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

MODIFICATO E INTEGRATO DAL PROVVEDIMENTO ISVAP DELL' 8 NOVEMBRE 2012 N. 3020 E DAL PROVVEDIMENTO IVASS DEL 15 APRILE 2014 N. 17.
LE MODIFICHE E INTEGRAZIONI SONO RIPORTATE IN CORSIVO

VERSIONE IN VIGORE DAL 30 GIUGNO 2014.

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

Sezione III – Componenti del sistema dei controlli interni

Capo III – Revisione interna

Capo IV – Gestione dei rischi

Capo V – Funzione di *compliance*

Capo VI – Disposizioni in materia di gruppo assicurativo

Capo VII – Obblighi di comunicazione all'IVASS

[1] Articolo introdotto dal Provvedimento IVASS n. 17 del 15 aprile 2014.
[2] Articolo introdotto dal Provvedimento IVASS n. 17 del 15 aprile 2014.
[3] Articolo introdotto dal Provvedimento IVASS n. 17 del 15 aprile 2014.
[4] Articolo introdotto dal Provvedimento IVASS n. 17 del 15 aprile 2014.
[5] Articolo introdotto dal Provvedimento IVASS n. 17 del 15 aprile 2014.
[6] Articolo introdotto dal Provvedimento IVASS n. 17 del 15 aprile 2014.

Capo VIII – Disposizioni in materia di esternalizzazione

Sezione I – Condizioni per l'esternalizzazione di attività

Sezione II – Obblighi di comunicazione all'IVASS

Capo IX – Disposizioni transitorie e finali

Elenco degli Allegati

Allegato 1[7]	*Documento sulle politiche di indirizzo: contenuto minimale*
Allegato 2[8]	Modello di comunicazione per l'esternalizzazione di attività essenziali o importanti
Allegato 3[9]	Prospetto di comunicazione per l'esternalizzazione di attività diverse da quelle essenziali o importanti

[7] Allegato sostituito dal comma 1 dell'articolo 37 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[8] Allegato sostituito dal comma 2 dell'articolo 37 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[9] Allegato sostituito dal comma 3 dell'articolo 37 del Provvedimento IVASS n. 17 del 15 aprile 2014.

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" *ovvero "IVASS": l'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo cui è succeduto l'IVASS, Istituto per la Vigilanza sulle assicurazioni, ai sensi dell'articolo 13 del decreto legge 6 luglio 2012, n. 95, convertito con legge 7 agosto 2012, n. 135*[10];

   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;

[10] Lettera modificata dall'articolo 1 del Provvedimento IVASS n. 17 del 15 aprile 2014. La versione precedente recitava:"" *ISVAP" o "Autorità": l'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo*".

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 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 *ed all’articolo 28 bis*[11].

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, *proporzionato alla natura, alla portata e alla complessità* dei rischi aziendali, *attuali e prospettici, inerenti all’attività dell’impresa*[12].

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;

[11] Lettera integrata dall’articolo 2 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[12] Comma modificato dalla lettera a) del comma 1 dell’articolo 3 del Provvedimento IVASS n. 17 del 15 aprile 2014.

b) l'adeguato controllo dei rischi *attuali e prospettici*[13];
b bis) la tempestività del sistema di reporting delle informazioni aziendali[14];
c) l'attendibilità e l'integrità delle informazioni contabili e gestionali;
d) la salvaguardia del patrimonio *anche in un'ottica di medio-lungo periodo*[15];
e) la conformità dell'attività dell'impresa alla normativa vigente, alle direttive e alle procedure aziendali.

2 bis. I presidi relativi al sistema dei controlli interni e di gestione dei rischi coprono ogni tipologia di rischio aziendale, anche secondo una visione prospettica ed in considerazione della salvaguardia del patrimonio. La responsabilità è rimessa agli organi sociali, ciascuno secondo le rispettive competenze. L'articolazione delle attività aziendali nonché dei compiti e delle responsabilità degli organi sociali e delle funzioni deve essere chiaramente definita[16].

Sezione II – Ruolo degli organi sociali

Art. 5
(Organo amministrativo) [17]

1. L'organo amministrativo ha la responsabilità ultima dei sistemi dei controlli interni *e di gestione dei rischi* dei quali *assicura* la costante completezza, funzionalità ed efficacia, anche con riferimento alle attività esternalizzate. L'organo amministrativo assicura che il sistema di gestione dei rischi consenta l'identificazione, la valutazione *anche prospettica* e il controllo dei rischi, ivi compresi quelli derivanti dalla non conformità alle norme, *garantendo l'obiettivo della salvaguardia del patrimonio, anche in un'ottica di medio-lungo periodo*.

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 di responsabilità alle unità operative, curandone l'adeguatezza nel tempo, *in modo da poterli adattare tempestivamente ai mutamenti degli obiettivi strategici e del contesto di riferimento in cui la stessa opera;*

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, con conseguente possibilità di prevedere adeguati piani di emergenza (c.d. "*contingency arrangements*") qualora decida di avocare a sé i 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. *Nell'ambito di tali direttive è ricompresa anche la politica relativa alle funzioni di risk management, compliance e di revisione interna. Verifica altresì che il sistema dei controlli interni sia coerente con gli indirizzi strategici e la propensione al rischio stabiliti e sia in grado di cogliere l'evoluzione dei rischi aziendali e l'interazione tra gli stessi;*

[13] Lettera integrata dalla lettera b) del comma 1 dell'articolo 3 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[14] Lettera inserita dalla lettera c) del comma 1 dell'articolo 3 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[15] Lettera integrata dalla lettera d) del comma 1 dell'articolo 3 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[16] Comma inserito dalla lettera e) del comma 1 dell'articolo 3 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[17] Articolo sostituito dall'articolo 4 del Provvedimento IVASS n. 17 del 15 aprile 2014. Le imprese di assicurazione e di riassicurazione si adeguano alle disposizioni di cui al presente articolo entro il 31 dicembre 2014, ai sensi del comma 3 dell'articolo 56 del Provvedimento IVASS n. 17 del 15 aprile 2014.

