RISK MANAGEMENT AND INTERNAL CONTROLS STANDARDS FOR INSURANCE COMPANIES

Table of Contents

INTRODUCTION

1. These Standards form part of the Risk Management and Internal Controls Regulation for Insurance Companies (Circular No. 25/2022 dated 30 December 2022). All Companies must comply with these Standards which expand on the Regulation. These Standards are mandatory and enforceable in the same manner as the Regulation.

2. A Company's Board is in ultimate control of the Company and therefore responsible for ensuring that a comprehensive approach to the systems of Risk Management and Internal Controls is implemented. There is no one-size-fits-all or single best solution. Accordingly, each Company could meet the minimum requirements of the Regulation and Standards in a different way and thus may adopt an organisational framework appropriate to the Risk Profile, nature, size and complexity of its business and structure. The onus is on the Board to demonstrate that it has implemented a comprehensive approach to systems of Risk Management and Internal Controls. Companies are encouraged to adopt leading practices that exceed the minimum requirements of the Regulation and Standards.

3. The Standards follow the structure of the Regulation, with each article corresponding to the specific article in the Regulation.

Article (1): DEFINITIONS

1.	**Affiliate:**	An entity that, directly or indirectly, is controlled by, or is under common control with another entity. The term control as used herein shall mean the holding, directly or indirectly, of voting rights in another entity, or of the power to direct or cause the direction of the management of another entity.
2.	**Authorized Manager:**	The person appointed by the foreign insurance company to manage its branch in the State.
3.	**Board**:	The Company's board of directors.
4.	**Central Bank**:	The Central Bank of the United Arab Emirates.
5.	**Chief Executive Officer:**	The most senior executive appointed by the Board, and in the case of foreign branches, this refers the Authorized Manager.
6.	**Central Bank Laws:**	Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities, as amended and Federal Law No. (6) of 2007 Concerning the Organization of Insurance Operations, as amended and its Executive Regulations.
7.	**Company:**	The insurance company incorporated in the State, or a foreign branch of an insurance Company, that is licensed to underwrite primary insurance and reinsurance, including Takaful insurance companies.
8.	**Conflict of Interest:**	A situation of actual or perceived conflict between the duty and private interests of a person, which could improperly influence the performance of his/her duties and responsibilities.

9.	**Confidential Data:**	Account or other data relating to a Company customer, who is or can be identified, either from the Confidential Data, or from the Confidential Data in conjunction with other information that is in, or is likely to come into, the possession of a person or organization that is granted access to the Confidential Data.
10.	**Control Function:**	Function (whether in the form of a person, unit or department) that has a responsibility in a Company to provide objective assessment, reporting and/or assurance; this includes the risk management, compliance, actuarial, internal audit and where applicable Shari'ah control and Shari'ah audit functions.
11.	**Controlling Shareholder:**	A shareholder who has the ability to directly or indirectly influence or control the appointment of the majority of the Board, or the decisions made by the Board or by the general assembly of the Company, through the ownership of a percentage of the shares or stocks or under an agreement or other arrangement providing for such influence.
12.	**Enterprise Risk Management (ERM):**	The strategies, policies and processes of identifying, assessing, measuring, monitoring, controlling, reporting and mitigating risks in respect of the Company's enterprise as a whole.
13.	**Financial Regulations:**	Insurance Authority Board of Directors' Decision No. (25) of 2014 Pertinent to Financial Regulations for Insurance Companies and the Insurance Authority Board of Directors' Decision No. (26) of 2014 Pertinent to Financial Regulations for Takaful Insurance Companies.
14.	**Group:**	A group of entities which includes an entity (the 'first entity') and: a. any Parent of the first entity; b. any Subsidiary of the first entity or of any Parent of the first entity; c. any Affiliate.
15.	**Internal Controls:**	A set of processes, polices and activities governing a Company's organisational and operational structure, including reporting and control functions.
16.	**Insurance Related Professions:**	Any person licensed to practice any of the activates of an insurance agent, actuary, insurance broker, surveyor and loss adjuster, insurance consultant or any other insurance-related profession that the Central Bank decides to regulate.
17.	**Model:**	A quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.

