;
 - e) l'efficienza dei controlli svolti sulle attività esternalizzate.

4. La funzione di revisione interna pianifica l'attività in modo da identificare le aree da sottoporre prioritariamente ad *audit*. Il piano di *audit* è sottoposto all'approvazione dell'organo amministrativo e individua, almeno, le attività a rischio, le operazioni e i sistemi da verificare, descrivendo i criteri sulla base dei quali questi sono stati selezionati e specificando le risorse necessarie all'esecuzione del piano. Analogo procedimento è seguito in caso di variazioni significative ai piani approvati, che comunque sono organizzati in modo da fronteggiare le esigenze impreviste.
5. A seguito dell'analisi sull'attività oggetto di controllo, la funzione procede, secondo le modalità e la periodicità fissata dall'organo amministrativo, a comunicare all'organo stesso, all'alta direzione ed all'organo di controllo la valutazione delle risultanze e le eventuali disfunzioni e criticità; resta fermo l'obbligo di segnalare con urgenza all'organo amministrativo e a quello di controllo le situazioni di particolare gravità. I rapporti di audit devono essere obiettivi, chiari, concisi, tempestivi e contenere suggerimenti per eliminare le carenze riscontrate e devono essere conservati presso la sede della società.
6. La revisione interna si conclude con l'attività di follow-up, consistente nella verifica a distanza di tempo dell'efficacia delle correzioni apportate al sistema.

Art. 16

(Esterneizzazione della funzione di revisione interna)

1. Le imprese per le quali, per le ridotte dimensioni e per le caratteristiche operative, l'istituzione della funzione di revisione interna non risponda a criteri di economicità, possono esternalizzare tale funzione, anche nell'ambito del gruppo assicurativo, nel rispetto delle condizioni di cui al Capo VIII.
2. Le attività relative alla funzione di revisione interna possono essere accentrate all'interno del gruppo assicurativo attraverso la costituzione di un'unità specializzata, a condizione che:
 - a) in ciascuna impresa del gruppo assicurativo sia individuato un referente che curi i rapporti con il responsabile della funzione di gruppo;
 - b) siano adottate adeguate procedure per garantire che le attività della funzione di revisione interna definite a livello di gruppo assicurativo siano adeguatamente calibrate rispetto alle caratteristiche operative della singola impresa.

Art. 17

(Collaborazione tra funzioni e organi deputati al controllo)

1. L'organo di controllo, la società di revisione, la funzione di revisione interna, di *risk management* e di *compliance*, l'organismo di vigilanza di cui al decreto legislativo 8 giugno 2001, n. 231, l'attuario incaricato e ogni altro organo o funzione a cui è attribuita una specifica funzione di controllo collaborano tra di loro, scambiandosi ogni informazione utile per l'espletamento dei rispettivi compiti.
2. L'organo amministrativo definisce e formalizza i collegamenti tra le varie funzioni a cui sono attribuiti compiti di controllo.

Capo IV – Gestione dei rischi

Art. 18

(Obiettivi del sistema di gestione dei rischi)