e) approva la politica di valutazione attuale e prospettica dei rischi, i criteri e le metodologie seguite per le valutazioni, con particolare riguardo a quelli maggiormente significativi; approva gli esiti delle valutazioni e li comunica all'alta direzione ed alle strutture interessate unitamente alle conclusioni cui lo stesso è pervenuto (approccio c.d. top down);

f) determina, sulla base delle valutazioni di cui alla lettera e), la propensione al rischio dell'impresa in coerenza con l'obiettivo di salvaguardia del patrimonio della stessa, fissando in modo coerente i livelli di tolleranza al rischio che rivede almeno una volta l'anno, al fine di assicurarne l'efficacia nel tempo;

g) approva, sulla base degli elementi di cui alle lettere e) ed f), la politica di gestione del rischio e le strategie anche in un'ottica di medio-lungo periodo nonché i piani di emergenza (c.d. contingency plan) di cui all'articolo 19, comma 4 al fine di garantire la regolarità e continuità aziendale;

h) approva, tenuto conto degli obiettivi strategici ed in coerenza con la politica di gestione dei rischi, le politiche di sottoscrizione, di riservazione, di riassicurazione e di altre tecniche di mitigazione del rischio nonché di gestione del rischio operativo, in coerenza con le lettere e), f) e g);

i) 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;

j) approva un documento, coerente con le disposizioni di cui alle lettere a), d), e) ed f) da diffondere a tutte le strutture interessate, in cui sono definiti i) i compiti e le responsabilità degli organi sociali, dei comitati consiliari e delle funzioni di risk management, di compliance e di revisione interna; ii) i flussi informativi, ivi comprese le tempistiche, tra le diverse funzioni, comitati consiliari e tra questi e gli organi sociali e iii), nel caso in cui gli ambiti di controllo presentino aree di potenziale sovrapposizione o permettano di sviluppare sinergie, le modalità di coordinamento e di collaborazione tra di essi e con le funzioni operative. Nel definire le modalità di raccordo, le imprese prestano attenzione a non alterare, anche nella sostanza, le responsabilità ultime degli organi sociali sul sistema dei controlli interni;

k) approva la politica aziendale, di cui all'articolo 31, in materia di esternalizzazione;

l) approva la politica aziendale per la valutazione del possesso dei requisiti di idoneità alla carica, in termini di onorabilità e professionalità, dei soggetti preposti alle funzioni di amministrazione, di direzione e di controllo nonché dei responsabili delle funzioni di risk management, compliance e revisione interna, o in caso di esternalizzazione di queste ultime all'interno o all'esterno del gruppo, rispettivamente, dei referenti interni o dei soggetti responsabili delle attività di controllo delle attività esternalizzate di cui all'art. 33, comma 3. Valuta la sussistenza dei requisiti in capo a tali soggetti con cadenza almeno annuale. In particolare, tale politica assicura che l'organo amministrativo sia nel suo complesso in possesso di adeguate competenze tecniche almeno in materia di mercati assicurativi e finanziari, sistemi di governance, analisi finanziaria ed attuariale, quadro regolamentare, strategie commerciali e modelli d'impresa;

m) approva la politica delle segnalazioni destinate all'IVASS (c.d. reporting policy), in coerenza con le vigenti disposizioni normative;

n) 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;

o) richiede di essere periodicamente informato sulla efficacia e sull'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, *dalle funzioni di risk management e di compliance*, dal personale, impartendo con tempestività le direttive per l'adozione di misure correttive*, di cui successivamente valuta l'efficacia;*

p) individua particolari eventi o circostanze che richiedono un immediato intervento da parte dell'alta direzione;

q) assicura che sussista un'idonea e continua interazione tra tutti i comitati istituiti all'interno dell'organo amministrativo stesso, l'alta direzione e le funzioni di risk management, di compliance e di revisione interna, anche mediante interventi proattivi per garantirne l'efficacia;

r) assicura un aggiornamento professionale continuo, esteso anche ai componenti dell'organo stesso, predisponendo, altresì, piani di formazione adeguati ad assicurare il bagaglio di competenze tecniche necessario per svolgere con consapevolezza il proprio ruolo nel rispetto della *natura, della portata e della complessità* dei compiti assegnati e preservare le proprie conoscenze nel tempo;

s) effettua, almeno una volta l'anno, una valutazione sulla dimensione, sulla composizione e sul funzionamento dell'organo amministrativo nel suo complesso, nonché dei suoi comitati, esprimendo orientamenti sulle figure professionali la cui presenza nell'organo amministrativo sia ritenuta opportuna e proponendo eventuali azioni correttive.

3. L'organo amministrativo assicura che la relazione sul sistema dei controlli interni e di gestione dei rischi illustri in modo adeguato *ed esaustivo l*a struttura organizzativa dell'impresa e rappresenta le ragioni che rendono tale struttura idonea ad assicurare la completezza, la funzionalità ed efficacia del sistema dei controlli interni e di gestione dei rischi.

4. L'organo amministrativo informa senza indugio l'Autorità di Vigilanza qualora vengano apportate significative modifiche alla struttura organizzativa dell'impresa illustrando le cause interne o esterne che hanno reso necessari tali interventi.

5. Le politiche di cui al comma 2 lettere d), h), k), l) e m) contengono almeno gli elementi riportati nell'allegato 1 al presente regolamento.

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 valutazione, *anche prospettica*[18], e di 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;

   b bis) attua, tenuto conto degli obiettivi strategici ed in coerenza con la politica di gestione dei rischi, le politiche di sottoscrizione, di riservazione, di riassicurazione e di altre tecniche di mitigazione del rischio nonché di gestione del rischio operativo[19]*;*

   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 *compiti*[20] 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

[18] Lettera integrata dalla lettera a) del comma 1 dell'articolo 5 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[19] Lettera inserita dalla lettera b) del comma 1 dell'articolo 5 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[20] Comma integrato dall'articolo 6 del Provvedimento IVASS n. 17 del 15 aprile 2014.