18. **Outsourcing:** An arrangement between a Company and a service provider, whether the service provider operates within or outside the UAE, for the latter to perform a process, service or activity which would otherwise be performed by the Company itself.

19. **Own Risk and Solvency Assessment (ORSA):** an internal process undertaken by a Company/ Group to assess the adequacy of its Risk Management and current and prospective solvency positions under normal and severe stress scenarios. It requires a Company to analyze all reasonably foreseeable and relevant material risks. It covers current and future risks and requires Company-specific judgment about risk management and the adequacy of their capital position that could have an impact on it's ability to meet both its business objectives as well as its policyholder obligations. This encourages management to anticipate potential business challenges, capital needs and to take proactive steps to reduce risks. ORSA is not a one-off exercise; it is a continuously evolving process and must be a component of a Company's Enterprise Risk Management (ERM) framework. Whilst there is not one specific way of conducting an ORSA, the output is expected to be a set of documents that demonstrate the results of management's proactive approach to its own self-assessment.

20. **Parent:** An entity (the 'first entity') which:

    a. holds a majority of the voting rights in another entity (the 'second entity');

    b. is a shareholder of the second entity and has the right to appoint or remove a majority of the Board of directors or managers of the second entity; or

    c. is a shareholder of the second entity and controls alone, pursuant to an agreement with other shareholders, a majority of the voting rights in the second entity; or

    d. if the second entity is a Subsidiary of another entity which is itself a Subsidiary of the first entity.

21. **Regulations:** Any resolution, regulation, circular, rule, standard or notice issued by the Central Bank.

22. **Risk Appetite:** The aggregate level and types of risk a Company is willing to assume, within its risk capacity, to achieve its strategic objectives and business plan.

23. **Risk Culture:** The set of norms, values, attitudes and behaviors of a Company that characterizes the way in which it conducts its activities related to risk awareness, risk taking and risk management and controls.

24. **Risk Governance System:** As part of the overall approach to Corporate Governance, the framework through which the Board and Senior Management establish

and make decisions about the Company's strategy and risk approach; articulate and monitor adherence to the Risk Appetite and Risks Limits relative to the Company's strategy; and identify, measure, manage, and control risks.

25. **Risk Limits:** Quantitative measure based on a Company's Risk Appetite which gives clear guidance on the level of risk to which the Company is prepared to be exposed and is set and applied in aggregate or individual units such as risk categories or business lines.

26. **Risk Profile:** Point in time assessment of the Company's gross and, as appropriate, net risk exposures aggregated within and across each relevant risk category based on forward looking assumptions.

27. **Risk Management:** The process through which risks are managed allowing all risks of a Company to be identified, assessed, monitored, mitigated (as needed) and reported on a timely and comprehensive basis.

28. **Senior Management:** The individuals or body responsible for managing the Company on a day-to-day basis in accordance with strategies, policies and procedures set out by the Board, generally including, but not limited to, the Chief Executive Officer, chief financial officer, chief risk officer, and heads of the compliance and internal audit functions.

29. **Staff:** All the persons working for a Company including the members of Senior Management, except for the members of its Board.

30. **State:** The United Arab Emirates.

31. **Stress Testing:** A method of assessment that measures the financial impact of stressing one or more factors which could severely affect the Company.

32. **Subsidiary:** An entity (the 'first entity') is a Subsidiary of another entity (the 'second entity') if the second entity:

    a. holds a majority of the voting rights in the first entity

    b. is a shareholder of the first entity and has the right to appoint or remove a majority of the Board of directors or managers of the first entity; or

    c. is a shareholder of the first entity and controls alone, pursuant to an agreement with other shareholders, a majority of the voting rights in the first entity; or

    d. if the first entity is a Subsidiary of another entity which is itself a Subsidiary of the second entity.

33. **Takaful Insurance:** A collective contractual arrangement aiming at achieving cooperation among a group of participants against certain risks whereby each

participant pays certain contribution fees to form an account called the participants' account through which entitled compensations are paid to the member in respect of whom the risk has realized. The Takaful Insurance Company shall manage this account and invest the funds collected therein against certain remuneration.

