ISVAP

Istituto per la Vigilanza sulle Assicurazioni Private e di Interesse Collettivo

(only the Italian version is authentic)

REGULATION N. 20 OF 26 MARCH 2008

REGULATION CONCERNING INTERNAL CONTROLS, RISK MANAGEMENT, *COMPLIANCE* AND THE OUTSOURCING OF ACTIVITIES OF INSURANCE UNDERTAKINGS, PURSUANT TO ARTICLES 87 AND 191 (1) OF LEGISLATIVE DECREE N. 209 OF 7 SEPTEMBER 2005 – CODE OF PRIVATE INSURANCE

AMENDED AND SUPPLEMENTED BY ISVAP ORDER N. 3020 OF 8 NOVEMBER 2012 AND BY IVASS ORDER N. 17 OF 15 APRIL 2014.
THE AMENDMENTS AND INTEGRATIONS ARE SHOWN IN ITALICS

VERSION IN FORCE ON 30 JUNE 2014.

ISVAP

(Italian private insurance supervisory authority)

Having regard to law n. 576 of 12 August 1982 and subsequent modifications and integrations, on the reform of insurance supervision;

Having regard to Legislative Decree n. 209 of 7 September 2005 and subsequent modifications and integrations, regarding the Code of Private Insurance;

adopts the following:

REGULATION

INDEX

[1] Article inserted by IVASS Order n. 17 of 15 April 2014.
[2] Article inserted by IVASS Order n. 17 of 15 April 2014.
[3] Article inserted by IVASS Order n. 17 of 15 April 2014.
[4] Article inserted by IVASS Order n. 17 of 15 April 2014.
[5] Article inserted by IVASS Order n. 17 of 15 April 2014.
[6] Article inserted by IVASS Order n. 17 of 15 April 2014.

List of Annexes

Annex 1[7]	*Document about policy papers: minimum contents*
Annex 2[8]	Model for notification of critical or important activities to be outsourced
Annex 3[9]	Statement of outsourced activities and services other than critical or important activities and services

[7] Annex replaced by article 37 (1) of IVASS Order n. 17 of 15 April 2014.
[8] Annex replaced by article 37 (2) of IVASS Order n. 17 of 15 April 2014.
[9] Annex replaced by article 37 (3) of IVASS Order n. 17 of 15 April 2014.

Chapter I – General provisions

Art. 1
(Legislative sources)

1. This Regulation has been adopted in compliance with articles 5 (2), 87 (1), 190 (1) and 191 (1, c) of legislative decree n. 209 of 7 September 2009.

Art. 2
(Definitions)

1. For the purposes of this Regulation, the following definitions shall apply:

   a) “senior management”: the managing director, the director general as well as the senior management which carries out management supervision duties;

   b) “critical or important activities”: activities which, if not performed or performed badly, would seriously compromise the ability of the undertaking to continue to comply with the conditions required to maintain its authorisation to carry out business, or would seriously compromise the undertaking’s financial results and stability or the continuity and quality of its services to policyholders;

   c) “appointed actuary”: the actuary appointed by the insurance undertakings pursuant to articles 31 (1) and 34 (1) of legislative decree n. 209 of 7 September 2005;

   d) "ultimate parent undertaking": the insurance or reinsurance undertaking or insurance holding company, whose head offices are in Italy, as defined by article 83 of legislative decree n. 209 of 7 September 2005 and the relevant provisions for its implementation;

   e) “decree”: legislative decree n. 209 of 7 September 2005, introducing the Code of private insurance;

   f) “outsourcing”: the agreement between an insurance undertaking and a supplier of services, even though not authorised to run insurance business, on the basis of which the supplier performs a process, service or activity which would otherwise be performed by the insurance undertaking itself;

   g) "insurance group": the group of companies referred to in article 82 of legislative decree n. 209 of 7 September 2005 and related implementation measures;

   h) “ISVAP” or “Authority" *or “IVASS”: Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo, which was replaced by IVASS, Istituto per la vigilanza sulle assicurazioni, pursuant to art.13 of decree-law n. 95 of 6 July 2012, converted, after amendment, by law n.135 of 7 August 2012*[10]*;*

   i) "administrative body": the board of directors or the management board, for undertakings which have adopted the system referred to in article 2409 *octies* of the civil code;

[10] Letter amended by article 1 of IVASS Order n. 17 of 15 April 2014. The previous version laid down:““*ISVAP” or “Authority”: Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (Supervisory Authority for Private Insurance Undertakings and Insurance Undertakings of Public Interest)*”.

j) “control body”: the statutory board of auditors, or, in undertakings which have adopted a different system from the one referred to in article 2380 (1) of the civil code, the board of surveillance or the management control committee;

k) "branch": a branch, not having a legal personality, that is part of an insurance or reinsurance undertaking and that directly exercises all or part of the insurance or reinsurance business;

l) “E.E.A.”: the European Economic Area pursuant to the agreement extending European Union regulations to States belonging to the European Free Trade Association, signed in Oporto on 2 May 1992 and ratified by Italian law n. 300 of 28 July 1993;

m) “audit firm”: the accounts auditing company as referred to in article 102 of legislative decree n. 209 of 7 September 2005;

n) "Member State": a Member State of the European Union or a State belonging to the European Economic Area and, as such, treated on a par with the member State of the European Union;

o) "third State": a State which is not a member of the European Union or does not belong to the European Economic Area;

p) “stress test”: an analysis aimed at assessing the impact on undertakings' financial situation of unfavourable trends in risk factors, taken individually or grouped together in a single scenario.

Art. 3
(Scope)

1. The provisions of this Regulation shall apply:

a) to insurance and reinsurance undertakings whose head offices are located in Italy;
b) to branches in Italy of insurance undertakings whose head offices are in a third country;
c) to branches in Italy of reinsurance undertakings whose head offices are in a third country;
d) to ultimate parent undertakings, however limited to the provisions under Chapter VI *and article 28 bis*[11].

Chapter II - System of internal controls

Section I - General principles

Art. 4
(Objectives of the system of internal controls)

1. Insurance undertakings shall set up an appropriate administrative and accounting organisation and an adequate system of internal controls, *proportionate to the*

[11] Letter supplemented by article 2 of IVASS Order n. 17 of 15 April 2014.

nature, scope and complexity of present and perspective corporate risks *inherent in the business of the undertaking*[12].

2. The system of internal controls shall consist in all the rules, procedures and organisational structures aimed at ensuring that the undertaking functions properly and progresses positively and at guaranteeing, with a fair safety margin:

   a) efficiency and effectiveness of corporate processes;
   b) adequate control of *present and perspective* risks[13];
   b bis) timeliness of the corporate information reporting system[14];
   c) reliability and integrity of accounting and management information;
   d) protection of assets *also in a medium and long-term perspective*[15];
   e) compliance of the undertaking's activities with current legislation and with the corporate directives and procedures.

2 bis. The safeguards relating to the system of internal controls and risk management shall cover any type of corporate risk, also based on a forward looking view and with a view to protecting assets. The corporate bodies shall be liable, each according to their own competences. The articulation of corporate activities and of the duties and responsibilities of corporate bodies and functions must be clearly defined[16]*.*

Section II – Role of corporate bodies

Art. 5
(Administrative body) [17]

1. The administrative body shall have the ultimate responsibility over the systems of internal controls *and risk management,* and shall *ensure* that they are always complete, functional and effective, also with regard to outsourced activities. The administrative body shall ensure that the risk management system allows risks to be detected, assessed *even on a forward looking basis* and controlled, including those risks arising from non-compliance with regulations, *guaranteeing the protection of assets even in a medium and long-term perspective.*

2. For the purposes referred to in paragraph 1, and within the scope of the tasks relating to strategic and organisational policy as indicated in article 2381 of the Italian Civil Code, the administrative body:

   a) approves the undertaking's organisational set-up, including the assignment of tasks and responsibilities to its operational units, making sure that they remain adequate over time, *so that they can quickly adjust to changes in the strategic objectives and context in which the undertaking conducts business;*

   b) ensures that adequate decision-making processes are adopted and formalised and that functions are appropriately separated;

[12] Paragraph amended by article 3 (1, a) of IVASS Order n. 17 of 15 April 2014.
[13] Letter supplemented by article 3 (1, b) of IVASS Order n. 17 of 15 April 2014.
[14] Letter inserted by article 3 (1, c) of IVASS Order n. 17 of 15 April 2014.
[15] Letter supplemented by article 3 (1, d) of IVASS Order n. 17 of 15 April 2014.
[16] Paragraph added by article 3 (1, e) of IVASS Order n. 17 of 15 April 2014.
[17] Article replaced by article 4 of IVASS Order n. 17 of 15 April 2014. Insurance and reinsurance undertakings shall comply with the provisions stated under this article by 31 December 2014, as per article 56 (3) of IVASS Order n. 17 of 15 April 2014.