1. Al fine di mantenere ad un livello accettabile, coerente con le disponibilità patrimoniali dell'impresa, i rischi a cui sono esposte, le imprese si dotano di un adeguato sistema di gestione dei rischi, proporzionato alle dimensioni, alla natura e alla complessità dell'attività esercitata, che consenta la identificazione, la valutazione e il controllo dei rischi maggiormente significativi, intendendosi per tali i rischi le cui conseguenze possono minare la solvibilità dell'impresa o costituire un serio ostacolo alla realizzazione degli obiettivi aziendali.
2. Le imprese provvedono alla catalogazione dei rischi in funzione della natura e dimensioni dell'attività. La catalogazione include almeno i seguenti rischi:
 - a) **rischio di assunzione**: il rischio derivante dalla sottoscrizione dei contratti di assicurazione, associato agli eventi coperti, ai processi seguiti per la tariffazione e selezione dei rischi, all'andamento sfavorevole della sinistralità effettiva rispetto a quella stimata;
 - b) **rischio di riservazione**: il rischio legato alla quantificazione di riserve tecniche non sufficienti rispetto agli impegni assunti verso assicurati e danneggiati;
 - c) **rischio di mercato**: il rischio di perdite in dipendenza di variazioni dei tassi di interesse, dei corsi azionari, dei tassi di cambio e dei prezzi degli immobili;
 - d) **rischio di credito**: il rischio legato all'inadempimento contrattuale degli emittenti degli strumenti finanziari, dei riassicuratori, degli intermediari e di altre controparti;
 - e) **rischio di liquidità**: il rischio di non poter adempiere alle obbligazioni verso gli assicurati e altri creditori a causa della difficoltà a trasformare gli investimenti in liquidità senza subire perdite;
 - f) **rischio operativo**: il rischio di perdite derivanti da inefficienze di persone, processi e sistemi, inclusi quelli utilizzati per la vendita a distanza, o da eventi esterni, quali la frode o l'attività dei fornitori di servizi;
 - g) **rischio legato all'appartenenza al gruppo**: rischio di "contagio", inteso come rischio che, a seguito dei rapporti intercorrenti dall'impresa con le altre entità del gruppo, situazioni di difficoltà che insorgono in un'entità del medesimo gruppo possano propagarsi con effetti negativi sulla solvibilità dell'impresa stessa; rischio di conflitto di interessi;
 - h) **rischio di non conformità alle norme**: il rischio di incorrere in sanzioni giudiziarie o amministrative, subire perdite o danni reputazionali in conseguenza della mancata osservanza di leggi, regolamenti o provvedimenti delle Autorità di vigilanza ovvero di norme di autoregolamentazione, quali statuti, codici di condotta o codici di autodisciplina; rischio derivante da modifiche sfavorevoli del quadro normativo o degli orientamenti giurisprudenziali;
 - i) **rischio reputazionale**: il rischio di deterioramento dell'immagine aziendale e di aumento della conflittualità con gli assicurati, dovuto anche alla scarsa qualità dei servizi offerti, al collocamento di polizze non adeguate o al comportamento della rete di vendita.

Art. 19

(Individuazione e valutazione dei rischi)

1. Le imprese raccolgono in via continuativa informazioni sui rischi, interni ed esterni, esistenti e prospettici, a cui sono esposte e che possono interessare tutti i processi operativi e le aree funzionali. La procedura di censimento dei rischi e i relativi risultati sono adeguatamente documentati.

2. Le imprese devono essere in grado, attraverso un adeguato processo di analisi, di comprendere la natura dei rischi individuati, la loro origine, la possibilità o necessità di controllarli e gli effetti che ne possono derivare, sia in termini di perdite che di opportunità. Il processo di analisi include sia una valutazione qualitativa sia, per i rischi quantificabili, l'adozione di metodologie di misurazione dell'esposizione al rischio, inclusi, ove appropriati, sistemi di determinazione dell'ammontare della massima perdita potenziale.
3. Nella misurazione le imprese considerano, ove possibile, le interrelazioni tra i rischi, valutandoli sia singolarmente sia su base aggregata.
4. Le metodologie di valutazione e misurazione dei rischi e i relativi risultati sono adeguatamente documentati.
5. Le politiche di assunzione, misurazione e gestione dei rischi sono definite e implementate avendo a riferimento la visione integrata delle attività e delle passività di bilancio, considerando che lo sviluppo di tecniche e modelli di *asset-liability management* è fondamentale per la corretta comprensione e la gestione delle esposizioni al rischio che possono derivare dalle interrelazioni e dal mancato equilibrio tra attività e passività.
6. I processi di individuazione e valutazione dei rischi sono effettuati su base continuativa, per tenere conto sia delle intervenute modifiche nella natura e dimensione degli affari e nel contesto di mercato, sia dell'insorgenza di nuovi rischi o del cambiamento di quelli esistenti. Particolare attenzione è posta alla valutazione dei rischi nascenti dall'offerta di nuovi prodotti o dall'ingresso in nuovi mercati.
7. Le imprese definiscono procedure in grado di evidenziare con tempestività l'insorgere di rischi che possono danneggiare la situazione patrimoniale ed economica o il superamento delle soglie di tolleranza fissate. Per le maggiori fonti di rischio identificate l'impresa predispone adeguati piani di emergenza.