2. SYSTEMS OF RISK MANAGEMENT AND INTERNAL CONTROLS

1. A Company must establish, implement and maintain systems of Risk Management and Internal Controls that enable it to identify, assess, measure, monitor, control, mitigate and report on risk. Systems of Risk Management and Internal Controls will vary with the specific circumstances of the Company, particularly the Risk Profile, nature, scale and complexity of its business and structure.

2. The Board is responsible for the implementation of an effective Risk Culture and Internal Controls across the Company and its Subsidiaries, Affiliates and international branches, where applicable. The Board approved systems of Risk Management and Internal Controls must incorporate a "three lines of defense" approach which includes the business lines being the first line, Control Functions of Risk Management, compliance and actuarial, being the second line and an independent and effective internal audit function as the third line.

   a. Business line management – must take the responsibility of identification and control of risks. The business line management must :
      1. Manage and identify risks arising from the activities of the business line;

      2. Ensure that activities are within the Company's Risk Appetite, Risk Management policies and limits;

      3. Design, implement and maintain effective system of Internal Controls; and

      4. Monitor and report on business line risks.

   b. Risk Management, actuarial and compliance functions- must take responsibility for setting standards and challenging business lines. The following must be adhered to:
      1. The Risk Management function must establish Company-wide, or if applicable, Group-wide risk and control strategies and policies, provide oversight and independent challenge of business lines' accountabilities, develop and communicate risk and control procedures, and monitor and report on compliance with Risk Appetite, policies and Risk Limits.

      2. The Compliance function must assess Company-wide adherence to requirements, develop and communicate compliance policies and procedures, measure, monitor and report on compliance with Central Bank laws and other relevant laws, corporate governance and Internal Controls rules, Regulations and policies to which the Company is subject.

      3. The actuarial function must provide advice on technical provisions, premium and pricing activities, capital adequacy, reinsurance and compliance with related statutory and regulatory requirements, at a minimum.

c. Internal audit function has the duty of providing independent assurance. The function is responsible to the following matters, at a minimum:
    1. Independently assess the effectiveness and efficiency of the Internal Controls, Risk Management and governance systems and processes.

    2. Independently assess the effectiveness of business line management in fulfilling their mandates and managing risks.

3. The Risk Management and Internal Controls systems must be comprised of the following at a minimum:
    a. Strategies setting out the approach of the Company to dealing with specific areas of risk and regulatory obligations in accordance with the Company's nature, Risk Profile, scale and complexity.

    b. Policies defining the procedures and other requirements that members of the Board and Staff need to follow in order to ensure consistency in approach.

    c. Process for the implementation of the Company's strategies and policies in order to ensure completeness in approach.

    d. Controls to ensure that strategies, policies and processes are in fact in place, are being observed and are attaining their intended objectives in order to ensure adequacy and appropriateness in approach.

3. EFFECTIVE RISK MANAGEMENT SYSTEM

1. The Risk Management system must address the following:

a. Identification:

1. All reasonably foreseeable and relevant material risks are taken into consideration.

2. New activities and products must be subject to risk review and must be approved by the Board, including strategic affairs, such as corporate strategy, mergers, acquisitions, major projects and investments.

b. Assessment:

1. Qualitative and quantitative assessments of all reasonably foreseeable and relevant material risks and risk interdependencies for risk and capital management.

2. Quantification of risk and risk interdependencies using appropriate tools under a sufficiently wide range of techniques for risk and capital management.

3. As necessary, include the results of Stress Testing to assess the resilience of the Company's total balance sheet against severe but plausible stresses including considerations of macroeconomic stresses.

c. Monitoring:

Early warning indicators that enable the appropriate response to all identified material risks. This shall reflect the relationship between the Company's Risk Appetite, Risk Limits, regulatory capital requirements, economic capital and the processes and methods for monitoring risk. A Company must have its own view on how much capital it needs over and above the regulatory capital to fulfill its wider economic needs and manage risks.

d. Mitigation:

1. Strategies and tools are in place to mitigate material risks.

2. The Company must reduce or control material risks to within Risk Appetite and Risk Limits, or transfer to/share with a third party.

3. If a Company cannot mitigate or control the risk, then it must cease or change the activity.

e. Reporting:

1. Risks and assessments must be reported to the Board using qualitative and quantitative indicators, including ORSA along with effective action plans, at least annually.