c) approves the system of delegating powers and responsibilities, making sure that it remains adequate over time; takes care in avoiding excessive concentration of powers on one person/entity and sets up instruments for assessing the exercise of delegated powers, with the consequent possibility of providing adequate contingency arrangements if it decides to reserve the delegated powers for itself;

d) defines the directives relating to the system of internal controls, reviewing them at least once a year and making sure that they develop along with corporate operations and external conditions. *Such directives shall also include the policy about the risk management, compliance and internal audit functions. It also verifies that the system of internal controls is consistent with the established strategic policy and risk appetite, and that it is able to capture the evolution of corporate risks and the interaction between them;*

e) approves the policy for the current and forward looking assessment of risks, and the criteria and methodologies used for assessments, with special regard to the most significant ones; approves the results of the assessments and communicates them to the senior management along with its conclusions (top down approach);

f) establishes, based on the assessments referred to under (e), the undertaking's risk appetite consistently with the goal of protecting its assets, by consistently setting the levels of risk tolerance it reviews at least once a year, to ensure their effectiveness over time;

g) approves, based on the elements under (e) and (f), the risk management policy and the strategies, also in a medium and long-term perspective, as well as the contingency plans referred to under article 19 (4) in order to guarantee corporate regularity and continuity;

h) approves, on account of the strategic objectives and consistently with the risk management policy, the underwriting, reserving, reinsurance and other techniques of risk mitigation as well as of operational risk management policies, in line with (e), (f) and (g);

i) defines, whenever the conditions for them are satisfied, the directives and criteria for the circulation and collection of data and information useful for the purposes of performing supplementary supervision as referred to in Title XV of the decree, as well as the directives relating to internal control for checking the related information flows for completeness and timeliness;

j) approves a document consistent with the provisions under (a), (d), (e) and (f) to be circulated to all the relevant structures, which defines i) the duties and responsibilities of corporate bodies, board committees and of the risk management, compliance and internal audit functions; ii) the information flows, including time-scales, between the different functions, the board committees and between the latter and the corporate bodies, and iii), in case the control areas contain areas of potential overlap or facilitate synergies, the arrangements for coordination and collaboration between them and the operational functions. When defining their connection arrangements undertakings shall take care not to alter, also substantially, the ultimate responsibilities of the corporate bodies with respect to the system of internal controls;

k) approves the corporate outsourcing policy referred to under article 31;

l) approves the corporate policy on the assessment of whether the persons charged with administration, management and control functions and the heads of the internal audit, risk management and compliance functions - or, in case

the latter functions are outsourced within or outside the group, the internal contact point or persons responsible for supervision over outsourced activities, referred to under article 33 (3) - fulfil the good repute, professional qualifications and independence requirements. Assesses, at least one a year, that the above persons fulfil said requirements. In particular, such policy shall make sure that the administrative body as a whole possesses sufficient technical knowledge at least in the field of insurance and financial markets, governance systems, financial and actuarial analysis, regulatory framework, business strategies and business models;

m) approves the reporting policy for IVASS, in line with current regulations;

n) checks that senior management correctly implements the system of internal controls and risk management in accordance with its issued directives and assesses its functionality and adequacy;

o) requires to be periodically informed about the effectiveness and adequacy of the system of internal control and risk management and that the most significant critical situations are promptly brought to its attention, whether they are detected by senior management, the internal audit function, *the risk management and compliance functions* or personnel, promptly issuing the directives for the adoption of corrective measures, *whose effectiveness it subsequently assesses;*

p) identifies certain events or circumstances that require prompt intervention by senior management;

q) ensures that there is appropriate interaction between all the committees established within the administrative body, the senior management and the risk management, compliance and internal audit functions, also proactively, to ensure its effectiveness;

r) ensures professional updating on a continuous basis, also extended to the members of the body, providing also adequate training plans to ensure technical skills and knowledge necessary to confidently perform their role while respecting the *nature, scale and complexity* of tasks and preserve their knowledge over time;

s) carries out, at least once a year, an assessment of the size, composition and functioning of the administrative body as a whole and of its committees, advising on the experts whose presence in the administrative body is considered appropriate and proposing possible corrective actions.

3. The administrative body shall ensure that the report on the system of internal controls and risk management adequately *and comprehensively* illustrates the undertaking's organisational structure, and represent the reasons why such a structure is capable of ensuring that the system of internal controls and risk management is complete, functional and effective.

4. The administrative body shall immediately inform the Supervisory Authority should significant changes be made to the organisational structure of the undertaking, illustrating the internal or external causes which made such changes necessary.

5. The policies referred to under paragraph 2 (d), (h), (k), (l) and (m) shall contain at least the elements referred to in annex 1 to this regulation.

Art. 6
(Internal control committee)

1. To carry out the tasks relating to the system of internal controls the administrative body can set up an Internal control committee, consisting of non-executive directors, who are preferably independent pursuant to article 2387 of the Civil Code, to whom it assigns the task of providing advice and making proposals.

2. In particular, the internal control committee shall assist the administrative body in determining policy guidelines in relation to the system of internal controls, periodical checks on its adequacy and its effective functioning, the identification and management of main corporate risks.

3. The administrative body shall define the committee's composition, tasks and operating procedures. The establishment of an internal control committee shall not relieve the administrative body of its own responsibilities.

Art. 7
(Senior management)

1. The senior management shall be responsible for the implementation, maintenance and monitoring of the system of internal controls and risk management, including risks arising from non-compliance with regulations, in accordance with the directives of the administrative body.

2. The senior management:

   a) defines in detail the organisational set-up of the undertaking, the tasks and responsibilities of the operational units and their staff, as well as the decision-making processes in line with the directives issued by the administrative body; within this sphere it implements the appropriate separation of tasks between individuals and functions so as to avoid, as far as it is possible, conflicts of interest;

   b) implements the policies relating to the assessment, *even on a forward looking basis*[18], and management of risks as established by the administrative body, ensuring the definition of operational limits and prompt checks on those same limits, as well as the monitoring of exposures to risks and compliance with the levels of tolerance;

   b bis) implements, on account of the strategic objectives and consistently with the risk management policy, the underwriting, reserving, reinsurance and other techniques of risk mitigation as well as of operational risk management policies[19]*;*

   c) sees to the maintenance of the functionality and overall adequacy of the organisational set-up, the system of internal controls and risk management, including risks arising from non-compliance with regulations;

   d) checks that the administrative body is periodically informed about the effectiveness and adequacy of the system of internal controls and risk management as well as of the compliance function and, nevertheless, promptly every time significant critical situations come to light;

[18] Letter supplemented by article 5 (1, a) of IVASS Order n. 17 of 15 April 2014.
[19] Letter inserted by article 5 (1, b) of IVASS Order n. 17 of 15 April 2014.

e) implement the instructions given by the administrative body on the measures to be adopted in order to correct faults that have come to light and make improvements;

f) proposes to the administrative body initiatives aimed at adjusting and reinforcing the system of internal controls and risk management.

Art. 8
(Control body)

1. The control body shall check the adequacy of the organisational, administrative and accounting set-up, as adopted by the undertaking, and see that it functions in practice.

2. To carry out its tasks as referred to in paragraph 1, the control body can request the collaboration of all structures that carry out supervisory *tasks*[20].

3. The control body:

a) acquires knowledge about the corporate organisational set-up at the start of its term of office, and examines the results of the auditing company's work on the assessment of the system of internal control and the administrative accounting system;

b) checks on the appropriateness of the definitions used in delegating powers, as well as the adequacy of the organisational set-up, paying particular attention to the separation of responsibilities in tasks and functions;

c) assesses the efficiency and effectiveness of the system of internal controls, with particular attention to the work of the internal audit function, where it must check that it has the necessary autonomy, independence and functionality; if this function has been outsourced, it assesses the content of the assignment on the basis of the relevant contract;

d) maintains adequate links with the internal audit function;

e) sees to the prompt exchange with the auditing company of data and information of relevance for the carrying out of its tasks, also examining the periodic reports by the auditing company;

f) brings to the attention of the administrative body any faults or weaknesses in the organisational set-up and system of internal controls, by indicating and urging appropriate corrective measures; during the term of office it plans and performs, also in coordination with the auditing company, periodic inspections aimed at ascertaining whether any already detected shortcomings or faults have been overcome and whether, in comparison with the assessments made at the beginning of its term of office, there have been any significant changes in the undertaking’s activity, which require an adjustment of the organisational set-up and of the system of internal controls;

g) when there are companies belonging to the same insurance group, it ensures that the functional and informative links with the control bodies in the other undertakings are in place;

h) keeps adequate documentation regarding the comments and proposals made and the subsequent checks performed to verify the implementation of the corrective measures.