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 *alla* natura, *alla portata ed alla complessità dei rischi inerenti all'attività dell'impresa*[21], 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 *la natura, la portata e la complessità delle operazioni dell'impresa, quest'ultima*[22] assicura, 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.

[21] Comma modificato dalla lettera a) del comma 1 dell'articolo 7 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[22] Comma modificato dalla lettera b) del comma 1 dell'articolo 7 del Provvedimento IVASS n. 17 del 15 aprile 2014.

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. 12 bis
(Sistema di gestione dei dati)[23]

1. *Le imprese prevedono un sistema di registrazione e di reportistica dei dati che ne consenta la tracciabilità al fine di poter disporre di informazioni complete ed aggiornate sugli elementi che possono incidere sul profilo di rischio dell'impresa e sulla sua situazione di solvibilità.*

2. *Il sistema di cui al comma 1 assicura nel continuo l'integrità, la completezza e la correttezza dei dati conservati e delle informazioni rappresentate anche al fine di consentire una ricostruzione dell'attività svolta e l'individuazione dei relativi responsabili; garantisce altresì l'agevole verifica delle informazioni registrate.*

3. *L'impresa definisce uno standard aziendale di data governance che individua ruoli e responsabilità delle funzioni coinvolte nell'utilizzo e nel trattamento delle informazioni aziendali.*

4. *Nel caso l'impresa ricorra ad un data warehouse aziendale, per finalità di analisi e di reportistica, le procedure di estrazione dei dati, di controllo e di caricamento negli archivi accentrati – al pari dell'attività di utilizzo dei dati – sono documentati al fine di consentire la verifica della qualità delle informazioni.*

5. *Le procedure di gestione e aggregazione dei dati sono documentate, con indicazione specifica delle circostanze in cui è consentita l'immissione manuale o rettifica dei dati aziendali.*

6. *I processi di acquisizione dei dati da strutture esterne sono documentati e presidiati.*

7. *I dati sono conservati con granularità adeguata a consentire le diverse analisi e aggregazione richieste dalle possibili procedure di utilizzo.*

8. *In sede di prima applicazione delle disposizioni di cui al presente articolo le imprese preparano un piano di implementazione entro il 31 ottobre 2014.*

Art. 13
(Produzione di dati e informazioni ai fini della vigilanza supplementare)

[23] Articolo inserito dall'articolo 8 del Provvedimento IVASS n. 17 del 15 aprile 2014.

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, *e della valutazione attuale e prospettica dei rischi a livello di gruppo che la capogruppo svolge ai sensi dell'articolo 27, comma 5,* adottando idonee procedure di controllo interno ed individuando *idonee misure di raccolta e di coordinamento tra i flussi informativi della vigilanza supplementare e quelli del gruppo assicurativo e della impresa*[24]*.*

2. Le imprese conservano i dati e le informazioni di cui al comma 1 presso la propria sede, per eventuali verifiche da parte *dell'IVASS*[25].

Art. 14
(Sistemi informatici)

1. I sistemi informatici devono essere appropriati rispetto *alla natura, alla portata ed alla complessità dell'attività dell'impresa, nonché dei conseguenti rischi*[26] 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 predispone un piano di integrazione dei sistemi informatici nel quale sono specificati:

   a) ambiti, funzioni, procedure, applicazioni e basi dati interessate dal processo di integrazione;

[24] Comma modificato dalla lettera a) del comma 1 dell'articolo 9 del Provvedimento IVASS n. 17 del 15 aprile 2014. La precedente versione recitava: "*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*".
[25] Comma modificato dalla lettera b) del comma 1 dell'articolo 9 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[26] Comma modificato dall'articolo 10 del Provvedimento IVASS n. 17 del 15 aprile 2014.

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)[27]

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 la 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) *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*;
   c) *la funzione deve avere collegamenti organici con tutti i centri titolari di funzioni di controllo interno*;
   d) *la struttura dedicata deve essere adeguata in termini di risorse umane e tecnologiche alla natura, alla portata e alla complessità dell'attività dell'impresa ed agli obiettivi di sviluppo che la stessa intende perseguire. Gli addetti alla struttura devono possedere competenze specialistiche e deve esserne 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. *Durante l'esecuzione dell'attività di audit e in sede di valutazione e segnalazione delle relative risultanze, la funzione di revisione interna svolge i compiti ad essa assegnati con autonomia ed obiettività di giudizio, in modo da preservare la propria indipendenza e imparzialità, in coerenza con le direttive a tal fine definite dall'organo amministrativo.*

[27] Articolo sostituito dall'articolo 11 del Provvedimento IVASS n. 17 del 15 aprile 2014.

5. *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. 15 bis
(Responsabile della funzione di revisione interna)[28]

1. *Il responsabile della funzione è nominato e revocato dall'organo amministrativo, sentito il Collegio Sindacale e, ove presente, anche il Comitato di Controllo Interno, e soddisfa i requisiti di idoneità alla carica fissati dalla politica di cui all'articolo 5, comma 2 lettera l). I compiti attribuiti al responsabile della funzione sono chiaramente definiti ed approvati con delibera dell'organo amministrativo, che ne fissa anche poteri, responsabilità e modalità di reportistica all' organo amministrativo stesso.*

2. *Il responsabile della funzione è dotato dell'autorità necessaria a garantire l'indipendenza della stessa.*

3. *Il responsabile della funzione di revisione interna pianifica annualmente l'attività in modo da identificare le aree da sottoporre prioritariamente a revisione. Tale piano e il relativo livello di priorità deve essere coerente con i principali rischi cui l'impresa è esposta. La programmazione degli interventi di verifica tiene conto sia delle eventuali carenze emerse nei controlli già eseguiti sia di eventuali nuovi rischi identificati. Il piano include anche attività di verifica delle componenti del sistema dei controlli interni ed in particolare del flusso informativo e del sistema informatico. Il piano di audit è approvato dall'organo amministrativo ed individua, almeno, le attività a rischio, le operazioni e i sistemi da verificare, descrivendo i criteri sulla base dei quali 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 definiti in modo da fronteggiare le esigenze impreviste.*