2. The Board is ultimately responsible for risk oversight. The Risk Management policy covers the frequency of reporting. Any deviation from Risk Appetite is subject to Board review and approval.

f. Risk Management policies:

1. Must enable Staff to understand their risk responsibilities.

2. Must explain the relationship between the Risk Management system and how it addresses risks according to the insurer's Risk Appetite and Risk Limits, and the overall corporate governance framework.

3. Must outline how relevant material risks are managed.

4. On-going communication and training on risk policies must be conducted.

2. Groups must adopt a strong and consistent Risk Management and compliance culture across the Group and at the entity levels. Coordination between the Group and the Company is required to ensure the overall effectiveness of Risk Management and Internal Controls.

3. The Risk Appetite statement is a written articulation of the aggregate level and types of risk that a Company is willing to accept or avoid in order to achieve its business objectives. At a minimum, it must include the following:

a. For each material risk, the maximum level of risk that the Company is willing to operate within, expressed as a limit in terms of:

1. Quantitative measures expressed relative to earnings, capital, liquidity and other relevant measures as appropriate.

2. Qualitative statements or limits, as appropriate, particularly for reputation, compliance and legal risks.

b. Delineation of any categories of risk that the Company is not prepared to assume.

c. The process for ensuring that the Risk Limits are set at an appropriate level for each risk, considering both the probability of loss and the magnitude of loss in the event that each material risk is realised.

d. The process for monitoring compliance with each Risk Limit and for taking appropriate action in the event that they are breached.

e. The timing and process for review of the Risk Appetite and Risk Limits.

f. Quantitative Risk Limits and metrics must include, but not be limited to:

1. Capital targets beyond regulatory requirements, such as economic capital or capital-at-risk;

2. Various liquidity ratios and survival horizons;

3. Earnings volatility;

4. Value at risk;

5. Risk concentrations by internal or external rating;

6. Expected loss, expense, commission and/or combined ratios;

7. Economic value added; and

8. Stressed targets of capital, liquidity and earnings.

9. Underwriting risk, including growth and renewal rates of business, risk retention, balance between lines of business, premium rate adequacy versus technical rates, and claim settlement.

10. Credit risk, including credit quality of reinsurers, credit quality of investment assets and receivable delay management.

11. Investment risk, including asset allocations to achieve adequate diversification and target investment returns. This must be linked to the asset-liability management (ALM) policy and investment policy which specifies the nature, role and extent of ALM activities and their relationship with product development, pricing and investment management.

12. Operational risk, including consideration of risks arising from people, systems, processes as well as cyber security.

4. The Risk Management system must include risk policies that cover at least the following areas:

    a. Credit risk;

    b. Balance sheet and market risk (including investment, asset-liability management, liquidity and derivatives risks);

    c. Reserving risk;

    d. Insurance risk (including underwriting, product design, pricing and claims settlement risks);

    e. Reinsurance risk;

    f. Operational risk (including business continuity, outsourcing, fraud, technology, legal and project management risks);

    g. Concentration risk; and

    h. Group risk.

4. EFFECTIVE SYSTEM OF INTERNAL CONTROLS

1. The Board or the Board audit committee must review, at least annually, the effectiveness of the Company's Internal Controls system and processes, by means of:

    a. Periodic discussions with Senior Management about the effectiveness of the Internal Controls system.

    b. A timely review of evaluations of Internal Controls conducted by Senior Management, internal auditors, the Risk Management function and external auditors.

    c. Periodic follow up to ensure that Senior Management has promptly complied with the recommendations and concerns on control weaknesses expressed by Risk Management, internal auditors and external auditors and the Central Bank.

    d. A periodic review of the appropriateness of the internal controls, commensurate to the Company's strategy and Risk Limits.

2. The Company's Internal Controls system must, at a minimum, address:

    a. Organisational structure: definitions of duties and responsibilities including clear delegations of authority, such as decision-making policies and processes and procedures, separation of critical functions, including, but not limited to, Risk Management, actuarial, accounting, audit and compliance.

b. Accounting and financial reporting policies and processes.

c. Checks and balances (or "four eyes" principle): segregation of duties, cross checking, dual control of assets and double signatures.

d. Safeguarding assets and investment: physical control and computer access, measures of prevention and early detection and reporting of misuse, such as fraud, embezzlement, unauthorised trading and computer intrusion.