[20] Paragraph supplemented by article 6 of IVASS Order n. 17 of 15 April 2014.

Art. 9
(Formalisation of documents)

1. The work of the administrative, management and control bodies shall be adequately documented so as to allow control over the management acts and decisions taken.

Section III – Constituents of the system of internal controls

Art. 10
(Internal control environment)

1. The administrative body shall promote a high level of integrity and an internal control environment so as to make all staff aware of the importance and usefulness of internal controls.

2. The senior management shall be responsible for promoting the internal control environment and ensure that staff are made aware of their own role and responsibilities so as to be effectively engaged in controls, seen as an integral part of their own activity. For this purpose it shall ensure the formalisation and adequate distribution among staff of the power delegation system and of the procedures which govern the assignment of tasks, the operational processes and the reporting channels.

3. The senior management shall promote continuous training and communication initiatives aimed at favouring the effective adherence of all staff to the principles of moral integrity and to ethical values.

4. To promote operational correctness and respect for integrity and ethical values by al staff, and to prevent deviant forms of conduct which undertakings might be called to answer for, pursuant to legislative decree n. 231 of 8 June 2001, as well as pursuant to article 325 of legislative decree n. 209 of 7 September 2005, they shall adopt an ethical code defining rules of behaviour, regulating potential conflicts of interests and envisaging adequate corrective actions, in case of deviation from the directives and procedures approved by the top management or violation of the current legislation or of the ethical code itself.

5. Undertakings shall avoid, at every corporate level, remuneration policies and practices which might be an incentive to illegal or deviant activity compared to the ethical and legal standards, or induce risk appetite in contrast with the interests of the company.

Art. 11
(Supervisory activities and separation of tasks)

1. The system of internal controls shall provide for the carrying out, at all the undertaking's levels, of control activities proportioned *to the nature, scope and complexity of the risks inherent in the undertaking's business*[21], which contribute

[21] Paragraph amended by article 7 (1, a) of IVASS Order n. 17 of 15 April 2014.

towards ensuring that the corporate directives are implemented and verifying that they are complied with.

2. The control activities referred to in paragraph 1 shall be formalised and reviewed on a periodic basis and involve the whole staff. Those activities shall include mechanisms for double signatures, authorisations, checks and comparisons, control lists and reconciliation of accounts, as well as limiting the access to transactions only to the persons assigned to them and the recording and periodical checks of the transactions performed.

3. Insofar as this is in accordance with *the nature, scope and complexity of the undertaking's operations, the latter*[22] shall ensure, within the scope of the corporate functions, an adequate level of independence of the staff responsible for control compared to those with operational duties.

Art. 12
(Information flows and communication channels)

1. Undertakings must possess accounting and management information which guarantee adequate decision-making processes and allow definitions and assessments to be made as to whether the strategic objectives established by the administrative body have been reached so that they can be reviewed, if necessary. For this purpose the senior management shall ensure that the administrative body has full knowledge of the most important corporate facts, also through an adequate reporting system.

2. The system of internal controls shall ensure that information complies with the principles of accuracy, completeness, promptness, consistency, transparency and pertinence in line with the following definitions:

   a) *accuracy*: the information must be verified at the moment it is received and before it is used;
   b) *completeness:* the information must cover all the important aspects of the company in terms of quantity and quality, including indicators which might have direct or indirect consequences on the strategic planning of business;
   c) *promptness:* the information must be available promptly so as to facilitate efficient decision-making processes and allow the undertaking to foresee and react promptly to future events;
   d) *consistency*: the information must be recorded using methods which make the information easy to compare;
   e) *transparency*: the information must be presented in such a way as to be easy to interpret, ensuring clarity in the essential components;
   f) *pertinence*: the information used must be in direct relation to the aims for which it is required and be continuously reviewed and expanded to ensure that it complies with the undertaking's needs.

3. The information addressed to third parties, such as the Authority, policyholders and the market must be reliable, prompt and pertinent and must be conveyed clearly and efficiently.

[22] Paragraph amended by article 7 (1, b) of IVASS Order n. 17 of 15 April 2014.

4. The system of internal accounting and data management shall correctly register the facts of administration and provide a true and correct representation of the undertaking's financial and economic position and in compliance with laws and secondary regulations.

5. Undertakings shall set up and maintain efficient communication channels both inside and outside the undertaking in all directions.

6. The system must facilitate the reporting of critical circumstances also using procedures that allow the personnel to bring the particularly serious situations to the direct attention of the highest levels within the hierarchy.

Art. 12 bis
(Data management system)[23]

1. *Undertakings shall envisage a data registration and reporting system that makes it possible to trace such data, so that complete and up-to-date information is available about the elements which can have an impact on the undertaking's profile and on its solvency situation.*

2. *The system referred to under paragraph 1 shall ensure, on an on-going basis, that the data kept and the information shown are whole, complete and correct, also in order to allow for the reconstruction of the activity performed and the identification of the relevant responsible persons; it shall also ensure that the information recorded is easily assessed.*

3. *The undertaking shall define a data governance corporate standard identifying the roles and responsibilities of the functions involved in the use and processing of corporate information.*

4. *In case the undertaking uses a corporate data warehouse for analysis and reporting purposes, the procedures for data extraction, control and loading onto the centralised archives – as well as the data use activity – shall be documented in order to allow the quality assessment of information.*

5. *Data management and aggregation procedures shall be documented, with the specific indication of the conditions under which manual entries or the correction of corporate data are allowed.*

6. *The processes of data acquisition from external structures shall be documented and monitored.*

7. *Data shall be stored with adequate granularity to enable the various analyses, and the aggregation required by the possible procedures for their use.*

8. *At first-time application of the provisions under this article undertakings shall prepare an implementation plan by 31 October 2014.*

[23] Article inserted by article 8 of IVASS Order n. 17 of 15 April 2014.

Art. 13
(Production of data and information for supplementary supervision)

1. Undertakings shall set up efficient information flows for the production of data and information which can be used for exercising supplementary supervision, where applicable, *and for the current and prospective assessment of risks at the group level made by the ultimate parent undertaking in line with article 27 (5)*, by adopting appropriate internal control procedures and identifying *appropriate collection and coordination measures between the information flows of supplementary supervision and those of the insurance group and undertaking*[24].

2. Undertakings shall keep the data and information as referred to in paragraph 1 on their head office, for potential inspections *by IVASS*[25].

Art. 14
(IT systems)

1. The IT systems must be appropriate in respect of *the nature, scope and complexity of the undertaking's activity and the consequent risks*[26] and must provide information both internally and externally, that comply with the principles referred to in article 12 (2).

2. For the purposes as referred to in paragraph 1:

   a) the administrative body shall approve a strategic plan on information and communication technology (ICT), aimed at ensuring the existence and maintenance of an overall systems architecture which is highly integrated both from an applicational and technological point of view and adequate for the needs of the undertaking;

   b) the development and production environments shall be separate. Access to the various environments shall be regulated and controlled through designed procedures, taking into account the need to limit the risks of fraud arising from outside intrusion or untrustworthy personnel. For this purpose the procedures shall ensure the logical security of the processed data, restricting access to the data to authorised personnel, in particular for the production environment, and stipulate that all violations are highlighted; the procedures shall be subject to inspections by the internal audit function;

   c) procedures for approving and acquiring hardware and software, as well as for the outsourcing of certain services, shall be formalised;

   d) procedures shall be adopted that ensure the physical safety of hardware, software and data banks also through the use of disaster recovery and backup procedures;

   e) to ensure continuity in the organisation’s processes, certain procedures and operational standards shall be adopted and documented, that are oriented towards the identification and management of events that could jeopardise the continuity of business, such as for example, unforeseen events, black outs, fires, floods, malfunction of hardware and software, operational errors by

[24] Paragraph amended by article 9 (1, a) of IVASS Order n. 17 of 15 April 2014. The previous version laid down: “*1. The undertakings shall set up efficient information flows for the production of data and information for exercising supplementary supervision, where applicable, by adopting appropriate internal control procedures and identifying a specific function for the production of such data and information*”.
[25] Paragraph amended by article 9 (1, b) of IVASS Order n. 17 of 15 April 2014.
[26] Paragraph amended by article 10 of IVASS Order n. 17 of 15 April 2014.

personnel in charge of systems management or by users, involuntary introduction of components that damage the IT and network system, and criminal acts aimed at reducing the availability of information.