4. *Ove necessario, potranno essere effettuate verifiche non previste dal piano di audit.*

5. *A seguito dell'analisi sull'attività oggetto di controllo, il responsabile della funzione di revisione interna procede, secondo le modalità e la periodicità fissata dall'organo amministrativo, a comunicare all'organo amministrativo, 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, contenere suggerimenti per eliminare le carenze riscontrate, riportando raccomandazioni in ordine ai tempi per la loro rimozione e sono conservati presso la sede della società. Le risultanze della specifica area oggetto di controllo sono altresì comunicate al responsabile della funzione interessata dall'attività di revisione.*

6. *Il responsabile della funzione di revisione interna presenta, almeno annualmente, una relazione all'organo amministrativo sull'attività svolta che riepiloga tutte le verifiche effettuate, i risultati emersi, i punti di debolezza o carenze rilevate e le raccomandazioni formulate per la loro rimozione; nella relazione riepilogativa devono essere inclusi anche gli interventi di follow-up con indicazione degli esiti delle verifiche di cui all'art. 15, comma 5, dei soggetti e/o funzioni designati per la rimozione, del tipo, dell'efficacia e della tempistica dell'intervento da essi effettuato per rimuovere le criticità inizialmente rilevate.*

[28] Articolo inserito dall'articolo 12 del Provvedimento IVASS n. 17 del 15 aprile 2014.

Art. 16
(Esternalizzazione della funzione di revisione interna)

1. Le imprese per le quali, per la *ridotta portata e complessità dei rischi inerenti all'attività dell'impresa*[29], 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 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 cui sono attribuiti compiti di controllo.

Capo IV – Gestione dei rischi

Art. 18
(Obiettivi del sistema di gestione dei rischi)[30]

1. Il sistema di gestione dei rischi di cui si dota l'impresa include le strategie, i processi, le procedure anche di reportistica necessarie per individuare, misurare, valutare, monitorare, gestire e segnalare su base continuativa i rischi attuali e prospettici a livello individuale e aggregato cui l'impresa è o potrebbe essere esposta e le relative interdipendenze.

2. Al fine di mantenere ad un livello accettabile, coerente con le disponibilità patrimoniali, i rischi cui sono esposte, le imprese si dotano di un adeguato sistema di gestione dei rischi, in *linea con la politica di gestione del rischio*, proporzionato alla natura*, alla portata* e alla complessità dell'attività esercitata, che consenta la identificazione, la valutazione *anche prospettica* e il controllo dei rischi, *con particolare attenzione a quelli* maggiormente significativi; *per tali* si intendono i rischi le cui conseguenze possono minare la solvibilità dell'impresa o costituire un serio ostacolo alla realizzazione degli obiettivi aziendali.

3. Le politiche di assunzione*, valutazione* 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

[29] Comma modificato dall'articolo 13 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[30] Articolo sostituito dall'articolo 14 del Provvedimento IVASS n. 17 del 15 aprile 2014.

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. *La politica di gestione dei rischi considera altresì il rischio derivante dagli investimenti, ivi incluso quello di liquidità, tenuto conto del cd. prudent person principle che, per gli obiettivi di cui al comma 1, è alla base delle scelte degli investimenti dell'impresa.*

4. *Le politiche di sottoscrizione, di riservazione, di riassicurazione e di altre tecniche di mitigazione del rischio nonché di gestione del rischio operativo devono tener conto degli obiettivi strategici dell'impresa ed essere coerenti con la politica di gestione dei rischi di cui al precedente comma 2. Ai fini della gestione del rischio operativo, le imprese individuano adeguate metodologie di analisi che tengano conto anche dell'insorgenza di eventi esterni.*

Art. 19
(Individuazione dei rischi)[31]

1. *Le imprese provvedono a definire le categorie di rischio in funzione della natura, della portata e della complessità dei rischi inerenti all'attività svolta, in un'ottica attuale e prospettica. 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.*

[31] Articolo sostituito dall'articolo 15 del Provvedimento IVASS n. 17 del 15 aprile 2014.

2. *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.*

3. *Le imprese devono essere in grado, attraverso un adeguato processo di analisi, di comprendere la natura dei rischi individuati, la loro origine, la loro possibile aggregazione e correlazione, la possibilità o necessità di controllarli e gli effetti che ne possono derivare, sia in termini di perdite che di opportunità.*

4. *Le imprese definiscono procedure in grado di evidenziare con tempestività l'insorgere di rischi che possono compromettere l'obiettivo della salvaguardia del patrimonio, anche in un'ottica di medio-lungo periodo, danneggiare la situazione patrimoniale ed economica o implicare il superamento delle soglie di tolleranza fissate. Per le maggiori fonti di rischio identificate l'impresa predispone adeguati piani di emergenza che dovranno essere rivisti, aggiornati periodicamente, valutandone l'efficacia, e comunque con cadenza almeno annuale, ed approvati dall'organo amministrativo.*

Art. 19 bis
(Valutazione dei rischi)[32]

1. *Le imprese valutano i rischi cui sono esposte in un'ottica attuale e prospettica almeno con cadenza annuale e, comunque, ogni volta che si presentino circostanze che potrebbero modificare in modo significativo il proprio profilo di rischio, secondo quanto disposto nella politica di valutazione dei rischi.*

2. *Ai fini delle valutazioni di cui al comma 1, le imprese definiscono un processo di analisi dei rischi che include sia una valutazione qualitativa sia, per quelli quantificabili, l'adozione di metodologie di misurazione dell'esposizione al rischio, inclusi, ove appropriati, sistemi di determinazione dell'ammontare della massima perdita potenziale. Ove possibile, le imprese considerano le interrelazioni tra i rischi, valutandoli sia singolarmente sia su base aggregata.*

3. *I processi di valutazione dei rischi sono effettuati su base continuativa, per tenere conto sia delle intervenute modifiche nella natura, nella portata e nella complessità dell'attività dell'impresa 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.*