5. CONTROL FUNCTIONS

1. The authority and responsibilities of each control function must be set out in writing and made part of the Company's governance documentation.

2. Staff who perform Control Functions must be suitable for their role and meet any applicable professional qualifications and standards. Higher expectations must be placed on the head of each control function.

3. The head of each control functions must regularly review the adequacy of the function's resources and request adjustments from Senior Management/ Board as necessary.

4. Each control function must have the authority to communicate on its own initiative with any employee and to have unrestricted access to information in any business unit that it needs to carry out its responsibilities. The control functions must have the right to conduct investigations of possible breaches and to request assistance from specialists from within or outside of the Company.

6. RISK MANAGEMENT FUNCTION

1. The Risk Management function must have responsibility for the following, at a minimum:

   a. Providing risk analysis and performance risk reviews to the Board and Senior Management;

   b. Identifying individual and aggregated risks (actual, emerging and potential) that the Company faces;

   c. Identifying, assessing, monitoring, mitigating, controlling and reporting risks, including the Company's capacity to absorb risk with due regard to the nature, probability, duration, correlation and potential severity of risks;

   d. Gaining and maintain an aggregated view of the Risk Profile of the Company on an entity and/or Group-wide basis;

e. Assessing the impact of the compensation arrangements and incentives;

f. Evaluating the internal and external risk environment on an on-going basis in order to identify and assess potential risks as early as possible. This may include looking at risks from different perspectives, such as by geographic region or by line of business;

g. Establishing a process for conducting forward-looking assessments of the Risk Profile on a regular basis;

h. Providing periodical reports to the Board, Senior Management and other Control Functions on the Risk Profiles, risk exposures and the necessary mitigation actions; and

i. Reporting material changes affecting the Risk Management system to the Board along with recommendations to improve the system.

2. The CRO, or equivalent, must:

   a. Not have a decision-making role in the Company's risk-taking functions, including underwriting or other equivalent function.

   b. Have no revenue-generating responsibilities.

   c. Have no compensation based on the performance of any of the Company's risk-taking functions.

   d. Not be the Chief Executive Officer of the Company, or the head of underwriting or reinsurance, or the head of the compliance or internal audit functions.

   e. Have a direct reporting line to the Board and/or risk committee and appropriate reporting lines to Senior Management.

   f. Have unfettered access directly to the Board's risk committee, including the ability to meet without other Senior Management present.

3. The Board must ensure that the Risk Management function is properly staffed, resourced and carries out its responsibilities independently and effectively. This includes unrestrained access to all information needed for the Risk Management function to fulfill its duties.

7. RISK MEASUREMENT AND THE USE OF MODELS

1. A Company must use measurement methodologies commensurate with the Risk Profile, nature, size and complexity of the business and the structure of the Company, including, but not limited to, scenario analysis and Stress Testing. Common metrics must be employed on a Company (or Group)-wide basis to foster a Company (or Group)-wide approach and effective identification and monitoring of risks across the Company (or Group).

2. Risk measurement and modelling techniques must be used in addition to qualitative risk analysis and monitoring. The comprehensive approach to risk management must include policies and procedures for the development and internal approval for the use of Models or other risk measurement methodologies. Where the Models, or data for the Models, are supplied by a third party, there must be a process for the validation of the Model and data relative to the specific circumstances of the Company.

3. A Company must perform regular validation and testing of Models. This must include evaluation of the conceptual soundness, ongoing monitoring including process verification and benchmarking and outcomes analysis, including back-testing. Stress Testing and scenario analysis must be used to take into account the risk of Model error and uncertainties associated with valuations and concentration risks.

4. Model-based approaches must be supplemented by other measures. These include qualitative assessment of the logic, judgement and types of information used in Models, as well as assessment of policies, procedures, Risk Limits and exposures, especially with respect to difficult to quantify risks such as operational, compliance and reputational.