3. When there are extraordinary transactions such as mergers or portfolio acquisitions, the undertaking shall prepare an IT systems integration plan in which the following shall be specified:

   a) environments, functions, procedures, applications and data bases involved in the integration process;
   b) the time-scales of each integration phase, with particular attention to data bases migration and to the dates on which the integration of portfolios (premiums, claims etc.) are completed;
   c) the units and organisational safeguards which are assigned the controls and monitoring of the entire integration process.

Chapter III – Internal audit

Art. 15
(Internal audit function)[27]

1. Undertakings shall set up an internal audit function, assigned with the task of monitoring and assessing the efficiency and effectiveness of the system of internal controls as well as the need for improvement, also through advisory and support activities in favour of the other corporate functions.

2. The Internal audit function must have the following characteristics:

   a) the position of the function within the sphere of the organisational structure must be such as to guarantee its independence and autonomy so that its objective judgement is not compromised; the internal audit function shall not be hierarchically subordinate to any head of an operational area; none of the persons assigned to the internal audit function must be given operational responsibilities or inspection tasks in activities over which they had authority or responsibility in the past, unless a reasonable period of time has elapsed since then;

   b) *those assigned to the function must be allowed free access to all corporate structures and documentation relating to the specific corporate area under inspection, including information which is useful in checking the adequacy of the controls performed on outsourced corporate functions;*

   c) *the function must have organic links with all the centres in charge of internal control functions;*

   d) *the dedicated structure must be adequate in terms of human and technological resources in respect of the nature, scope and complexity of the undertaking's activity and the development objectives it intends to achieve. The staff within the structure must have specialist expertise, and their professional training must be looked after carefully.*

3. The internal audit function shall align its activity to the professional standards commonly accepted at a national and international level and shall check on:

[27] Article replaced by article 11 of IVASS Order n. 17 of 15 April 2014.

a) the management processes and organisational procedures;
b) the regularity and functionality of the information flows among corporate areas;
c) the adequacy and reliability of information systems, so that the quality of the information on which the corporate top management bases its own decisions is not invalidated;
d) compliance of administrative and accounting processes with correctness and fair accounting standards;
e) the efficiency of the controls performed on outsourced activities.

4. During audits and when assessing and reporting the relevant results the internal audit function shall perform the tasks attributed to it with autonomy and objectivity of judgement, so as to preserve its independence and impartiality, in line with the relevant directives by the administrative body.

5. *The internal audit shall finish with the follow-up activities, consisting in future checks on the effectiveness of the corrections made to the system.*

Art. 15 bis
(Head of the internal audit function)[28]

1. The head of the function shall be appointed or dismissed by the administrative body after hearing the Statutory Board of Auditors and, where provided, also the Internal Control Committee, and comply with the fit and proper requirements set by the policy referred to under article 5 (2, l). The tasks assigned to the head of the function shall be clearly defined and approved by a resolution of the administrative body, which also establishes the head of the function's powers, responsibilities and procedures for reporting to the administrative body.

2. The head of the function shall possess the necessary authority to ensure the functions' independence.

3. The head of the internal audit function shall plan his/her activities annually, so as to detect the areas which need to be subjected to an audit in priority. Such plan and its priority level shall be consistent with the main risks to which the undertaking is exposed. The planning of the audit actions shall take account of any deficiencies found during the audits already made and of any new risk detected. The plan shall also include audits of the constituents of the system of internal controls, in particular of the information flow and IT system. The audit plan shall be approved by the administrative body and identify, at least, the risk activities, operations and systems to be audited, describing the criteria on the basis of which these have been selected and specifying the resources required to carry out the plan. A similar procedure shall be carried out if significant changes are made to the approved plans, which nevertheless shall be defined in order to cope with unforeseen needs.

4. Where necessary, audits which are not included in the audit plan may be carried out.

5. Following the analysis of the activity under inspection, the head of the function shall, in accordance with the procedures and periodicity established by the administrative body, communicate to the administrative body, senior management and control body his/her assessment of the results and of any

[28] Article inserted by article 12 of IVASS Order n. 17 of 15 April 2014.

dysfunctions and critical situations; it shall also have the obligation to urgently bring to the attention of the administrative and control body any particularly serious situations. Audit reports must be impartial, clear, concise and timely, contain suggestions to remove any deficiency and recommendations about the time-scales for removing them; they must be kept at the undertaking's head office. The results of the specific area subject to control shall be also disclosed to the head of the function concerned with the audit.

6. *The head of the internal audit function shall submit to the administrative body, at least annually, a report about his/her activity summarising all the audits, results, weaknesses or deficiencies and the recommendations made for their removal; the summary report shall include the follow-ups, with the indication of the outcome of the assessments referred to under art. 15 (5) of the persons and/or functions to be removed, and the type, effectiveness and time-scales of the action made to remove the critical situations initially found.*

Art. 16
(Outsourcing of the internal audit function)

1. Undertakings for which, *due to the reduced scale and complexity of the risks inherent in the undertaking's business*[29], the establishment of an internal audit function is not economically feasible can outsource such function, also within the insurance group, in compliance with the conditions referred to in Chapter VIII.

2 The activities of the internal audit function can be grouped together within the insurance group by setting up a specialised unit, provided that:

a) each undertaking in the insurance group selects a referent subject who serves as contact with the group head of the function;
b) appropriate procedures are adopted to ensure that the activities of the internal audit function, as defined at insurance group level, are suitably calibrated to the operational characteristics of the individual undertakings.

Art. 17
(Collaboration between functions and bodies charged with control)

1. The control body, the auditing company, the internal audit, risk management and compliance functions, the monitoring board as referred to in legislative decree n. 231 of 8 June 2001, the appointed actuary and every other body or function which is assigned a specific control function shall collaborate with each other, exchanging all information which is useful in carrying out their respective tasks.

2. The administrative body shall define and formalise the links between the various functions assigned with control tasks.

[29] Paragraph amended by article 13 of IVASS Order n. 17 of 15 April 2014.

Chapter IV – Risk management

Art. 18
(Objectives of the risk management system)[30]

1. *The risk management system with which the undertaking has equipped itself shall comprise the strategies, processes and procedures - including reporting procedures - necessary to identify, measure, assess, monitor, manage and report, on a continuous basis, the current and future risks, at an individual and at an aggregated level, to which the undertaking is or could be exposed, and their interdependencies.*

2. To the maintain the risks to which undertakings are exposed at a reasonable level, consistent with their available assets, they shall set up an adequate risk management system, *in line with their risk management policy*, proportionate to the nature, *scale* and complexity of the business they do, which allows the detection, the *forward-looking* assessment and control of the risks, *with particular regard to* the most significant ones. Significant risks are defined as those whose consequences could compromise the undertaking's solvency or create a serious obstacle to the achievement of corporate objectives.

3. Policies relating to risk assumption, *assessment* and management shall be defined and implemented by taking as a reference point the integrated view of the balance sheet assets and liabilities, considering that the development in techniques and asset-liability management models is fundamental for a correct understanding and management of exposures to risks, which can occur due to inter-relationships and imbalance between assets and liabilities. *The risk management policy shall also take account of the risk arising from investments, including the liquidity risk, and the so-called prudent person principle which, in line with the objectives under paragraph 1, underlies the undertaking's investment choices.*

4. *The underwriting, reinsurance and other techniques of risk mitigation as well as of operational risk management policies must take account of the undertaking's strategic objectives and be consistent with the risk management policy referred to under paragraph 2. For the purposes of operational risk management, undertakings shall identify adequate methods of analysis which take also account of the occurrence of external events.*

Art. 19
(Identification of risks)[31]

1. *Undertakings shall define the risk categories according to the nature, scale and complexity of the risks inherent to the business pursued, both on a current and on a forward-looking basis. The catalogue shall include at least the following risks:*

   a) ***underwriting risk:*** *the risk arising from the underwriting of insurance contracts, associated with the events covered and processes followed due to the pricing and selection of risks, with unfavourable trends in actual claims compared to those forecast;*

   b) ***reserving risk:*** *the risk linked to the quantification of technical provisions that are not sufficient compared to the commitments undertaken in favour of those policyholders or third parties;*

[30] Article replaced by article 14 of IVASS Order n. 17 of 15 April 2014.
[31] Article replaced by article 15 of IVASS Order n. 17 of 15 April 2014.

c) ***market risk:*** *the risk of making losses due to variations in interest rates, share prices, exchange rates and real estate prices;*

d) ***credit risk:*** *the risk linked to breaches of contract by issuers of financial instruments, reinsurers, intermediaries and other counter-parties;*

e) ***liquidity risk:*** *the risk of not being able to fulfil one's obligations to policyholders and other creditors due to difficulties in transforming investments into liquid cash without suffering losses;*

f) ***operational risk:*** *the risk of losses arising from inefficiency of people, processes and systems, including those used for distance selling, or external events, such as fraud or the activities of service suppliers;*

g) ***group risk:*** *risk of "contagion", i.e. the risk that, subsequent to the relationships that take place between an undertaking and the other entities in the group, difficult situations arising in one entity within the same group can spread with negative effects on the solvency of the undertaking itself; risk of conflict of interests;*

h) ***risk of non-compliance with regulations:*** *the risk of incurring judicial or administrative sanctions, suffering losses or damage to reputation as a consequence of the failure to comply with laws, regulations or provisions issued by the supervisory Authority or self-regulatory rules, such as articles, codes of conduct or self-disciplinary codes; risk arising from unfavourable changes in the law or judicial orientation;*

i) ***reputational risk:*** *the risk of deterioration in the corporate image and of an increase in the conflict with insurance customers, due to the poor quality of services offered, the placement of inadequate policies or the behaviour of the sales network.*

2. *Undertakings shall collect information on a continual basis about internal and external, and current and future risks to which they are exposed and which could involve all the operational processes and functional areas. The procedure relating to risk census and its related results are adequately documented.*

3. Using an adequate process of analysis, undertakings must be able to understand the nature of the risks they have identified, their origins, their possible aggregation and correlation, the possibility or need to control them and the effects that could arise, both in terms of losses and opportunities.