Art. 20
(*Stress test*)

1. Per ciascuna delle fonti di rischio identificate dalle imprese come maggiormente significative sulla base dei processi di cui all'articolo 19, le imprese stesse effettuano analisi prospettiche quantitative attraverso l'uso di *stress test*.
2. Gli *stress test*, basati su modelli deterministici o stocastici, sono disegnati e sviluppati in coerenza con le dimensioni e la natura dell'attività dell'impresa e ripetuti con la frequenza resa necessaria dal tipo di rischio, dall'evoluzione delle dimensioni e dell'attività dell'impresa e del contesto di mercato, e in ogni caso con cadenza almeno annuale.
3. I risultati degli *stress test*, unitamente alle ipotesi sottostanti, sono portati all'attenzione dell'organo amministrativo, al fine di offrire un contributo alla revisione e al miglioramento delle politiche di gestione dei rischi, delle linee operative e dei limiti di esposizione fissati dall'organo amministrativo stesso.
4. Se i risultati delle prove di *stress* indicano una particolare vulnerabilità di fronte a una data serie di circostanze, le imprese adottano idonee misure per gestire adeguatamente i relativi rischi.
5. Su richiesta dell'ISVAP, le imprese effettuano *stress test* standardizzati sulla base di fattori di rischio e parametri prefissati dall'ISVAP stesso.

Art. 21
(Funzione di *risk management*)

1. Le imprese istituiscono una funzione di *risk management*, appropriata alla natura, dimensione e complessità dell'attività, che:
 - a) concorre alla definizione delle metodologie di misurazione dei rischi;
 - b) concorre alla definizione dei limiti operativi assegnati alle strutture operative e definisce le procedure per la tempestiva verifica dei limiti medesimi;
 - c) valida i flussi informativi necessari ad assicurare il tempestivo controllo delle esposizioni ai rischi e l'immediata rilevazione delle anomalie riscontrate nell'operatività;
 - d) predispone la reportistica nei confronti dell'organo amministrativo, dell'alta direzione e dei responsabili delle strutture operative circa l'evoluzione dei rischi e la violazione dei limiti operativi fissati;
 - e) verifica la coerenza dei modelli di misurazione dei rischi con l'operatività svolta dalla impresa
 - f) concorre all'effettuazione delle prove di *stress test* di cui all'articolo 20.
2. La collocazione organizzativa della funzione di *risk management* è lasciata all'autonomia delle imprese, nel rispetto del principio di separatezza tra funzioni operative e di controllo. Le imprese valutano se utilizzare unità interne o avvalersi di strutture esterne nel rispetto dei criteri di cui al Capo VIII.
3. Le attività relative alla funzione di *risk management* possono essere accentrate all'interno del gruppo assicurativo attraverso la costituzione di un'unità specializzata, a condizione che:
 - a) in ciascuna impresa del gruppo assicurativo sia individuato un referente che curi i rapporti con il responsabile della funzione di gruppo;
 - b) siano adottate adeguate procedure per garantire che le attività della funzione di *risk management* definite a livello di gruppo assicurativo siano adeguatamente calibrate rispetto al profilo di rischio della singola impresa.
4. La funzione di *risk management*, anche quando non costituita in forma di specifica unità organizzativa, risponde all'organo amministrativo. La collocazione organizzativa della funzione di *risk management* deve essere tale da non dipendere da funzioni operative.
5. Il collegamento tra la funzione di revisione interna e quella di *risk management* è definito e formalizzato dall'organo amministrativo.

