



Istituto per la Vigilanza sulle Assicurazioni Private e di Interesse Collettivo

REGULATION N. 20 OF 26 MARCH 2008

(Only the Italian version is authentic)

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

ISVAP

Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo

(Supervisory Authority for Private Insurance Undertakings

and Insurance Undertakings of Public Interest)

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, introducing the Code of Private Insurance;

adopts the following

REGULATION

INDEX

Chapter I - General provisions

- Art. 1. (Legislative sources)
- Art. 2. (Definitions)
- Art. 3. (Scope)

Chapter II - System of internal controls

Section I - General principles

- Art. 4. (Aims of the system of internal controls)

Section II – Role of the undertakings bodies

- Art. 5. (Administrative body)
- Art. 6. (Internal control committee)
- Art. 7. (Senior management)
- Art. 8. (Control body)
- Art. 9. (Formalization of documents)

Section III – Constituents of the system of internal controls

- Art. 10. (Internal control culture)
- Art. 11. (Supervisory activities and separation of tasks)
- Art. 12. (Information flows and channels of communication)

(only the Italian version is authentic)

- Art. 13. (Function for the production of data and information for the purposes of supplementary supervision)
- Art. 14. (IT systems)

Chapter III – Internal Audit

- Art. 15. (Internal audit function)
- Art. 16. (Outsourcing of the Internal audit function)
- Art. 17. (Collaboration between functions and bodies assigned with supervisory duties)

Chapter IV – Risk management

- Art. 18. (Aims of the risk management system)
- Art. 19. (Identification and evaluation of risks)
- Art. 20. (Stress test)
- Art. 21. (Risk management function)

Chapter V – Compliance function

- Art. 22. (Aims of the assessment of compliance)
- Art. 23. (Compliance function)
- Art. 24. (Compliance responsible officer)
- Art. 25. (Outsourcing the Compliance function)

Chapter VI – Provisions relating to insurance groups

- Art. 26. (Role of parent undertaking)
- Art. 27. (Internal control and risk management in the group)

Chapter VII – Requirements regarding notification to ISVAP

- Art. 28. (Notifications to ISVAP)

Chapter VIII – Provisions relating to outsourcing

Section I – Conditions for outsourcing

- Art. 29. (Outsourcing of activities)
- Art. 30. (Outsourcing of critical or important activities)
- Art. 31. (Outsourcing policy and choice of suppliers)
- Art. 32. (Outsourcing contract)
- Art. 33. (Control over outsourced activities)
- Art. 34. (ISVAP's intervention powers)

Section II – Requirements regarding notification to ISVAP

- Art. 35. (Notification when outsourcing critical or important activities)
- Art. 36. (Outsourcing of the Internal audit, Risk management and Compliance functions)
- Art. 37. (Notification when outsourcing other activities)

Chapter IX – Transitional and final provisions

- Art. 38. (Transitional provisions)
- Art. 39. (Repeal of regulations)

(only the Italian version is authentic)

Art. 40. (Publication)

Art. 41. (Entry into force)

List of Annexes

Annex 1	Form for notification of critical or important activities to be outsourced.
Annex 2	List of outsourced activities and services other than critical or important activities and services
Annex 3	List of current outsourcing contracts

(only the Italian version is authentic)

Chapter I – General provisions

Art. 1 (Legislative sources)

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

Art. 2 (Definitions)

1. For the purposes of this Regulation, the following meanings are used:
 - a) “senior management”: the managing director, the director general, as well as the management which carries out management supervision duties
 - b) “critical or important activities”: activities, which, if they were not performed or were 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 its business, or would seriously compromise the undertaking’s financial results and stability or the continuity and quality of its services to the 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) “parent undertaking”: the insurance or reinsurance undertaking or insurance holding company, whose head offices are in Italy, as defined by article 83 of the legislative decree n. 209 of 7 September 2005 and the relative provisions for its implementation;
 - e) “decree”: the legislative decree n. 209 of 7 September 2005, bearing the Code of Private Insurance;
 - f) “outsourcing”: the agreement between an insurance undertaking and a supplier of services, even though not authorised to run an 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 as referred to in article 82 of the legislative decree no. 209 of 7 September 2005 and the relative provisions for its implementation;
 - h) “ISVAP” or “Authority”: Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (the Supervisory Authority for Private Insurance Undertakings and Insurance Undertakings of Public Interest);
 - i) “administrative body”: the board of directors, or the management board in undertakings which have adopted the system pursuant to article 2409 octies of the Italian Civil Code;
 - 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 Italian Civil Code, the board of surveillance or the management control committee;
 - k) “branch”: an office, not having legal personality, which is part of an insurance or reinsurance undertaking and which performs directly, wholly or partially, 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;