4. *Undertakings shall define procedures which can promptly highlight the appearance of risks that might jeopardise the safeguard of their assets, also in the medium and long term, damage their financial and economic situation or involve the overcoming of the established tolerance thresholds. The undertaking shall prepare adequate contingency plans in respect of the major risk sources detected; such plans shall be periodically reviewed and updated, and their effectiveness shall be assessed at least annually, and shall be approved by the administrative body.*

Art. 19 bis
(Evaluation of risks)[32]

1. *Undertakings shall evaluate the risks to which they are exposed, both on a current and on a forward-looking basis, at least once a year and at any time circumstances*

[32] Article inserted by article 16 of IVASS Order n. 17 of 15 April 2014.

arise that could significantly alter their risk profile, in accordance with the provisions of the risk assessment policy.

2. *For the purpose of the evaluations referred to under paragraph 1, undertakings shall define a process of risk analysis including a qualitative assessment and, for quantifiable risks, the adoption of methods to measure risk exposure, including, where appropriate, systems for determining the maximum potential loss. When measuring risk and where appropriate, undertakings shall consider the inter-relations between risks, assessing them singularly and on an aggregate basis.*

3. *The processes for evaluating risks shall be carried out on a continual basis so as to take into account the changes in the nature, scope and complexity of the undertaking's activity and the market context and also the appearance of new risks or changes in those that exist already. Particular attention shall be given to evaluating risks that may arise from offering new products of from entering into new markets.*

4. *The methods of evaluation and measuring risks and the related results shall be adequately documented.*

5. *The results of the evaluations, along with the methods used, shall be submitted to the administrative body which, after discussing and approving them, shall disclose them to the senior management and to the structures concerned along with its conclusions*[33]*.*

Art. 20
(Stress tests and other analysis tools)[34]

1. For each of the sources of risk that undertakings have identified as being particularly significant on the basis of the processes referred to in article *19 bis*, undertakings shall carry out *qualitative* and quantitative prospective analyses, by *also* [35]using stress tests.

2. *Quantitative analyses*, based on deterministic or stochastic models, shall be designed and developed to be consistent with *the nature, scale and complexity of the risks inherent in the undertaking's business* and repeated according to the frequency required by the type of risk, the development *in the nature, scale and complexity of the undertaking's business* and the market context, and shall be done, in any case, at least once a year[36].

3. The results *of the qualitative and quantitative analyses*, together with the underlying assumptions *and methodologies used*[37], shall be brought to the attention of the administrative body so as to make a contribution towards the review and improvement of risk management policies, operational guidelines and exposure limits established by the administrative body itself.

[33] Insurance and reinsurance undertakings shall comply with the provisions stated under thisparagraph by 31 December 2014, pursuant to article 56 (3) of IVASS Order n. 17 of 15 April 2014.
[34] Heading integrated by article 17 (1, a) of IVASS Order n. 17 of 15 April 2014.
[35] Paragraph supplemented by article 17 (1, b) of IVASS Order n. 17 of 15 April 2014.
[36] Paragraph replaced by article 17 (1, c) of IVASS Order n. 17 of 15 April 2014. The previous version laid down: "*2. Stress tests, based on deterministic or stochastic models, are designed and developed to be consistent with the size and nature of the undertaking's business and are repeated according to the frequency required by the type of risk, the development in the size and nature of the undertaking's business and the market context, and are done, in any case, at least once a year".*
[37] Paragraph amended by article 17 (1, d) of IVASS Order n. 17 of 15 April 2014.

4. If the results of the quantitative analyses indicate a particular vulnerability towards a given series of circumstances, undertakings shall adopt appropriate measures for adequately managing the relevant risks.

5. When requested to do so by IVASS, undertakings shall carry out standardised *qualitative or quantitative*[38] *analyses* on the basis of pre-established risk factors and parameters.

Art. 21
(Risk management function)[39]

1. *Undertakings shall set up a risk management function, proportionate to the nature, scale and complexity of the risks inherent to the undertaking's business, which:*

   a) *contributes towards the definition of the risk management policy and defines the criteria and relevant methods of measuring risks as well as the results of the evaluations, which it shall submit to the administrative body. After discussing and approving them, the administrative body shall disclose them to the senior management and to the structures concerned along with its conclusions, as per article 5 (2, e);*

   b) *contributes towards the definition of the operational limits assigned to the operational structures and defines the procedures for promptly checking such limits;*

   c) *validates the information flows required to ensure prompt control of exposures to risk and the immediate detection of faults found in operations;*

   d) *makes the evaluations referred to in article 19 bis, of the undertaking's risk profile and reports to the administrative body the risks that the undertaking has identified as being particularly significant, as per article 18 (2, last sentence), also in potential terms;*

   e) *prepares the procedures for reporting to the administrative body, senior management and the heads of the operational structures regarding the development in risks and the breach of established operational limits;*

   f) *checks the adequacy of the risk measuring models with the operations carried out by the undertaking and contributes to the carrying out of the quantitative analyses referred to under article 20;*

   g) *monitors the implementation of the risk management policy and the overall undertaking's risk profile.*

2. *The establishment of the risk management function shall be formalised in a specific resolution by the administrative body, which shall define its responsibilities, tasks, operational procedures and the nature and frequency of reporting to the corporate bodies and other functions involved, in accordance with the document approved by the administrative body as per article 5 (2, j).*

3. *The organisational position of the risk management function shall be left to the autonomy of undertakings, but in accordance with the principle of separation between operational and control functions. Undertakings shall set up the risk management function in the form of a specific organisational unit or, taking into consideration the nature, the reduced scale and complexity of the risks inherent in*

[38] Paragraph amended by article 17 (1, e) of IVASS Order n. 17 of 15 April 2014.
[39] Article replaced by article 18 of IVASS Order n. 17 of 15 April 2014.

the undertaking's business, by also using resources belonging to other corporate units. In the latter case, independence shall be ensured by the presence of appropriate safeguards that guarantee separation of duties and prevent conflicts of interest. The risk management function shall report to the administrative body, even when it is not constituted in the form of a specific organisational unit. The organisational position of the risk management function must be such as not to depend on operational functions.

4. *The links between the risk management function and the internal audit and compliance functions shall be defined and formalised by the administrative body.*

5. *The risk management function shall be nevertheless separated from the internal audit function and shall be periodically subject to audit by the latter.*

Art. 21 bis
(Head of the risk management function)[40]

1. *Irrespective of the organisational form chosen pursuant to article 21 (3), undertakings shall appoint the head of the risk management function who satisfies the fit and proper requirements set by the policy referred to in article 5 (2, l). The administrative body shall be responsible for appointing and dismissing this head.*

2. *The Compliance responsible officer must not be the head of an operational area nor must he report to persons in charge of these areas.*

3. *The head of the function shall submit to the administrative body, at least annually, a scheme of operations illustrating the main risks to which the undertaking is exposed and his/her proposals in relation to those risks. The scheme shall also take account of any deficiencies found during the previous assessments and of any new risks.*

4. *The head of the function shall draft a report, at least once a year, for the administrative body on the adequacy and effectiveness of the risk management system, the methodologies and models used for the protection against such risks, about his/her activity, the assessments made, the results and the critical situations found, and illustrating the status of implementation of the relevant improvement actions, if taken.*

Art. 21-ter
(Outsourcing of the risk management function)[41]

1. *Undertakings in which, due to the reduced scale and complexity of the risks inherent in the undertaking's business, the establishment of a specific risk management function is not economically feasible, can outsource such function, in compliance with the conditions as referred to in Chapter VIII.*

2. *The activities of the risk management functions can be grouped together within an insurance group through the establishment of a specialised unit, provided that:*

   a) *each undertaking in the insurance group selects a referent subject who serves as contact with the group head of the function;*

[40] Article inserted by article 19 of IVASS Order n. 17 of 15 April 2014.
[41] Article inserted by article 20 of IVASS Order n. 17 of 15 April 2014.

b) adequate procedures are adopted to ensure that the activities of the risk management function, as defined at insurance group level, are suitably calibrated to the risk profile of the individual undertakings.