4. *Le metodologie di valutazione e misurazione dei rischi e i relativi risultati sono adeguatamente documentati.*

5. *Gli esiti delle valutazioni, unitamente alle metodologie utilizzate, sono trasmessi all'organo amministrativo che, dopo averli discussi e approvati, li comunica all'alta direzione ed alle strutture interessate unitamente alle conclusioni cui lo stesso è pervenuto*[33]*.*

Art. 20
(Stress test ed altri strumenti di analisi)[34]

[32] Articolo inserito dall'articolo 16 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[33] Le imprese di assicurazione e di riassicurazione si adeguano alle disposizioni di cui al presente comma entro il 31 dicembre 2014, ai sensi del comma 3 dell'articolo 56 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[34] Rubrica integrata dalla lettera a) del comma 1 dell'articolo 17 del Provvedimento IVASS n. 17 del 15 aprile 2014.

1. Per ciascuna delle fonti di rischio identificate dalle imprese come maggiormente significative sulla base dei processi di cui all'articolo *19 bis*, le imprese effettuano analisi prospettiche *qualitative e* quantitative, *anche*[35] attraverso l'uso di *stress test.*

2. *Le analisi quantitative, basate* su modelli deterministici o stocastici, sono disegnate e sviluppate in coerenza con *la natura, la portata e la complessità dei rischi inerenti all'attività di impresa* e ripetute con la frequenza resa necessaria dal tipo di rischio, dall'evoluzione *della natura, della portata e della complessità dell'attività*dell'impresa e del contesto di mercato, e in ogni caso con cadenza almeno annuale[36].

3. I risultati *delle analisi qualitative e quantitative*, unitamente alle ipotesi sottostanti *e alle metodologie utilizzate*[37]*,* 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 analisi quantitative 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'IVASS, le imprese effettuano *analisi qualitative o quantitative*[38] standardizzate sulla base di fattori di rischio e parametri prefissati.

Art. 21
(Funzione di risk management)[39]

1. L' impresa istituisce una funzione di risk management, proporzionata alla natura, alla portata e alla complessità dei rischi inerenti all'attività dell'impresa stessa, che:

a) concorre alla definizione della politica di gestione del rischio e definisce i criteri e le relative metodologie di misurazione dei rischi nonché gli esiti delle valutazioni, che trasmette all'organo amministrativo. Quest'ultimo, dopo averli discussi e approvati, li comunica all'alta direzione ed alle strutture interessate unitamente alle conclusioni cui lo stesso è pervenuto ai sensi dell'articolo 5, comma 2, lettera e);

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) effettua le valutazioni, di cui all'articolo 19 bis, del profilo di rischio dell'impresa e segnala all'organo amministrativo i rischi individuati come maggiormente significativi di cui all'articolo 18, comma 2, ultimo periodo, anche in termini potenziali;

e) 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;

f) verifica la coerenza dei modelli di misurazione dei rischi con l'operatività svolta dalla impresa e concorre all'effettuazione delle analisi quantitative di cui all'articolo 20;

[35] Comma integrato dalla lettera b) del comma 1 dell'articolo 17 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[36] Comma sostituito dalla lettera c) del comma 1 dell'articolo 17 del Provvedimento IVASS n. 17 del 15 aprile 2014. La precedente versione recitava: "*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*".
[37] Comma modificato dalla lettera d) del comma 1 dell'articolo 17 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[38] Comma modificato dalla lettera e) del comma 1 dell'articolo 17 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[39] Articolo sostituito dall'articolo 18 del Provvedimento IVASS n. 17 del 15 aprile 2014.

g) monitora l'attuazione della politica di gestione del rischio e il profilo generale di rischio dell'impresa nel suo complesso.

2. L'istituzione della funzione di risk management 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, in coerenza con il documento approvato dall'organo amministrativo di cui all'articolo 5, comma 2 lettera j).

3. 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 costituiscono la funzione di risk management in forma di specifica unità organizzativa o, tenuto conto della natura e della ridotta portata e complessità dei rischi inerenti all'attività dell'impresa, anche mediante il ricorso a risorse appartenenti ad altre unità aziendali. In tale ultimo caso, l'indipendenza va assicurata attraverso la presenza di adeguati presidi che garantiscano la separatezza di compiti e prevengano conflitti di interesse. 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.

4. Il collegamento tra la funzione di risk management e le funzioni di revisione interna e di compliance è definito e formalizzato dall'organo amministrativo.

5. La funzione di risk management è comunque separata dalla funzione di revisione interna ed è sottoposta a verifica periodica da parte di quest'ultima.

Art. 21 bis
(Responsabile della funzione di risk management)[40]

1. Indipendentemente dalla forma organizzativa scelta ai sensi dell'articolo 21, comma 3, le imprese nominano un responsabile della funzione di risk management che soddisfa i requisiti di idoneità alla carica fissati dalla politica di cui all'articolo 5, comma 2, lettera l). 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.

3. Il responsabile della funzione presenta, una volta all'anno, all'organo amministrativo un programma di attività in cui sono identificati i principali rischi cui l'impresa è esposta e le proposte che intende effettuare in relazione ai rischi stessi. La programmazione tiene conto anche delle carenze eventualmente riscontrate nei controlli precedenti e di eventuali nuovi rischi.

4. Il responsabile della funzione predispone, almeno una volta all'anno, una relazione all'organo amministrativo sull'adeguatezza ed efficacia del sistema di gestione dei rischi, delle metodologie e dei modelli utilizzati per il presidio dei rischi stessi, sull'attività svolta, sulle valutazioni effettuate, sui risultati emersi e sulle criticità riscontrate, e dando conto dello stato di implementazione dei relativi interventi migliorativi, qualora effettuati.

Art. 21 ter
(Esternalizzazione della funzione di risk management)[41]

[40] Articolo inserito dall'articolo 19 del Provvedimento IVASS n. 17 del 15 aprile 2014.