Capo V – Funzione di *compliance*

Art. 22
(Obiettivi della verifica di conformità alle norme)

1. Nell'ambito del sistema dei controlli interni, le imprese si dotano, ad ogni livello aziendale pertinente, di specifici presidi volti a prevenire il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite patrimoniali o danni di reputazione, in conseguenza di violazioni di leggi, regolamenti o provvedimenti delle Autorità di vigilanza ovvero di norme di autoregolamentazione.

2. Nella identificazione e valutazione del rischio di non conformità alle norme, le imprese pongono particolare attenzione al rispetto delle norme relative alla trasparenza e correttezza dei comportamenti nei confronti degli assicurati e danneggiati, all'informativa precontrattuale e contrattuale, alla corretta esecuzione dei contratti, con particolare riferimento alla gestione dei sinistri e, più in generale, alla tutela del consumatore.

Art. 23
(Funzione di *compliance*)

1. Le imprese istituiscono una funzione di *compliance*, proporzionata alla natura, dimensione e complessità dell'attività svolta, cui è affidato il compito di valutare che l'organizzazione e le procedure interne siano adeguate al raggiungimento degli obiettivi di cui all'articolo 22.
2. L'istituzione della funzione di *compliance* è formalizzata in una specifica delibera dell'organo amministrativo, che ne definisce le responsabilità, i compiti, le modalità operative, la natura e la frequenza della reportistica agli organi sociali e alle altre funzioni interessate.
3. La funzione di *compliance*:
 - a) identifica in via continuativa le norme applicabili all'impresa e valuta il loro impatto sui processi e le procedure aziendali;
 - b) valuta l'adeguatezza e l'efficacia delle misure organizzative adottate per la prevenzione del rischio di non conformità alle norme e propone le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio;
 - c) valuta l'efficacia degli adeguamenti organizzativi conseguenti alle modifiche suggerite;
 - d) predispone adeguati flussi informativi diretti agli organi sociali dell'impresa e alle altre strutture coinvolte.
4. La funzione di *compliance* deve possedere adeguati requisiti di indipendenza, avere libero accesso a tutte le attività dell'impresa e a tutte le informazioni pertinenti e disporre delle risorse quantitativamente e professionalmente adeguate per lo svolgimento delle attività.
5. Le imprese, nella loro autonomia, organizzano la funzione di *compliance* valutando se costituirla in forma di specifica unità organizzativa o mediante il ricorso a risorse appartenenti ad altre unità aziendali. In tale ultimo caso l'indipendenza va garantita attraverso la presenza di adeguati presidi per garantire separatezza di compiti e prevenire conflitti di interesse.
6. In ogni caso, è garantita la separatezza della funzione di *compliance* dalle funzioni operative e dalle altre funzioni di controllo, attraverso la definizione espressa dei rispettivi ruoli e competenze.
7. Il collegamento tra la funzione di *compliance* e le funzioni di revisione interna e di *risk management* è definito e formalizzato dall'organo amministrativo.
8. La funzione di *compliance* è comunque separata dalla funzione di revisione interna ed è sottoposta a verifica periodica da parte della stessa.

Art. 24
(Responsabile della funzione di *compliance*)

1. Indipendentemente dalla forma organizzativa scelta ai sensi dell'articolo 23, comma 5, le imprese nominano un responsabile della funzione di *compliance*, in possesso di adeguati

requisiti di professionalità, indipendenza ed autorevolezza. La nomina e la revoca del responsabile sono di competenza dell'organo amministrativo.

2. Il responsabile della funzione non deve essere posto a capo di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di dette aree. Qualora giustificato dalle dimensioni o dalle caratteristiche operative, la responsabilità della funzione può essere attribuita ad un amministratore, purché privo di deleghe.
3. Il responsabile della funzione predisporre, almeno una volta l'anno, una relazione all'organo amministrativo sulla adeguatezza ed efficacia dei presidi adottati dall'impresa per la gestione del rischio di non conformità alle norme.