Chapter V – Compliance FUNCTION

Art. 22
(Objectives of the assessment of compliance)

1. Within the sphere of the system of internal controls, undertakings shall set up, at every pertinent corporate level, specific safeguards whose aim it is to prevent the risk of incurring judicial or administrative sanctions, suffering losses or damage to reputation as a consequence of breaches of the laws, regulations or provisions issued by the supervisory Authority or self-regulatory rules.

2. In identifying and assessing the risk of non-compliance with regulations, undertakings shall pay particular attention to compliance with regulations relating to transparency and correctness in behaviour towards policyholders and third parties, pre-contractual and contractual information and the correct execution of contracts, with particular reference to claims management and, more in general, consumer protection.

Art. 23
(Compliance function)

1. Undertakings shall set up a compliance function, proportionate to the nature, scale and complexity of the risks inherent in the undertaking's business[42], which shall be given the task of evaluating whether the organisation and internal procedures are adequate for achieving the objectives referred to in article 22.

2. The establishment of the compliance function shall be formalised in a specific resolution by the administrative body, which shall define its responsibilities, tasks, operational procedures and the nature and frequency of reporting to the corporate bodies and other departments involved.

3. The compliance function:
   a) identifies on a continual basis the regulations that apply to the undertaking and assesses their impact on the company's processes and procedures;
   b) assesses the adequacy and effectiveness of the organisational measures adopted to prevent the risk of non-compliance with regulations and proposes organisational and procedural changes aimed at ensuring adequate protection against the risk;
   c) assesses the effectiveness of the organisational adjustments following the proposed changes;
   d) prepares adequate information flows to the undertaking's corporate bodies and the other structures involved.

[42] Paragraph amended by article 21 (1, a) of IVASS Order n. 17 of 15 April 2014.

4. The compliance function must have adequate independence, free access to all the undertaking's activities and pertinent information, and have sufficient and adequately professional resources at its disposal to carry out its duties.

5. *The organisational position of the compliance function shall be left to the autonomy of undertakings, but in accordance with the principle of separation between operational and control functions. Undertakings shall set up the compliance function in the form of a specific organisational unit or, taking into consideration the nature, the reduced scale and complexity of the risks inherent in the undertaking's business, by also using resources belonging to other corporate units. In the latter case, independence shall be ensured by the presence of appropriate safeguards that guarantee separation of duties and prevent conflicts of interest. The compliance function shall report to the administrative body, even when it is not constituted in the form of a specific organisational unit. The organisational position of the compliance function must be such as not to depend on operational functions*[43]*.*

6. *(repealed)*[44]

7. The links between the Compliance function and the Internal audit and Risk management functions are defined and formalised by the administrative body.

8. The compliance function shall be nevertheless separated from the internal audit function and shall be periodically subject to audit by *the latter*[45].

Art. 24
(Head of the compliance function)

1. Irrespective of the organisational form chosen pursuant to article 23 (5), undertakings shall appoint a head of the compliance function *who satisfies the fit and proper requirements set by the policy in accordance with article 5 (2, l)*[46]*.* The administrative body shall be responsible for appointing and dismissing this head.

2. The head of this function must not be in charge of any operational areas, nor may he/she be hierarchically subordinated to the heads of such areas. As justified by *the nature, scope and complexity of the undertaking's activity*[47], an administrator may be put in charge of this function, provided he/she has not otherwise been delegated.

2 bis. The head of the function shall submit to the administrative body, at least annually, a scheme of operations illustrating the actions he/she intends to take in relation to the the risk of non-compliance with regulations. The scheme of actions shall also take account of any deficiencies found during the previous assessments and of any new risks[48]*.*

2 ter. Where necessary, assessments which are not included in the scheme of operations may be carried out[49]*.*

[43] Paragraph replaced by article 21 (1, b) of IVASS Order n. 17 of 15 April 2014. The previous version laid down: "*5. In line with their own autonomy, undertakings organise the compliance function, assessing whether to establish it in the form of a specific organisational unit or whether to use resources belonging to other company units. If the latter is the case, then the function's independence must be guaranteed by the creation of adequate safeguards to ensure the separation of tasks and prevent conflicts of interest*".
[44] Paragraph repealed by article 21 (1, c) of IVASS Order n. 17 of 15 April 2014.
[45] Paragraph supplemented by article 21 (1, d) of IVASS Order n. 17 of 15 April 2014.
[46] Paragraph amended by article 22 (1, a) of IVASS Order n. 17 of 15 April 2014.
[47] Paragraph amended by article 22 (1, b) of IVASS Order n. 17 of 15 April 2014.
[48] Paragraph added by article 22 (1, c) of IVASS Order n. 17 of 15 April 2014.
[49] Paragraph added by article 22 (1, d) of IVASS Order n. 17 of 15 April 2014.

3. *The head of the function shall draft a report, at least once a year, for the administrative body on the adequacy and effectiveness of the safeguards adopted by the undertaking for the protection against the risk of non-compliance with regulations, about the activity performed, the assessments made, the results and the critical situations found, and illustrating the status of implementation of the relevant improvement actions, if taken*[50]*.*

Art. 25
(Outsourcing the compliance function)

1. Undertakings in which, *due to the reduced scale and complexity of the risks inherent in the undertaking's business*[51], the establishment of a specific compliance function is not economically feasible, can outsource such function, in compliance with the conditions as referred to in Chapter VIII.

2. The activities of the compliance function can be grouped together within an insurance group through the establishment of a specialised unit, provided that:

   a) each undertaking in the insurance group selects a referent subject who serves as contact with the group head of the function;
   b) adequate procedures are adopted to ensure that the policies relating to the management of the risk of non-compliance, as defined at insurance group level, are suitably calibrated to the operational characteristics of the individual undertakings.

Chapter VI – Provisions relating to insurance groups

Art. 26
(Role of the ultimate parent undertaking)

1. Within the scope of its activity of management and coordination of the insurance group, the ultimate parent undertaking shall exercise:

   a) strategic control over the development of the various areas of business in which the insurance group operates and the risks related to them. The control shall centre round the expansion of the business carried out by the companies belonging to the insurance group and the policies relating to acquisition or alienation of companies in the insurance group;
   b) management control aimed at ensuring the maintenance of balanced conditions in the economic and financial situations of the individual undertakings and of the insurance group as a whole;
   c) a technical, operational control aimed at assessing the various risk profiles that each subsidiary brings to the insurance group.

[50] Paragraph replaced by article 22 (1, b) of IVASS Order n. 17 of 15 April 2014. The previous version laid down: *"The responsible officer prepares a report, at least once a year, for the administrative body on the adequacy and effectiveness of the safeguards adopted by the undertaking in managing the risk of non-compliance with standards."*
[51] Paragraph amended by article 23 of IVASS Order n. 17 of 15 April 2014.

Art. 27
(Internal control and risk management in the insurance group)[52]

1. *On the understanding that each insurance and reinsurance undertaking having its head office in Italy and belonging to an insurance group sets up its control and risk management system in accordance with the provisions of Chapters III, IV and V, the ultimate parent undertaking shall set up a system of internal controls and risk management for the insurance group which is consistent with the governance requirements at group level, and adequate for carrying out effective control over the group's overall strategic choices and the management balance of each individual component.*

2. *The responsibility of the administrative body of each undertaking in the insurance group for its governance and the undertakings' system of internal controls and risk management shall not be affected.*

3. *In particular, it shall provide for:*

   a) *formalised procedures of coordination and linking (also as regards information) between the companies belonging to the insurance group and the ultimate parent undertaking for all the areas of business;*
   b) *mechanisms for integrating the accounting systems, also with the aim of ensuring the reliability of data on a consolidated basis;*
   c) *periodical information flows which allow the achievement of strategic objectives and the compliance with regulations to be verified;*
   d) *reporting and accounting procedures which allow the transactions between entities in the insurance group to be checked, quantified, monitored and controlled;*
   e) *procedures which ensure the consistency between the data and information produced for the purposes of supplementary supervision and those produced for the purposes of supervising the insurance group;*
   f) *the definition of tasks and responsibilities of the various units assigned with the control of risks, including the risk management unit within the insurance group, and the mechanisms for coordination;*
   g) *procedures that are appropriate for ensuring, in a centralised fashion, the identification, measuring, management and control of risks at insurance group level.*

4. *In the group risk management system the ultimate parent undertaking shall ensure that the risk management policy at insurance group level is implemented on a consistent and ongoing basis within the whole group, taking account of the risks of each undertaking included within supplementary supervision and of interdependencies, in particular:*
   - *of reputational risks, risks deriving from intra-group transactions, and concentration risks (including contagion risk), at the group level;*
   - *of the interdependencies between risks deriving from the pursuit of insurance business in different undertakings and jurisdictions;*
   - *of the risks deriving from undertakings with head office in third States included within supplementary supervision;*
   - *of the risks deriving from undertakings not subject to sectoral regulations included within supplementary supervision;*

[52] Article replaced by article 24 of IVASS Order n. 17 of 15 April 2014.