1. *Le imprese nelle quali, per la natura e per la ridotta portata e complessità dei rischi inerenti all'attività dell'impresa, l'istituzione di una specifica funzione di risk management 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 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.*

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, *alla portata e alla complessità dei rischi inerenti all'attività dell'impresa*[42] 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;

[41] Articolo inserito dall'articolo 20 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[42] Comma modificato dalla lettera a) del comma 1 dell'articolo 21 del Provvedimento IVASS n. 17 del 15 aprile 2014.

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. *La collocazione organizzativa della funzione di compliance è lasciata all'autonomia delle imprese, nel rispetto del principio di separatezza tra funzioni operative e di controllo. Le imprese costituiscono la funzione compliance in forma di specifica unità organizzativa o, tenuto conto della natura e della ridotta portata e complessità dei rischi inerenti all'attività dell'impresa, anche mediante il ricorso a risorse appartenenti ad altre unità aziendali. In tale ultimo caso, l'indipendenza va assicurata attraverso la presenza di adeguati presidi che garantiscano la separatezza dei compiti e prevengano conflitti di interesse. La funzione di compliance, anche quando non costituita in forma di specifica unità organizzativa, risponde all'organo amministrativo. La collocazione organizzativa della funzione di compliance deve essere tale da non dipendere da funzioni operative*[43]*.*

6. *(abrogato)*[44]

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 *di quest'ultima*[45].

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, che soddisfi i requisiti di idoneità alla carica fissati dalla politica di cui all'articolo 5, comma 2 lettera l*[46]*.* 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 *dalla natura, dalla portata e dalla complessità delle attività dell'impresa*[47], la responsabilità della funzione può essere attribuita ad un amministratore, purché privo di deleghe.

2 bis. Il responsabile della funzione presenta annualmente all'organo amministrativo un programma di attività in cui sono indicati gli interventi che intende eseguire relativamente al rischio di

[43] Comma sostituito dalla lettera b) del comma 1 dell'articolo 21 del Provvedimento IVASS n. 17 del 15 aprile 2014. La precedente versione recitava: "*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*".
[44] Comma abrogato dalla lettera c) del comma 1 dell'articolo 21 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[45] Comma integrato dalla lettera d) del comma 1 dell'articolo 21 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[46] Comma modificato dalla lettera a) del comma 1 dell'articolo 22 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[47] Comma modificato dalla lettera b) del comma 1 dell'articolo 22 del Provvedimento IVASS n. 17 del 15 aprile 2014.

non conformità alle norme. La programmazione degli interventi tiene conto sia delle carenze eventualmente riscontrate nei controlli precedenti sia di eventuali nuovi rischi[48]*.*

2 ter. Ove necessario potranno essere effettuate verifiche non previste nel programma di attività[49]*.*

3. Il responsabile della funzione predispone, 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, sull'attività svolta, sulle verifiche effettuate, sui risultati emersi e sulle criticità riscontrate, dando conto dello stato di implementazione dei relativi interventi migliorativi, qualora effettuati[50]*.*

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

1. Le imprese nelle quali, *per la natura e per la ridotta portata e complessità dei rischi inerenti all'attività dell'impresa*[51]*,* 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.

[48] Comma inserito dalla lettera c) del comma 1 dell'articolo 22 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[49] Comma inserito dalla lettera d) del comma 1 dell'articolo 22 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[50] Comma sostituito dalla lettera e) del comma 1 dell'articolo 22 del Provvedimento IVASS n. 17 del 15 aprile 2014. La precedente versione recitava: "*Il responsabile della funzione predispone, 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.*"
[51] Comma modificato dall'articolo 23 del Provvedimento IVASS n. 17 del 15 aprile 2014.

Art. 27
(Controllo interno e gestione dei rischi nel gruppo assicurativo)[52]

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 e di gestione dei rischi, coerente con i requisiti di governance di gruppo, idoneo ad effettuare un controllo effettivo sia sulle scelte strategiche del gruppo nel suo complesso che sull'equilibrio gestionale delle singole componenti.*

2. *Resta impregiudicata la responsabilità dell'organo amministrativo di ciascuna impresa del gruppo assicurativo relativamente alla propria governance, al sistema dei controlli interni e di gestione dei rischi dell'impresa stessa.*

3. *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, ivi inclusa quella deputata alla gestione 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.*

4. *Nel sistema di gestione dei rischi del gruppo, la capogruppo deve garantire che la politica della gestione del rischio a livello di gruppo assicurativo sia attuata in modo coerente e continuativo all'interno dell'intero gruppo, tenendo conto dei rischi di ciascuna impresa ricompresa nel perimetro della vigilanza supplementare nonché delle reciproche interdipendenze, in particolare:*
   - *dei rischi reputazionali, di quelli derivanti da operazioni infragruppo, di concentrazione, incluso il rischio di contagio, a livello di gruppo;*
   - *delle interdipendenze tra rischi derivanti dallo svolgimento dell'attività assicurativa in imprese e in giurisdizioni differenti;*
   - *dei rischi derivanti da imprese con sede legale in Stati terzi ricomprese nel perimetro della vigilanza supplementare;*
   - *dei rischi derivanti da imprese non soggette a normativa di settore ricomprese nel perimetro della vigilanza supplementare;*
   - *dei rischi derivanti da altre imprese soggette a specifica normativa di settore ricomprese nel perimetro della vigilanza supplementare.*

5. *La capogruppo, tenuto conto delle disposizioni di cui al comma 4, valuta, con cadenza almeno annuale, i rischi cui il gruppo assicurativo è esposto in un'ottica attuale e prospettica. Gli esiti delle valutazioni, unitamente alle metodologie utilizzate, sono*

[52] Articolo sostituito dall'articolo 24 del Provvedimento IVASS n. 17 del 15 aprile 2014.