Art. 25

(Esterneizzazione della funzione di *compliance*)

1. Le imprese nelle quali, per le ridotte dimensioni e per le caratteristiche operative, l'istituzione di una specifica funzione di *compliance* non risponda a criteri di economicità, possono esternalizzare tale funzione nel rispetto delle condizioni di cui al Capo VIII.
2. Le attività relative alla funzione di *compliance* possono essere accentrate all'interno del gruppo assicurativo attraverso la costituzione di un'unità specializzata, a condizione che:
 - a) in ciascuna impresa del gruppo assicurativo sia individuato un referente che curi i rapporti con il responsabile della funzione di gruppo;
 - b) siano adottate adeguate procedure per garantire che le politiche di gestione del rischio di non conformità definite a livello di gruppo assicurativo siano adeguatamente calibrate rispetto alle caratteristiche operative della singola impresa.

Capo VI – Disposizioni in materia di gruppo assicurativo

Art. 26

(Ruolo della capogruppo)

1. La capogruppo, nel quadro dell'attività di direzione e coordinamento del gruppo assicurativo, esercita:
 - a) un controllo strategico sull'evoluzione delle diverse aree di attività in cui il gruppo assicurativo opera e dei rischi ad esse correlate. Il controllo verte sia sull'espansione delle attività svolte dalle società appartenenti al gruppo assicurativo sia sulle politiche di acquisizione o dismissione da parte delle società del gruppo assicurativo;
 - b) un controllo gestionale volto ad assicurare il mantenimento delle condizioni di equilibrio economico, finanziario e patrimoniale, sia delle singole imprese che del gruppo assicurativo nel suo insieme;
 - c) un controllo tecnico operativo, finalizzato alla valutazione dei vari profili di rischio apportati al gruppo assicurativo dalle singole controllate.

Art. 27

(Controllo interno e gestione dei rischi nel gruppo assicurativo)

1. Fermo restando che ciascuna impresa di assicurazione e riassicurazione con sede legale in Italia appartenente al gruppo assicurativo si dota di un sistema di controllo e gestione dei rischi secondo le disposizioni di cui ai Capi III, IV e V, la capogruppo dota il gruppo

assicurativo di un sistema di controlli interni idoneo ad effettuare un controllo effettivo sia sulle scelte strategiche del gruppo nel suo complesso che sull'equilibrio gestionale delle singole componenti.

2. In particolare, sono previste:

- a) procedure formalizzate di coordinamento e collegamento, anche informativo, tra le società appartenenti al gruppo assicurativo e la capogruppo per tutte le aree di attività;
- b) meccanismi di integrazione dei sistemi contabili, anche al fine di garantire l'affidabilità delle rilevazioni su base consolidata;
- c) flussi informativi periodici che consentano di verificare il perseguimento degli obiettivi strategici nonché il rispetto delle normative;
- d) procedure di segnalazione e contabili che consentano l'accertamento, la quantificazione, il monitoraggio e il controllo delle operazioni tra entità del gruppo assicurativo;
- e) procedure che assicurino la coerenza tra i dati e le informazioni prodotti ai fini dell'esercizio della vigilanza supplementare e quelli prodotti ai fini dell'esercizio della vigilanza sul gruppo assicurativo;
- f) la definizione dei compiti e delle responsabilità delle diverse unità deputate al controllo dei rischi all'interno del gruppo assicurativo e i meccanismi di coordinamento;
- g) procedure idonee a garantire in modo accentrato la identificazione, la misurazione, la gestione e il controllo dei rischi a livello del gruppo assicurativo.

3. La capogruppo formalizza e rende noti a tutte le società del gruppo assicurativo i criteri di identificazione, misurazione, gestione e controllo di tutti i rischi. Essa, inoltre, valida i sistemi e le procedure di controllo all'interno del gruppo assicurativo.