- *of the risks deriving from other undertakings subject to specific sectoral regulations included within supplementary supervision;*

5. *Taking account of the provisions of paragraph 4 the ultimate parent undertaking shall evaluate, at least annually, the risks to which the insurance group is exposed, both on a current and on a forward-looking basis. The results of the evaluations, along with the methods used, shall be submitted to the administrative body which, after discussing and approving them, shall disclose them to the senior management and to the structures concerned along with its conclusions. It shall also define a process for the forward looking assessment of risks at insurance group level, comprising those deriving from undertakings included within supplementary supervision, including the risks deriving from undertakings with head office in third States, not subject to sectoral regulations and from other undertakings subject to specific sectoral regulations. Such evaluation shall take account of the interdependencies between risks*[53]*.*

6. *The ultimate parent undertaking shall formalise and disclose to all the insurance group companies the criteria used to identify , measure, manage and control all risks. In addition, it shall validate the control systems and procedures within the insurance group.*

7. *To verify that the insurance group companies behave in a way that complies with the ultimate parent undertaking's guidelines and that the internal control systems are effective, the ultimate parent undertaking shall make sure that periodical inspections are performed inside the insurance group companies, also using the internal audit functions of the latter.*

8. *Methods of evaluation and measuring risks at insurance group level, and assumptions and their outcome shall be adequately documented.*

9. *The ultimate parent undertaking shall promptly informs IVASS of any specific legal provisions, in force in the State where the foreign companies in the insurance group have their head offices, that are an obstacle to the compliance with the provisions of this Chapter.*

Chapter VII – Requirements regarding notification *to IVASS*[54]

Art. 28
(Notifications to *IVASS*)[55]

1. Undertakings shall notify IVASS of the appointment or revocation of the heads of the internal audit, risk management and compliance functions within thirty days of the adoption of the related act. *In case of appointment, undertakings shall communicate that they have checked that the heads of the functions – or, in case functions are outsourced within or outside the insurance group, the internal contact point or person responsible for supervision over outsourced activities – fulfil the good repute, professional qualifications and independence requirements, in line with the relevant corporate policy*[56]*.*

[53] Insurance and reinsurance undertakings shall comply with the provisions stated under thisparagraph by 31 December 2014, pursuant to article 56 (3) of IVASS Order n. 17 of 15 April 2014.
[54] Heading amended by article 25 of IVASS Order n. 17 of 15 April 2014.
[55] Heading amended by article 26 (1, a) of IVASS Order n. 17 of 15 April 2014.
[56] Paragraph amended by article 26 (1, b) of IVASS Order n. 17 of 15 April 2014.

2. Along with the annual financial statements, undertakings shall send *IVASS a report:*[57]

   a) on the system of internal controls, which describes the overall system of internal controls including the main procedures it is made up of, illustrating any initiatives taken or changes made, the internal audits performed, any highlighted faults and the corrective measures adopted.
   This report shall also contain information on the undertaking's organisational structure, referred to under art. 5 (3), particularly with regard to:

   - *the composition and appointment of the administrative body and of the internal committees of the administrative body (appointment procedures, executive and non-executive directors, independent directors and evaluation processes of the requirement of independence, number of positions of each director in other companies, good repute and professional qualifications requirements and specific skills of each director);*
   - *the role of the administrative body and the committees within the administrative body itself (tasks and responsibilities, modalities of work, number of meetings, degree of participation in meetings and activity carried out for the fulfilment of the tasks set out in this regulation, in particular for the definition of strategies and their periodic review);*
   - *the modalities of the self-evaluation process of the administrative body and any corrective measures taken for improvement, also taking into account the level of professionalism of directors with respect to the operations and risk profile of the undertaking;*
   - *the powers granted by the administrative body, with indication of how the delegated powers are controlled (reporting lines);*
   - *the criteria used for the definition of the remuneration policy, with illustration of the information that the administrative body is obliged to provide to the meeting pursuant to art. 24 of ISVAP Regulation n. 39/2011 of 9 June 2011;*
   - *the measures taken to monitor the interests of directors in the company's operations on which they are called upon to decide, the related party transactions and conflicts of interest in general;*
   - *the composition, roles, organisation, responsibility and name of the head of the internal audit, risk management and compliance function, also in case such functions have been outsourced, including information about the policies and procedures established in order to ensure that the heads of such functions and the internal contact point or person responsible for supervision over such activities, in case they are outsourced within or outside the insurance group, meet the professional qualifications and good repute requirements;*
   - *the representation of the structure referred not only to the insurance group but also to all the subjects referred to, as counterparts of intra-group transactions, under art. 5 of ISVAP Regulation n. 25 of 27 May 2008, of the ownership structure and shareholder relations;*
   - *any changes that may have been made to the corporate organisational chart and the system of delegating powers, already communicated to IVASS[58];*

[57] Paragraph amended by article 26 (1, c) of IVASS Order n. 17 of 15 April 2014.

b) on the undertaking's risk management system, illustrating:

- *the strategies, processes and reporting procedures, internal and external, and how it is able to effectively identify, measure, monitor, manage and report, on a continuous basis, the risks on an individual and aggregated level, to which the undertaking is or could be exposed;*
- *how the risk management system, including the risk management function, is implemented and integrated into the decision-making processes of the undertaking and how the undertaking implements the principles underlying the investment policy and the investment risk management system referred to under ISVAP Regulation n. 36 of 31 January 2011*[59]*.*

3. The documentation referred to in paragraph 2 shall be subject to prior evaluation by the administrative body.

Art. 28 bis
(Report by the Ultimate parent undertaking – notification to IVASS)[60]

1. *Along with the financial statements, in its capacity as entity responsible for the group management and coordination activity the ultimate parent undertaking shall send IVASS a report illustrating:*

a) the instructions given to the group companies in the performance of the management and coordination activity;

b) the coordination systems between the corporate bodies and the internal audit, risk management and compliance functions of the group, and between the latter and the relevant bodies and functions of the individual undertakings of the insurance group.

c) the internal control mechanisms and risk management processes adopted in compliance with article 87 of the decree and the relevant implementing provisions regarding internal control and risk management, including the findings of the checks made on the group companies;

d) the measures taken in order to implement IVASS' provisions relating to insurance groups;

e) the outcome of the checks aimed to verify that each insurance group company complies with the measures adopted in accordance with IVASS' provisions.

f) how the systems of internal controls and risk management, and internal and external reporting procedures are consistently implemented in all the group undertakings and how such procedures relate to the information flows from the undertakings included in the area of supplementary supervision.

2. *The report referred to in paragraph 1 shall be subject to prior evaluation by the administrative body.*

[58] Letter integrated by ISVAP Order n. 3020 of 8 November 2012 and subsequently replaced by article 26 (1, d) of IVASS Order n. 17 of 15 April 2014.
[59] Letter replaced by article 26 (1, e) of IVASS Order n. 17 of 15 April 2014.
[60] Article inserted by article 27 of IVASS Order n. 17 of 15 April 2014.

Chapter VIII – Provisions relating to outsourcing

Section I – Conditions for outsourcing

Art. 29
(Outsourcing of activities)

1. Undertakings may enter into outsourcing contracts provided that the nature and quantity of outsourced business and the procedures used for its transfer does not cause the transferring company to lose its original purpose.

2. Under no circumstances, however, can the activity of risk underwriting be outsourced.

3. Under no circumstances does outsourcing exonerate the undertaking's corporate bodies and senior management from their own responsibilities.

Art. 30
(Outsourcing of critical or important activities)

1. When undertakings assign a third party to carry out critical or important activities, they shall ensure that the outsourcing procedures:

   a) do not compromise the quality of the undertaking's governance system;
   b) do not compromise the financial results and stability of the undertaking and the continuity of its activities;
   c) do not compromise the ability of the undertaking to provide policyholders and third parties with a continuous and satisfactory service;
   d) do not create an unjustified increase in operational risks.