trasmessi all'organo amministrativo che, dopo averli discussi e approvati, li comunica all'alta direzione ed alle strutture interessate unitamente alle conclusioni cui lo stesso è pervenuto. Definisce altresì un processo per la valutazione prospettica dei rischi a livello di gruppo assicurativo, che includa anche quelli derivanti da imprese incluse nel perimetro della vigilanza supplementare, ivi compresi i rischi derivanti da imprese con sede legale in Stati terzi, non soggette a normative di settore e da altre imprese soggette a specifica normativa di settore. Detta valutazione tiene conto delle interdipendenze tra i rischi[53]*.*

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

7. *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.*

8. *Le metodologie di valutazione dei rischi a livello di gruppo assicurativo, le ipotesi e i relativi risultati sono adeguatamente documentati.*

9. *La capogruppo informa tempestivamente l'IVASS 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'IVASS*[54]

Art. 28
(Comunicazioni *all'IVASS*)[55]

1. Le imprese comunicano *all'IVASS* 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. *Nel caso di nomina, le imprese comunicano di aver effettuato le verifiche sulla sussistenza dei requisiti di onorabilità, professionalità e indipendenza dei responsabili delle funzioni e nei casi di esternalizzazione di tali funzioni all'interno o all'esterno del gruppo assicurativo, del referente interno o del responsabile delle attività di controllo per le attività esternalizzate, secondo quanto indicato nella politica aziendale in materia*[56]*.*

2. Unitamente al bilancio di esercizio, le imprese trasmettono *all'IVASS una relazione*[57]:

   a) *sul sistema dei controlli interni, che descriva il sistema dei controlli interni nel suo complesso, ivi incluse le principali procedure che lo costituiscono, illustrando altresì 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.*
   Tale relazione dovrà altresì contenere informazioni sulla struttura organizzativa dell'impresa, di cui all'art. 5, comma 3, con particolare riguardo a:

[53] Le imprese di assicurazione e di riassicurazione si adeguano alle disposizioni di cui al presente comma entro il 31 dicembre 2014, ai sensi del comma 3 dell'articolo 56 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[54] Rubrica modificata dall'articolo 25 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[55] Rubrica modificata dalla lettera a) del comma 1 dell'articolo 26 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[56] Comma modificato dalla lettera b) del comma 1 dell'articolo 26 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[57] Comma modificato dalla lettera c) del comma 1 dell'articolo 26 del Provvedimento IVASS n. 17 del 15 aprile 2014.

- *composizione e nomina dell'organo amministrativo e dei comitati interni all'organo amministrativo medesimo (procedure di nomina, amministratori esecutivi e non esecutivi, amministratori indipendenti e processi di valutazione del requisito di indipendenza, numero degli incarichi di ciascun amministratore in altre società, requisiti di onorabilità e professionalità e specifiche competenze professionali di ciascun amministratore);*
- *ruolo dell'organo amministrativo e dei comitati interni all'organo amministrativo medesimo (compiti e responsabilità, modalità di svolgimento dei lavori, numero delle riunioni, grado di partecipazione alle riunioni, attività svolta per l'assolvimento dei compiti assegnati dal presente regolamento, soprattutto in materia di definizione delle strategie e loro revisione periodica);*
- *modalità di svolgimento del processo di autovalutazione dell'organo amministrativo ed eventuali misure correttive assunte per il miglioramento, anche tenuto conto del livello di professionalità degli amministratori rispetto all'operatività e al profilo di rischio dell'impresa;*
- *deleghe conferite dall'organo amministrativo, con indicazione delle modalità di controllo sui poteri delegati (linee di reporting);*
- *criteri seguiti per la definizione della politica di remunerazione, con illustrazione dell'informativa che l'organo amministrativo è tenuto a fornire all'assemblea ai sensi dell'art. 24 del Regolamento ISVAP n. 39 del 9 giugno 2011;*
- *misure intraprese per monitorare gli interessi degli amministratori nelle operazioni della società sulle quali è chiamato a decidere, le operazioni con parti correlate ed in generale i conflitti di interesse;*
- *composizione, ruoli, organizzazione, responsabilità e nominativo del responsabile della funzione di revisione interna, di risk management e di compliance, anche nel caso in cui tali funzioni siano state esternalizzate, incluse le informazioni sulle politiche e sulle procedure stabilite per assicurare che i soggetti responsabili delle predette funzioni ed il referente interno o responsabile delle attività di controllo sulle suddette attività, in caso di esternalizzazione all'interno o all'esterno del gruppo assicurativo, soddisfino i requisiti di professionalità e onorabilità;*
- *rappresentazione della struttura riferita non solo al gruppo assicurativo ma anche a tutti i soggetti richiamati, come controparti di operazioni infragruppo, dall'art. 5 del Regolamento ISVAP n. 25 del 27 maggio 2008, degli assetti proprietari e rapporti con gli azionisti;*
- *le modifiche eventualmente apportate all'organigramma aziendale e al sistema delle deleghe già comunicati all'IVASS*[58]*;*

b) sul sistema di gestione dei rischi dell'impresa che illustri:

- *le strategie, i processi e le procedure di segnalazione, interne ed esterne, nonché le modalità adottate per individuare, misurare, monitorare, documentare, gestire e segnalare efficacemente, su base continuativa i rischi a livello individuale e aggregato cui l'impresa è o potrebbe essere esposta;*
- *le modalità con cui il sistema di gestione dei rischi, compresa la funzione di risk management, è attuato e integrato nei processi decisionali dell'impresa nonché le modalità con cui l'impresa dà esecuzione ai principi che supportano la politica degli investimenti e che sono alla base del sistema di gestione del rischio di investimento, di cui al Regolamento ISVAP n. 36 del 31 gennaio 2011*[59]*.*

[58] Lettera integrata dal Provvedimento ISVAP n. 3020 dell'8 novembre 2012 e successivamente sostituita dalla lettera d) del comma 1 dell'articolo 26 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[59] Lettera sostituita dalla lettera e) del comma 1 dell'articolo 26 del Provvedimento IVASS n. 17 del 15 aprile 2014.