4. Al fine di verificare la rispondenza dei comportamenti delle società appartenenti al gruppo assicurativo agli indirizzi della capogruppo e l'efficacia dei sistemi di controllo interno, la capogruppo si attiva affinché siano effettuati accertamenti periodici nei confronti delle società che compongono il gruppo assicurativo, anche mediante la funzione di revisione interna delle stesse.

5. La capogruppo informa tempestivamente l'ISVAP dei casi in cui specifiche disposizioni di legge vigenti nello Stato in cui hanno sede legale le società estere del gruppo assicurativo ostino al rispetto delle disposizioni del presente Capo.

Capo VII – Obblighi di comunicazione all'ISVAP

Art. 28

(Comunicazioni all'ISVAP)

1. Le imprese comunicano all'ISVAP la nomina e la revoca dei responsabili della funzione di revisione interna, di *risk management* e di *compliance* entro trenta giorni dall'adozione del relativo atto.

2. Unitamente al bilancio di esercizio, le imprese trasmettono all'ISVAP la seguente documentazione:

- a) una relazione sul sistema dei controlli interni e di gestione dei rischi, che illustri le iniziative eventualmente intraprese nell'esercizio o le modifiche apportate, le attività di revisione interna svolte, le eventuali carenze segnalate e le azioni correttive adottate;
- b) le modifiche eventualmente apportate all'organigramma aziendale e al sistema delle deleghe già comunicati all'ISVAP;

- c) una relazione sulle eventuali modifiche apportate in termini di risorse e di organizzazione alla funzione di revisione interna, di *risk management* e di *compliance*.
3. La documentazione di cui al comma 2 è previamente sottoposta alla valutazione dell'organo amministrativo.

Capo VIII – Disposizioni in materia di esternalizzazione

Sezione I - Condizioni per l'esternalizzazione

Art. 29

(Esternalizzazione di attività)

1. Le imprese possono concludere accordi di esternalizzazione a condizione che la natura e la quantità delle attività esternalizzate e le modalità della cessione non determinino lo svuotamento dell'attività dell'impresa cedente.
2. Non può in ogni caso essere esternalizzata l'attività di assunzione dei rischi.
3. L'esternalizzazione non esonera in alcun caso gli organi sociali e l'alta direzione dell'impresa dalle rispettive responsabilità.

Art. 30

(Esternalizzazione di attività essenziali o importanti)

1. Quando le imprese affidano ad un terzo l'esecuzione di attività essenziali o importanti, garantiscono che le modalità di esternalizzazione:
 - a) non rechino pregiudizio alla qualità del sistema di *governance* dell'impresa;
 - b) non compromettano i risultati finanziari e la stabilità dell'impresa e la continuità delle sue attività;
 - c) non compromettano la capacità dell'impresa di fornire un servizio continuo e soddisfacente agli assicurati e ai danneggiati;
 - d) non determinino un ingiustificato incremento del rischio operativo.

Art. 31

(Politica di esternalizzazione e scelta dei fornitori)

1. L'organo amministrativo definisce la politica per la esternalizzazione delle attività dell'impresa, con delibera che include almeno:
 - a) i criteri di individuazione delle attività da esternalizzare;
 - b) i criteri di selezione dei fornitori, sotto il profilo della professionalità, dell'onorabilità e della capacità finanziaria;
 - c) l'adozione di metodi per la valutazione del livello delle prestazioni del fornitore (*service level agreement*).