(only the Italian version is authentic)

- m) “auditing company: the accounts auditing company as referred to in article 102 of the 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, which is as such equivalent to member state of the European Union;
- o) “Third Country”: a state which is not a member of the European Union or does not belong to the European Economic Area ;
- p) “stress test”: a qualitative or quantitative analysis aimed at assessing the impact on the financial situation of undertakings, of unfavourable trends in risk factors, taken individually or grouped together in a single scenario

**Art. 3
(Scope)**

1. The provisions in these Regulation 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 parent undertakings, but limited to the provisions included in Chapter VI.

Chapter II – System of internal controls

Section I - General principles

**Art. 4
(Aims 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 size and operational characteristics of the undertaking and the nature and intensity of company risks.
2. The internal control system is made up of a series of 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) the efficiency and effectiveness of undertaking processes;
 - b) adequate control of risks;
 - c) the reliability and integrity of accounting and management information;
 - d) the protection of assets;
 - e) the compliance of the undertaking’s activities with current legislation and with the undertaking’s directives and procedures.

(only the Italian version is authentic)

Section II – Role of the undertaking bodies

Art. 5

(Administrative body)

1. The administrative body has the final responsibility over the system of internal controls and must ensure that it is always thorough, functional and effective, also with regard to outsourced activities. The administrative body ensures that the system of risk management allows the most significant risks to be identified, assessed and controlled, including those risks arising from non-compliance with regulations.
2. For the purposes referred to in paragraph 1, and within the scope of its 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 they remain adequate over time;
 - b) ensures that adequate decision-making processes are adopted and formalised and that an appropriate separation of functions is implemented;
 - c) approves the system of delegating powers and responsibilities, making sure that it remains adequate over time, and takes care in avoiding excessive concentration of powers on one person/entity and setting up instruments for assessing the exercise of delegated powers;
 - d) defines the directives relating to the system of internal controls, reviewing them at least once a year and making sure that they remain adequate to the developments in company operations and external conditions;
 - e) defines and, at least once a year, assesses in view of a possible revision the strategies and policies relating to the adoption, assessment and management of the most significant risks in line with the level of the undertaking's asset adequacy; on the basis of the results of the processes to identify and assess risks, it establishes the levels of risk tolerance and reviews them at least once a year;
 - f) defines, whenever the conditions for them are satisfied, the directives and criteria for the circulation and collection of data and information that are 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 thorough nature and promptness of the related information flows;
 - g) 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;
 - h) asks 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 identified by senior management, the internal audit function or personnel, promptly issuing the directives for the adoption of corrective measures;
 - i) identifies particular events or circumstances that require immediate intervention by senior management.

(only the Italian version is authentic)

Art. 6

(Internal control committee)

1. For carrying 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 assists 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 principal company risks.
3. The administrative body defines the committee's composition, tasks and functional procedures. The establishment of an Internal control committee does not relieve the administrative body of its own responsibilities.

Art. 7

(Senior management)

1. Senior management is 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. Senior management:
 - a) defines in detail the organisational set-up of the undertaking, the tasks and responsibilities of the operational units and their relative 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 departments so as to avoid, as far as is possible, the creation of conflicts of interest;
 - b) implements the policies relating to the adoption, assessment 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 risk tolerance;
 - 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;
 - e) implements the instructions given by the administrative body regarding measures to be adopted in order to correct make improvements to faults that have come to light;
 - 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 checks on the adequacy of the organisational, administrative and accounting set-up, as adopted by the undertaking, and to see that it functions in practice.