3. La documentazione di cui al comma 2 è previamente sottoposta alla valutazione dell'organo amministrativo.

Art. 28 bis
(Relazione della Capogruppo – comunicazione all'IVASS)[60]

1. *La capogruppo, unitamente al bilancio in qualità di responsabile dell'attività di direzione e coordinamento del gruppo, invia all'IVASS una relazione che illustri:*

   a) *le direttive impartite alle società del gruppo nell'ambito dell'attività di direzione e coordinamento;*

   b) *i sistemi di coordinamento tra gli organi sociali e le funzioni di risk management, compliance e revisione interna del gruppo e tra questi e i relativi organi e funzioni delle singole imprese del gruppo assicurativo;*

   c) *i sistemi di controllo interno e le procedure di gestione dei rischi adottate ai sensi dell'articolo 87 del decreto e delle relative disposizioni di attuazione in materia di controllo interno e gestione dei rischi, inclusi gli esiti degli accertamenti effettuati sulle società del gruppo;*

   d) *i provvedimenti adottati per dare attuazione alle disposizioni impartite dall'IVASS in materia di gruppo assicurativo;*

   e) *gli esiti delle attività di verifica volte ad accertare l'adempimento da parte delle singole imprese componenti il gruppo assicurativo dei provvedimenti adottati in attuazione delle disposizioni dell'IVASS;*

   f) *le modalità con cui i sistemi dei controlli interni e di gestione dei rischi nonché le procedure di reportistica, interne ed esterne, sono attuate in modo coerente in tutte le imprese del gruppo e come le procedure stesse si relazionano con il flusso informativo proveniente dalle imprese incluse nell'area della vigilanza supplementare.*

2. *La relazione di cui al comma 1 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

[60] Articolo inserito dall'articolo 27 del Provvedimento IVASS n. 17 del 15 aprile 2014.

(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;

a bis) i criteri per la qualificazione delle attività come essenziali o importanti, in aggiunta a quanto previsto dalle definizione del presente Regolamento[61]*;*

   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*) *e la frequenza delle stesse*[62];

c bis) i piani di emergenza dell'impresa e le relative procedure, ivi incluse le strategie di uscita nei casi di esternalizzazioni di funzioni e attività essenziali o importanti[63]*.*

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 *almeno*[64] 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;

[61] Lettera inserita dalla lettera a) del comma 1 dell'articolo 28 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[62] Lettera integrata dalla lettera b) del comma 1 dell'articolo 28 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[63] Lettera inserita dalla lettera c) del comma 1 dell'articolo 28 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[64] Comma integrato dall'articolo 29 del Provvedimento IVASS n. 17 del 15 aprile 2014.

f) il fornitore garantisca l'accesso completo ed immediato dell'IVASS 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'IVASS;
i) il contratto non possa essere oggetto di sub-cessione 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*, *sia all'interno che all'esterno del gruppo assicurativo,* deve trattarsi di soggetti con adeguati *requisiti di idoneità alla carica così come definiti dalla politica di cui all'articolo 5, comma 2, lettera l)*[65].

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'*IVASS*[66])

[65] Comma modificato dall'articolo 30 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[66] Rubrica modificata dalla lettera a) del comma 1 dell'articolo 31 del Provvedimento IVASS n. 17 del 15 aprile 2014.

1. *L'IVASS*[67] verifica che l'esternalizzazione delle attività e la loro esecuzione rispettino le condizioni di cui al presente Capo.

2. Qualora, in considerazione *della natura, della portata e della complessità dei rischi inerenti all'attività dell'impresa nonché* 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'*IVASS*[68] 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'IVASS.

Sezione II - Obblighi di comunicazione all'*IVASS*[69]

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'IVASS, 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 *2*[70]*.*

2. Le imprese comunicano tempestivamente all'IVASS se in corso di contratto sono intervenuti cambiamenti rilevanti in merito al fornitore che incidono sul servizio.

3. Le imprese comunicano all'IVASS la cessazione del contratto di esternalizzazione, allegando una relazione sulle modalità di reinternalizzazione dell'attività o di affidamento ad altro fornitore.

Art. 36
(Comunicazioni in caso di esternalizzazione delle funzioni di revisione interna, di risk management e di compliance) [71]

1. *Nel caso di esternalizzazione della funzione di revisione interna, di risk management e di compliance, le imprese ne danno preventiva comunicazione all'IVASS, almeno sessanta giorni prima della esecuzione del contratto, allegando la bozza del contratto stesso e comunicando 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'IVASS. Dovrà altresì essere comunicato il nominativo del referente interno o del responsabile delle attività di controllo sulle funzioni esternalizzate comprensivo delle informazioni di cui all'articolo 33, comma 3.*

2. *Le imprese comunicano tempestivamente all'IVASS se in corso di contratto sono intervenuti cambiamenti rilevanti in merito al fornitore che incidono sul servizio*

[67] Comma modificato dalla lettera dalla lettera b) del comma 1 dell'articolo 31 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[68] Comma modificato dalla lettera dalla lettera c) del comma 1 dell'articolo 31 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[69] Rubrica modificata dall'articolo 32 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[70] Comma modificato dall'articolo 33 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[71] Articolo sostituito dall'articolo 34 del Provvedimento IVASS n. 17 del 15 aprile 2014.

3. *Le imprese comunicano all'IVASS la cessazione del contratto di esternalizzazione, allegando una relazione sulle modalità di reinternalizzazione dell'attività o di affidamento ad un altro fornitore, fornendo, in tale ultimo caso, le informazioni di cui al comma 1.*

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'*IVASS* dei contratti stipulati, in occasione dell'invio del bilancio di esercizio, utilizzando il modello di cui all'allegato *3*[72].

Capo IX – Disposizioni transitorie e finali

Art. 38
(Disposizioni transitorie)

(abrogato)[73]

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 dientrata in vigore del presente Regolamento il termine di adeguamento alle disposizioni di cuiall'articolo 32 è fissato al 1° aprile 2009.

Roma,

Il Presidente

[72] Comma modificato dall'articolo 35 del Provvedimento IVASS n. 17 del 15 aprile 2014.
[73] Articolo abrogato dall'articolo 36 del Provvedimento IVASS n. 17 del 15 aprile 2014.