Art. 32
(Accordi di esternalizzazione)

1. Nella stipulazione degli accordi di esternalizzazione le imprese di assicurazione hanno cura di assicurare in particolare che siano soddisfatte le seguenti condizioni:
 - a) la chiara definizione dell'attività oggetto della cessione, delle modalità di esecuzione e del relativo corrispettivo;
 - b) il fornitore svolga adeguatamente l'esecuzione delle attività esternalizzate nel rispetto della normativa vigente e delle disposizioni dell'impresa;
 - c) il fornitore informi tempestivamente l'impresa di qualsiasi fatto che possa incidere in maniera rilevante sulla propria capacità di eseguire le attività esternalizzate in conformità alla normativa vigente e in maniera efficiente ed efficace;
 - d) il fornitore garantisca la riservatezza dei dati relativi all'impresa ed agli assicurati;
 - e) l'impresa abbia facoltà di controllo e accesso all'attività e alla documentazione del fornitore;
 - f) il fornitore garantisca l'accesso completo ed immediato dell'ISVAP ai locali e alla documentazione del fornitore stesso;
 - g) l'impresa possa recedere dal contratto senza oneri sproporzionati o tali da pregiudicare, in concreto, l'esercizio del diritto di recesso;
 - h) l'impresa possa recedere o modificare il contratto in caso di richiesta dell'ISVAP;
 - i) il contratto non possa essere oggetto di subcessione senza il consenso dell'impresa.
2. Gli accordi di esternalizzazione sono formalizzati in forma scritta.
3. Nel caso di accordi di esternalizzazione della funzione di revisione interna, *risk management* e *compliance*, da stipularsi esclusivamente con un fornitore con sede legale nello SEE, le imprese assicurano altresì che siano adeguatamente definiti:
 - a) obiettivi, metodologie e frequenza dei controlli;
 - b) modalità e frequenza dei rapporti con l'organo amministrativo e l'alta direzione;
 - c) possibilità di riconsiderare le condizioni del servizio al verificarsi di modifiche di rilievo nell'operatività e nell'organizzazione dell'impresa di assicurazione.

Art. 33
(Controllo sulle attività esternalizzate)

1. Relativamente alle attività esternalizzate, il sistema dei controlli interni garantisce controlli di standard analoghi a quelli che sarebbero attuati se le attività fossero svolte direttamente dall'impresa. La politica di gestione dei rischi include i rischi specifici connessi all'esternalizzazione.
2. Ai fini di cui al comma 1, le imprese adottano idonei presidi organizzativi e contrattuali che consentano di monitorare costantemente le attività esternalizzate, la loro conformità a norme di legge e regolamenti e alle direttive e procedure aziendali, il rispetto dei limiti operativi e delle soglie di tolleranza al rischio fissate dall'impresa e di intervenire tempestivamente ove il fornitore non rispetti gli impegni assunti o la qualità del servizio fornito sia carente.
3. Ferme restando le limitazioni di cui all'articolo 29, le imprese individuano al proprio interno uno o più responsabili delle attività di controllo sulle attività esternalizzate e ne formalizzano compiti e responsabilità. Il numero dei responsabili deve essere proporzionato alla natura e alla quantità delle attività esternalizzate e, nel caso di esternalizzazione delle funzioni di revisione interna, *risk management* e *compliance*, deve trattarsi di soggetti con adeguate caratteristiche di autorevolezza e indipendenza.

4. Le imprese adottano idonee misure per assicurare la continuità della attività in caso di interruzione o grave deterioramento della qualità del servizio reso dal fornitore, inclusi adeguati piani di emergenza o di reinternalizzazione delle attività.
5. Qualora l'impresa di assicurazione e il fornitore di servizi appartengano allo stesso gruppo assicurativo, l'impresa nell'adozione dei presidi contrattuali e organizzativi previsti dal presente Capo può tener conto della misura in cui esercita sul fornitore il controllo ai sensi dell'articolo 72 del decreto e delle relative disposizioni di attuazione.