(only the Italian version is authentic)

2. In order 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 functions.
3. The control body:
 - a) acquires knowledge about the company's organisational set-up at the start of its term of office, and examines the results of the auditing company's work regarding 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 the necessary autonomy, independence and functionality exists; if this function has been outsourced, it assesses the content of the assignment on the basis of the relative contract;
 - d) maintains adequate links with the Internal audit function;
 - e) it sees to the prompt exchange of important data and information with the auditing company so that it can carry out its tasks, also examining the periodic reports provided by the auditing company.
 - f) it 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 course of its period in office, it plans and performs, also in coordination with the auditing company, periodic supervisory inspections aimed at ascertaining whether any shortcomings or faults that have been brought to its attention have been overcome and whether, in comparison with the audit inspection at the beginning of its period in office, there have been any significant changes in the undertaking's activity, which require an adjustment to the organisational set-up and 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.

Art. 9

(Formalization of documents)

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

Section III – Constituents of the system of internal controls

Art. 10

(Internal control culture)

(only the Italian version is authentic)

1. The administrative body promotes a high level of integrity and an internal control culture so as to make all the personnel aware of the importance and usefulness of internal controls.
2. Senior management is responsible for promoting an internal control culture and ensures that staff are made aware of their own role and responsibilities so as to be effectively committed to an involvement in controls, seen as an integral part of their own activity. For this purpose it ensures the formalisation and adequate distribution among the personnel of the power delegation system and procedures system, which govern the assignment of tasks, operational processes and reporting channels.
3. Senior management promotes continuous training and communication initiatives aimed at favouring the effective support of all the personnel for the principles of moral integrity and ethical values.
4. So as to promote operational correctness and respect for integrity and moral values among the whole personnel, as well as to prevent deviant forms of conduct which they might be called to answer for, pursuant to legislative decree n. 231 of 8 June 2001, as well as pursuant to article 325 of the legislative decree n. 209 of 7 September 2005, the undertakings adopt an ethical code which defines rules of behaviour, governs situations of potential conflict of interests and foresees adequate corrective actions, if there is some deviancy from the directives and procedures approved by the management or violation of the current legislation or the ethical code itself.
5. Undertakings avoid, at every level of the company, payment policies and practices which might be an incentive to illegal or deviant activity compared to the ethical and legal standards, or induce inclinations towards risks in contrast with the interests of the company.

Art. 11

(Supervisory activities and separation of tasks)

1. The system of internal controls provides for the carrying out of control activities at all levels of the undertaking, that are in proportion to the size, nature and complexity of the business activities, and which contribute towards ensuring that the company directives are implemented and towards verifying that they are complied with.
2. The control activities referred to in paragraph 1 are formalised and reviewed on a periodic basis and involve the whole personnel. These activities include mechanisms for double signatures, authorisations, checks, and comparisons, control lists and reconciliation of accounts, as well as the limited access to transactions only to the persons assigned to them and the recording and periodical checks of the transactions performed.
3. If the size of the company permits it, undertakings ensure, within the scope of the company's functions, an adequate level of independence of the staff assigned control tasks compared to those with operational duties.

Art. 12

(Information flows and channels of communication)

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 ensures that the administrative body has full knowledge of the most

(only the Italian version is authentic)

important company facts, also through the preparation of an adequate reporting system.

2. The system of internal controls ensures that the information complies with the principles of accuracy, completeness, promptness, consistency, openness 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 in the 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) *openness*: 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 directly relevant to the aims for which they are 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.
4. The system of internal accounting and management data correctly registers the facts of administration and provides a true and correct representation of the financial and economic position of the undertaking and in compliance with the laws and secondary regulations.
5. The undertakings set up and maintain efficient channels of communication 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. 13

(Production of data and information for the purposes of supplementary supervision)

1. The undertakings 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.
2. The undertakings keep the data and information as referred to in paragraph 1 on their own premises, for potential inspections by ISVAP.

(only the Italian version is authentic)

Art. 14
(IT systems)

1. The IT systems must be appropriate in respect of the size and activities of the undertaking 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 approves 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 are separate. Access to the various environments are 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 ensure the logical security of treated data, restricting access to the data to authorised personnel, in particular for the production environment, and stipulate that all violations are highlighted; the procedures are subject to inspections from the Internal audit function;
 - c) the procedures for approving and acquiring hardware and software, as well as for the outsourcing of certain services, are formalised;
 - d) procedures are adopted that ensure the physical safety of hardware, software and data banks also through the use of disaster recovery and backups;
 - e) in order to ensure continuity in the organisation's processes, certain procedures and operational standards are adopted and documented, that are oriented towards the identification and management of events that could jeopardise the continuity of the business, such as for example, unforeseen events, black outs, fires, floods, malfunction of hardware and software components, operational errors by personnel in charge of systems management or by users, involuntary introduction of components that are damaging for the IT and network system, criminal acts aimed at reducing the availability of the information.
3. When there are extraordinary transactions such as mergers or portfolio acquisitions, the undertaking prepares an IT systems integration plan in which the following are specified:
 - a) environments, functions, procedures, applications and data bases involved in the integration process;
 - b) the timescales associated with each integration phase with particular attention to the migration of data bases and to the dates on which the integration of portfolios (premiums, claims etc.) shall be completed;
 - c) the units and organisational centres which will be assigned the controls and monitoring of the entire integration process.