Art. 31
(Outsourcing policy and choice of suppliers)

1. The administrative body shall define the policy for outsourcing the undertaking's activities, with a resolution including at least:

   a) the criteria for identifying the activities to be outsourced;

   a bis) the criteria for the classification of activities as critical or important activities, in addition to the provisions of this Regulation[61]*;*

   b) the criteria for selecting suppliers, as regards their professional experience, good repute and financial standing;

   c) the adoption of methods for evaluating the level of supplier services (service level agreements) *and the frequency of such evaluations*[62];

   c bis) the undertaking's contingency plans and the relevant procedures, including exit strategies in cases of outsourcing of critical or important functions and activities[63]*.*

[61] Letter inserted by article 28 (1, a) of IVASS Order n. 17 of 15 April 2014.
[62] Letter supplemented by article 28 (1, b) of IVASS Order n. 17 of 15 April 2014.
[63] Letter inserted by article 28 (1, c) of IVASS Order n. 17 of 15 April 2014.

Art. 32
(Outsourcing agreements)

1. When entering into outsourcing agreements, insurance undertakings shall be careful to ensure in particular that *at least*[64] the following conditions are met:

   a) clear definition of the activity being transferred, the procedures for carrying it out and the related consideration;
   b) that the supplier carries out the outsourced activities in an adequate manner and in compliance with current legislation and the undertaking's instructions;
   c) that the supplier promptly informs the undertaking of any fact that might have a significant effect on its ability to carry out the outsourced activities in compliance with current legislation and in an efficient and effective manner;
   d) that the supplier ensures that the details relating to the undertaking and its insurance customers will remain confidential;
   e) that the undertaking has the right of control and access to the supplier's activity and documentation;
   f) that the supplier ensures IVASS complete and immediate access to its premises and its documentation;
   g) that the undertaking can withdraw from the contract without disproportionate charges or such as to effectively compromise the exercise of the right to withdrawal;
   h) that the undertaking can withdraw from or modify the contract if requested to do so by IVASS;
   i) that the contract cannot be subcontracted out without the approval of the undertaking.

2. Outsourcing agreements shall be formalised in writing.

3. If there are outsourcing agreements relating to the internal audit, risk management and compliance functions, that will be entered into exclusively with a supplier whose head offices are in the EEA, undertakings shall also ensure that the following are adequately defined:

   a) objectives, methods and frequency of controls;
   b) procedures and frequency of relations with the administrative body and senior management;
   c) possibility for re-considering the service conditions if significant changes occur in the operations and organisation of the insurance undertaking.

Art. 33
(Control over outsourced activities)

1. As regards outsourced activities, the system of internal controls shall ensure standard controls similar to those that would have been implemented if the activities had been carried out directly by the undertaking. The risk management policy shall include the specific risks linked to outsourcing.

2. For the purposes of paragraph 1, undertakings shall set up appropriate organisational and contractual safeguards that allow the constant monitoring of the

[64] Paragraph supplemented by article 29 of IVASS Order n. 17 of 15 April 2014.

outsourced activities, their compliance with legal requirements and regulations and the corporate directives and procedures, the respect of the operational limits and risk tolerance thresholds established by the undertaking; they also allow for prompt intervention whenever the supplier does not comply with its commitments or the quality of the service provided is poor.

3. Without prejudice to the limitations referred to in article 29, undertakings shall select within their own organisations one or more persons responsible for supervision over outsourced activities and formalise their duties and responsibilities. The number of persons with such responsibilities shall be proportionate to the nature and quantity of outsourced activities, and, if the internal audit, risk management and compliance functions have been outsourced *within or outside the insurance group*, the persons in question must have adequate *fit and proper requirements set by the policy in accordance with article 5 (2,l)*[65].

4. Undertakings shall set up appropriate measures for ensuring the continuity of the activities, should there be an interruption or severe deterioration in the quality of the service provided by the supplier, which shall include adequate contingency or reinternalisation plans.

5. If the insurance undertaking and the service provider belong to the same insurance group, when the undertaking sets up the contractual and organisational safeguards as stipulated in this Chapter, it may take into account the extent to which it exercises control over the supplier pursuant to article 72 of the decree and the relative provisions for its implementation.

Art. 34
(*IVASS*'[66] intervention powers)

1. *IVASS*[67] shall verify whether the outsourcing of activities and their execution comply with the provisions in this Chapter.

2. When considering the nature, scale and complexity of the risks inherent in the undertaking's business as well as the financial position of the insurance undertaking, the nature of the outsourced activity, the characteristics and market position of the supplier or the quality of the service provided, if *IVASS*[68] is of the opinion that the sound and prudent management of the undertaking or the interests of policyholders and third parties may be compromised, or that the full exercise of the supervisory functions is not allowed, it may order the undertaking to modify the outsourcing agreement or, in the most serious cases, withdraw from the agreement.

3. The outsourcing of business to a supplier resident outside the EEA must be submitted to IVASS for prior approval.

[65] Paragraph amended by article 30 of IVASS Order n. 17 of 15 April 2014.
[66] Heading amended by article 31 (1, a) of IVASS Order n. 17 of 15 April 2014.
[67] Paragraph amended by article 31 (1, b) of IVASS Order n. 17 of 15 April 2014.
[68] Paragraph amended by article 31 (1, c) of IVASS Order n. 17 of 15 April 2014.

Section II – Requirements regarding notification to *IVASS*[69]

Art. 35
(Notification when outsourcing critical or important activities)

1. When outsourcing critical or important activities, undertakings shall notify IVASS in advance, at least forty-five days before the contract enters into force, providing information about the outsourced activity, the supplier, the duration of the outsourcing and the place where the outsourced activity will be carried out, in line with the model shown in annex 2[70].

2. Undertakings shall promptly notify IVASS if, during the period of the contract, significant changes have occurred in relation to the supplier, which have an effect on the service.

3. Undertakings shall notify IVASS of the termination of the outsourcing agreement, and attach a report on the procedures for reinternalising the activity or assigning it to another supplier.

Art. 36
(Notifications in case of outsourcing of the internal auditing, risk management and compliance functions) [71]

1. *In case of outsourcing of the internal auditing, risk management and compliance functions, undertakings shall notify IVASS in advance, at least sixty days before the contract enters into force, enclosing the draft contract and providing any other information allowing to evaluate compliance with the principles of economic viability, efficiency and reliability, as well as the existence of the conditions for IVASS' full exercise of its supervisory and inspection activities. The name of the internal contact point or of the person responsible for supervision over outsourced activities, including the information referred to under article 33 (3) must also be communicated.*

2. *Undertakings shall promptly notify IVASS if, during the period of the contract, significant changes have occurred in relation to the supplier, which have an effect on the service.*

3. *Undertakings shall notify IVASS of the termination of the outsourcing agreement, attaching a report on how they sill reinternalise the activity or outsource it with another supplier; in the latter case the information referred to under paragraph 1 shall be provided.*

Art. 37
(Notifications in case of outsourcing of other activities)

1. When outsourcing activities other than critical or important activities, undertakings shall notify IVASS of the contracts concluded, using the model in annex 3, when they send their financial statement for the year[72].

[69] Heading amended by article 32 of IVASS Order n. 17 of 15 April 2014.
[70] Paragraph amended by article 33 of IVASS Order n. 17 of 15 April 2014.
[71] Article replaced by article 34 of IVASS Order n. 17 of 15 April 2014.

Chapter IX – Transitional and final provisions

Art. 38
(Transitional provisions)

(repealed)[73]

Art. 39
(Repeal of regulations)

1. From the date of entry into force of this regulation,, the following shall be repealed:
   a) ISVAP Circular N. 577/D of 30 December 2005;
   b) ISVAP Circular N. 456 of 6 November 2001, limited to point 2.

Art. 40
(Publication)

1. This Regulation shall be published in the Official Journal of the Italian Republic and in the Authority's Bulletin and website.

Art. 41
(Entry into force)

1. This Regulation shall enter into force on the day following its publication in the Official Journal of the Italian Republic.

2. Undertakings shall be required to comply with the provisions stated under Chapter V, as well as with articles 27 (3), 31, 33 and 35 by 1 January 2009. For the activities already outsourced on the date this Regulation entries into force, the term of compliance with the provisions as referred to in article 32 is fixed on 1 April 2009.

Rome,

The President

[72] Paragraph amended by article 35 of IVASS Order n. 17 of 15 April 2014.
[73] Article repealed by article 36 of IVASS Order n. 17 of 15 April 2014.