Art. 34

(Poteri di intervento dell'ISVAP)

1. L'ISVAP verifica che l'esternalizzazione delle attività e la loro esecuzione rispettino le condizioni di cui al presente Capo.
2. Qualora, in considerazione della dimensione e della posizione finanziaria dell'impresa di assicurazione, della natura dell'attività esternalizzata, delle caratteristiche e della posizione di mercato del fornitore o della qualità del servizio da questo reso, l'ISVAP ritenga che possa essere compromessa la sana e prudente gestione dell'impresa o arrecato pregiudizio agli interessi degli assicurati e dei danneggiati, ovvero non sia consentito il pieno esercizio delle funzioni di vigilanza, può imporre all'impresa di modificare il contratto di esternalizzazione, ovvero, nei casi più gravi, di recedere dal contratto.
3. L'esternalizzazione di attività ad un fornitore residente fuori dal SEE deve essere sottoposta alla preventiva autorizzazione dell'ISVAP.

Sezione II - Obblighi di comunicazione all'ISVAP

Art. 35

(Comunicazione in caso di esternalizzazione di attività essenziali o importanti)

1. Nel caso di esternalizzazione di attività essenziali o importanti, le imprese ne danno preventiva comunicazione all'ISVAP, almeno quarantacinque giorni prima della esecuzione del contratto, comunicando i dati relativi all'attività ceduta, al fornitore, alla durata dell'esternalizzazione e al luogo in cui si svolge l'attività esternalizzata, secondo il modello di cui all'allegato 1.
2. Le imprese comunicano tempestivamente all'ISVAP se in corso di contratto sono intervenuti cambiamenti rilevanti in merito al fornitore che incidono sul servizio.
3. Le imprese comunicano all'ISVAP la cessazione del contratto di esternalizzazione, allegando una relazione sulle modalità di reinternalizzazione dell'attività o di affidamento ad altro fornitore.

Art. 36

(Esternalizzazione della funzione di revisione interna, di *risk management* e di *compliance*)

1. Nel caso di esternalizzazione della funzione di revisione interna, di *risk management* e di *compliance*, le imprese danno preventiva comunicazione all'ISVAP, allegando la bozza del contratto.

2. Al contratto può essere data esecuzione trascorsi sessanta giorni dalla ricezione da parte dell'ISVAP della bozza di contratto e di ogni altro elemento informativo che consenta di valutare il rispetto dei criteri di economicità, efficienza ed affidabilità, nonché la sussistenza dei presupposti per il pieno esercizio dell'attività di vigilanza, anche ispettiva, da parte dell'ISVAP.

Art. 37

(Comunicazioni in caso di esternalizzazione di altre attività)

1. Nel caso di esternalizzazione di attività diverse da quelle essenziali o importanti le imprese danno comunicazione all'ISVAP dei contratti stipulati, in occasione dell'invio del bilancio di esercizio, utilizzando il modello di cui all'allegato 2.

Capo IX – Disposizioni transitorie e finali

Art. 38

(Disposizioni transitorie)

1. Entro centoventi giorni dall'entrata in vigore del presente Regolamento, le imprese trasmettono all'ISVAP un prospetto riepilogativo dei contratti di esternalizzazione in vigore, secondo il modello di cui all'allegato 3.

Art. 39

(Abrogazione di norme)

1. Dalla data di entrata in vigore del presente Regolamento, sono abrogate:
 - a) la circolare ISVAP n. 577/D del 30 dicembre 2005;
 - b) la circolare ISVAP n. 456 del 6 novembre 2001, limitatamente al punto 2.

Art. 40

(Pubblicazione)

1. Il presente Regolamento è pubblicato nella Gazzetta Ufficiale della Repubblica Italiana, nel Bollettino e sul sito internet dell'Autorità.

Art. 41

(Entrata in vigore)

1. Il presente Regolamento entra in vigore il giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.
2. Le imprese sono tenute ad adeguarsi alle disposizioni di cui al Capo V, nonché agli articoli 27, comma 3, 31, 33 e 35 entro il 1° gennaio 2009. Per le attività già esternalizzate alla data di entrata in vigore del presente Regolamento il termine di adeguamento alle disposizioni di cui all'articolo 32 è fissato al 1° aprile 2009.

Roma, 26 marzo 2008

Il Presidente
(Giancarlo Giannini)