Chapter III – Internal audit

Art. 15
(Internal audit function)

1. Undertakings 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

(only the Italian version is authentic)

needs for improvement, also through advisory and support activities in favour of the other company departments.

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 must not report to any of the operational department heads in the hierarchy; 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) the responsible officer of the function is appointed by the administrative body: he/she must have specific competence and professional experience for carrying out such activities; the tasks assigned to the responsible officer are clearly defined and approved by resolution of the board, which also establishes the responsible officer's powers, responsibilities and procedures for reporting to the administrative body;
 - c) those assigned to the function must be allowed free access to all the company structures and documentation relating to the specific company area under inspection, including information which is useful in checking the adequacy of the controls performed on outsourced company functions;
 - d) the function must have organic links with all the centres in charge of internal control functions; the responsible officer is provided with the necessary authority to guarantee his/her functions' independence;
 - e) the specific structure must be adequate in terms of human and technological resources for the size of the undertaking and the development objectives which it intends to achieve. The staff within the function must have specialist abilities and professional training must be looked after carefully.
3. The Internal audit function aligns its own activities to the professional standards commonly accepted at a national and international level and checks on:
 - a) the management processes and organisational procedures;
 - b) the regularity and functionality of the information flows among the company areas;
 - c) the adequacy of the information systems and their reliability so that the quality of the information, on which the undertaking's senior management bases its own decisions, is not invalidated;
 - d) the compliance of the administrative and accounting processes with standards of correctness and fair accounting;
 - e) the efficiency of the controls performed on outsourced activities.
4. The Internal audit function plans its activities so as to identify the priorities regarding which areas need to be subjected to an audit. The audit plan is submitted for approval to the administrative body and identifies, 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 is carried out if significant changes are made to the approved plans, which nevertheless, are organised in order to address unforeseen needs.
5. Following the analysis of the activities under inspection, the function proceeds, in accordance with the procedures and periodicity established by the administrative body, to

(only the Italian version is authentic)

inform the administrative body itself, senior management and the control body about its assessment of the results and potential dysfunctions and critical situations; it also has the obligation to urgently bring to the attention of the administrative body and the control body any particularly serious situations. The audit reports must be impartial, clear, concise, prompt and must contain suggestions to remove any deficiency; they must be kept at undertaking's head office.

6. The internal audit finishes with the follow-up activities, consisting of future checks on the effectiveness of the corrections made to the system.

Art. 16

(Outsourcing of the Internal audit function)

1. Undertakings, for which the establishment of an Internal audit function is not economically feasible due to their small size and operational characteristics, can outsource this function, also within the sphere of the insurance group, in compliance with the conditions as referred to in Chapter VIII.
2. The activities of the Internal audit 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 person in charge who looks after relations with the group's function responsible officer;
 - b) adequate procedures are adopted to ensure that the activities of the Internal audit function, as defined at insurance group level, are adequately regulated to comply with the operational characteristics of each company.

Art. 17

(Collaboration between functions and bodies assigned with supervisory duties)

1. The control body, the auditing company, the Internal audit, the Risk management and the 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 department 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 defines and formalises the links between the various departments assigned with monitoring tasks.

Chapter IV – Risk Management

Art. 18

(Aims of the Risk management system)

1. In order to maintain the risks, to which they are exposed, at a reasonable level, consistent with each undertaking's available assets, undertakings set up an adequate system of risk management, which is proportionate to their own size, nature and complexity of the business they do, which allows them to identify, assess and control their most significant risks. Significant risks are defined as those whose consequences could compromise the undertaking's solvency or create a serious obstacle to the achievement of the company's objectives.
2. Undertakings make a catalogue of risks in line with the nature and size of the business.

(only the Italian version is authentic)

The catalogue includes 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 reserves that are not sufficient compared to the commitments assumed in favour of those policyholders or those who have suffered damages;
- 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, brokers 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. a risk which occurs, subsequent to the relationships that take place between an undertaking and the other entities in the group: difficult situations can arise in one entity within the same group and 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 company's image and an increase in conflict with insurance customers, due to the poor quality of services offered, the placement of inadequate policies or the behaviour of the sales network.

Art. 19

(Identification and evaluation of risks)

1. Undertakings 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.
2. Using an adequate process of analysis, undertakings must be able to understand the nature of the risks they have identified, their origins, the possibility or need to control them and the effects that could arise, both in terms of losses and opportunities. The process of analysis includes a qualitative assessment and, for quantifiable risks, the adoption of methods to measure the exposure to risk, including, where appropriate, systems for determining the maximum potential loss.
3. When measuring risk and where appropriate, undertakings shall consider the inter-relations between risks, assessing them singularly and on an aggregate basis.

(only the Italian version is authentic)

4. The methods of evaluation and measuring risks and the related results are adequately documented.
5. Policies relating to the assumption, measuring and management of risks are defined and implemented, taking as a reference point the overall view of the balance sheet assets and liabilities, considering that the development in techniques and models of asset-liability management 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.
6. The processes for identifying and evaluating risks are carried out on a continual basis so as to take into account the changes in the nature and size of the business and the market context and also the appearance of new risks or changes in those that exist already. Particular attention is given to evaluating risks that may arise from offering new products or from entering into new markets.
7. Undertakings define the procedures which can promptly highlight the appearance of risks that might damage their financial and economic situation or exceed the established tolerance thresholds. The undertaking prepares adequate emergency plans in respect of the major risk sources it has identified.

Art. 20

(Stress test)

1. With regard to the sources of risk that the undertakings have identified as being particularly significant, on the basis of the processes referred to in article 19, the undertakings themselves carry out some prospective analyses using the *stress test*.
2. Stress tests, based on determined and random 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.
3. The results of the stress test, together with the underlying hypotheses, are brought to the attention of the administrative body so as to make a contribution towards the review and improvements to the policies on risk management, and the operational guidelines and exposure limits established by the administrative body itself.
4. If the results of the stress tests indicate a particular vulnerability towards a given series of circumstances, the undertakings adopt appropriate measures for adequately managing the relative risks.
5. When requested to do so by ISVAP, undertakings carry out standardised stress tests on the basis of risk factors and parameters established by ISVAP itself.

Art. 21

(Risk management function)

1. Undertakings set up a risk management function, appropriate to the nature, size and complexity of the business, which:
 - a) contributes towards the definition of methods of measuring risks;
 - b) contributes towards the definition of operational limits assigned to the operational

(only the Italian version is authentic)

- structures and defines the procedures for promptly checking the same 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) 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;
 - e) checks the adequacy of the risk measuring models with the operations carried out by the undertaking.
 - f) contributes towards the administration of the stress tests referred to in article 20.
2. The organisational position of the risk management function is left to the autonomy of the undertakings, but in accordance with the principle of separation between operational and supervisory departments. The undertakings assess whether to use internal staff or to use external structures in compliance with the criteria laid down in Chapter VIII.
 3. 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 person in charge who looks after relations with the group's function responsible officer;
 - b) adequate procedures are adopted to ensure that the activities of the Risk management function, as defined at insurance group level, are adequately regulated to comply with the risk profile of each company.
 4. The Risk management function reports to the administrative body, even when it is not constituted in a specific organisational form. The organisational position of the Risk management function must be such as not to be dependent on the operational departments.
 5. The links between the Internal audit function and the Risk management function are defined and formalised by the administrative body.

Chapter V – Compliance function

Art. 22

(Aims of the assessment of compliance with regulations)

1. Within the sphere of the system of internal controls, undertakings set up, at every pertinent level of the company, specific centres 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 with 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 standards, undertakings pay particular attention to the compliance with standards relating to openness and correctness in behaviour towards insurance customers and claimants, pre-contractual and contractual information, the correct fulfilment of contracts, with particular reference to the management of claims and, more in general, consumer protection.

(only the Italian version is authentic)

Art. 23
(Compliance function)

1. Undertakings set up a Compliance function, proportionate to the nature, size and complexity of their business, which is 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 is formalised in a specific resolution passed by the administrative body, which defines its responsibilities, tasks, operational procedures and the nature and frequency of reporting to the company 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 standards and proposes organisational and procedural changes aimed at ensuring adequate control over the risk;
 - c) assesses the effectiveness of the organisational improvements following the changes it has proposed;
 - d) prepares adequate information flows to the undertaking's company bodies and the other structures involved.
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. 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.
6. In any case, the separation of the Compliance function from the operational departments and other supervisory departments, is guaranteed by expressly defining their respective roles and scope of activities.
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 is nevertheless separated from the Internal audit functions and is periodically subjected to an audit by it.

Art. 24
(Compliance responsible officer)

1. Irrespective of the organisational form chosen pursuant to article 23 (5), undertakings appoint a person in charge of the Compliance function, who has adequate professional experience and skills, independence and authoritative. The manager is appointed and removed by the administrative body.

(only the Italian version is authentic)

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. A director may be appointed as responsible officer, as long as he has no delegations of power and the size and operational characteristics justify it
3. 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.

Art. 25

(Outsourcing the Compliance function)

1. Undertakings, for which the establishment of a specific Compliance function is not economically feasible due to their small size and operational characteristics, can outsource this 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 person in charge who looks after relations with the group's function responsible officer;
 - 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 adequately regulated to comply with the operational characteristics of each company.

Chapter VI – Provisions relating to insurance groups

Art. 26

(Role of parent undertaking)

1. Within the scope of its activities of corporate governance of the insurance group, the parent undertaking exercises:
 - 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 centres 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 controlled undertaking brings to the insurance group.

Art. 27

(Internal control and risk management in the insurance group)

1. On the understanding that each insurance and reinsurance undertaking whose head offices are in Italy and that belongs to an insurance group, sets up its own system of control and management of risks in accordance with the provisions included in Chapters III, IV and V, the parent undertaking sets up a system of internal controls for the insurance group, which is adequate for carrying out effective control over the group's overall

(only the Italian version is authentic)

strategic choices and the management balance of each individual component.

2. In particular, it provides for:

- a) formalised procedures of coordination and linking (also as regards information) between the companies belonging to the insurance group and the parent undertaking for all the areas of business;
- b) mechanisms for integrating the accounting systems, also with the aim of ensuring the reliability of the registered items on a consolidated basis;
- c) periodical information flows which allow the achievement of strategic objectives and the compliance with regulations to be verified;
- d) highlighting 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 within the insurance group and the mechanisms for coordination;
- g) procedures that are appropriate for ensuring, in a centralised form, the identification, measuring, management and control of risks at insurance group level.

3. The parent undertaking formalises and informs all the companies in the insurance group about the criteria used to identify measure, manage and control all risks. In addition, it validates the control systems and procedures within the insurance group.

4. In order to verify that the companies belonging to the insurance group behave in a way that complies with the parent undertaking's guidelines and that the internal control systems are effective, the parent undertaking makes sure that periodical inspections are performed inside the companies that make up the insurance group, also using the Internal audit functions of the companies themselves.

5. The parent undertaking promptly informs ISVAP of any specific legal provisions, which are in force in the countries where the foreign companies in the insurance group have their head offices, and that are an obstacle to the compliance with the provisions of this Chapter.

Chapter VII – Requirements regarding notification to ISVAP

Art. 28

(Notifications to ISVAP)

1. Undertakings shall notify ISVAP of the appointment or revocation of the responsible officers of Internal audit, Risk management and Compliance functions within thirty days of the adoption of the related act.
2. Together with the annual financial statements, undertakings shall send ISVAP the following documentation:
 - a) a report on the system of internal controls and risk management, which illustrates any initiatives taken or changes made during the year, the internal audits performed, any highlighted faults and the corrective measures adopted;

(only the Italian version is authentic)

- b) any changes that may have been made to the company's organisational chart and the system of delegating powers, which was previously sent to ISVAP;
 - c) a report on any changes made in terms of resources or organisation as regards the Internal audit, Risk management and Compliance functions.
3. The documentation referred to in paragraph 2 is subject to prior evaluation by the administrative body.

Chapter VIII – Provisions relating to outsourcing

Section I – Conditions for outsourcing

Art. 29 (Outsourcing activities)

1. Undertakings may enter into outsourcing contracts provided that the nature and quantity of outsourced activities and the procedures used for their transfer does not cause the transferring company to lose all its activities.
2. Under no circumstances, however, can the activity of risk underwriting be outsourced.
3. Under no circumstances does outsourcing exonerate the company bodies and the senior management of the undertaking 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 its insurance customers and claimants 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 defines the policy for outsourcing the undertaking's activities, with a resolution which includes at least:
 - a) the criteria for identifying the activities to be outsourced;
 - b) the criteria for selecting the 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 agreement).

(only the Italian version is authentic)

Art. 32
(Outsourcing contract)

1. When entering into outsourcing contracts, insurance undertakings shall be careful to ensure in particular that the following conditions are complied with:
 - a) clear definition of the activity being transferred, the procedures for carrying it out and the related fee;
 - 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 ISVAP 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 ISVAP;
 - i) that the contract cannot be subcontracted out without the approval of the undertaking.
2. Outsourcing agreements are formalised in writing.
3. If there are outsourcing agreements relating to 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 for reporting to 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 ensures 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 includes the specific risks linked to outsourcing.
2. As regards the contents of paragraph 1, undertakings set up appropriate organisational and contractual safeguards that allow the constant monitoring of the outsourced activities, their compliance with legal requirements and regulations and the company directives and procedures, their respect of the operational limits and the 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

(only the Italian version is authentic)

deficient.

3. On the understanding that the limitations referred to in article 29 still apply, undertakings select one or more persons within their own organisations to be in charge of control activities over the 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, the persons in question must have adequate authoritative and independent qualities.
4. Undertakings 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 emergency plans and possibility of reintegrating the activities within the undertaking.
5. If the insurance undertaking and the service provider belong to the same insurance group, when it sets up the contractual and organisational safeguards as stipulated in this Chapter, the undertaking 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

(ISVAP's intervention powers)

1. ISVAP verifies whether the outsourcing of activities and their execution comply with the provisions in this Chapter.
2. When considering the size and 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 ISVAP is of the opinion that the sound and prudent management of the undertaking or the interests of the insurance customers or claimants may be compromised, or that it is not allowed to fully exercise its supervisory functions, it may order the undertaking to modify the outsourcing agreement or, in the most serious cases, withdraw from the agreement.
3. The outsourcing of activities to a supplier resident outside the EEA must be submitted to ISVAP for prior approval.

Section II – Requirements regarding notification to ISVAP

Art. 35

(Notification when outsourcing critical or important activities)

1. When outsourcing critical or important activities, undertakings shall notify ISVAP 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 1.
2. Undertakings promptly notify ISVAP, 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 notify ISVAP of the termination of the outsourcing agreement, attaching a report on the procedures for re-integrating the activity or assigning it to another supplier.

(only the Italian version is authentic)

Art. 36

(Outsourcing of the Internal audit, Risk management and Compliance functions)

1. When outsourcing the Internal audit, Risk management and Compliance functions, undertakings shall notify ISVAP in advance, attaching a draft of the contract.
2. The contract can come into force sixty days after ISVAP has received the draft version of the contract and any other information which allows it to evaluate the compliance with the principles of economic viability, efficiency and reliability, as well as the existence of the conditions for ISVAP's full exercise of its supervisory and inspective activities.

Art. 37

(Notification when outsourcing other activities)

1. When outsourcing activities other than critical and important activities, undertakings notify ISVAP of the signed contracts, using the form in Annex 2, when they send their financial statement for the year.

Chapter IX – Transitional and final provisions

Art. 38

(Transitional provisions)

1. Within one hundred and twenty days of these Regulations coming into force, the undertakings send ISVAP a summary table of the outsourcing contracts in force, in accordance with the form in Annex 3.

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 06 November 2001, limited to point 2.

Art. 40

(Publication)

1. This Regulation shall be published in the Official Journal of the Republic of Italy and in ISVAP'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 Republic of Italy.
2. The undertakings shall comply with the provisions contained in Chapter V, as well as articles 27 (3), 31, 33 and 35 by 1 January 2009. For the activities already outsourced on the date this Regulation enters into force, the term of compliance with the provisions as referred to in article 32 is fixed on 1 April 2009.

The President
(Giancarlo Giannini)