8. STRESS TESTING OF MATERIAL RISKS

1. A Company must have a forward looking Stress Testing programme that addresses *inter alia*, underwriting, reserving, asset-liability management, investments, liquidity, reinsurance, concentration of risk, operational risk, risk-mitigation techniques and conduct of business , taking into account, that based on the Risk Profile of the Company, capital may be required in excess of the minimum capital requirements. The Stress Testing programme must also include any risks that are material for the Company given the nature of the business. These may include, but are not limited to, Credit risk, balance sheet and market risks, reserving; pricing, claims, reinsurance, operational, concentration and Group risks.

2. A Company's Stress-Testing programme must be undertaken on a regular basis to facilitate the tracking of trends over time and developments in key risk factors and exposure amounts, in addition to ad hoc Stress Tests, when needed. The programme must cover at a minimum a range of scenarios based on reasonable and plausible assumptions regarding dependencies and correlations. Senior Management and, as applicable, the Board or Board risk committee must review and approve the scenarios.

3. Stress Test programme results must be periodically reviewed by the Board or the Board risk committee. Results must be incorporated into reviews of the Risk Appetite, capital and liquidity planning processes. The Risk management function is responsible for recommending any action required, for example adjustments of Risk Limits or contingency arrangements, based on Stress Test results. The results of Stress Tests and scenario analysis must be communicated to the relevant business line management and functional heads within the Company to assist them in understanding and mitigating the risks inherent in their activities. Stress test programme results must factor into the Company's contingency planning, particularly liquidity Risk Management and contingency funding.

9. COMPLIANCE FUNCTION

1. Compliance Staff must have a sound understanding of the Central Bank laws and other relevant laws, Regulations, rules and standards, relevant to the Company's business and keep abreast with their development and any amendments thereof. The professional skills of compliance Staff must be maintained through regular and systematic education and training, including courses on real cases relating to money laundering, financing of terrorism and proliferation financing.

2. The compliance function must have access to any member of Staff and all records and data of the Company, and if applicable, the Company's Affiliates and Subsidiaries, which are required to comply with the Central Bank's requirements.

3. A consistent approach to compliance across the Group may be achieved through the establishment of a Group compliance function accountable to the Board of the Controlling Shareholder, or through compliance functions established in each entity (or branch) and accountable to those entities' Boards and also reporting to the Group's head of compliance.

4. The compliance function must be assigned responsibility for the following, at a minimum:

    a. Establishing a compliance policy and a compliance plan. The compliance policy must define the responsibilities, competencies and reporting duties of the compliance function. The compliance plan must set out the planned activities of the compliance function which take into account all relevant areas of the activities of the Company and exposure to compliance risk.

    b. Assessing the adequacy of the measures adopted by the Company to prevent non-compliance with Central Bank Laws and Regulations.

    c. Maintaining a corporate culture that is based on responsible conduct and compliance with internal and external obligations.

    d. Identifying, assessing, monitoring, mitigating, reporting on, and addressing regulatory obligations and the risks associated therewith.

    e. Conducting on-going training on regulatory obligations for Staff responsible for high risk activities.

    f. Enabling confidential reporting by Staff regarding any breach of legal or regulatory obligations or internal policies.

    g. Addressing any instances of non-compliance and ensuring that disciplinary action is taken, along with the required reporting to the Central Bank.

10. ACTUARIAL FUNCTION

An effective actuarial function must be well resourced and properly authorised and staffed as it plays a major role in the Company's overall system of Risk Management and Internal Controls. The actuarial function conducts all the actuarial undertakings per Article (10) of the Regulation, which must include, among other undertakings, the following:

1. Applying methodologies and procedures to assess the sufficiency of the Company's liabilities, including policy provisions and aggregate claim liabilities, as well as determination or reserves for financial risks and to ensure that their calculation is consistent with the requirements set out in the Financial Regulations. This must also include assessing the uncertainty associated with the estimates made in the calculation of the Company's liabilities;

2. Asset liability management with regards to the adequacy and the sufficiency of assets and future revenues to cover the Company's obligations to policyholders and capital requirements, as well as other obligations or activities;

3. Reviewing the Company's investment policies and completing the valuation of assets;

4. The solvency position of the Company, including a calculation of minimum capital required for regulatory purposes and liability and loss provisions;

5. Advising on the Company's prospective solvency position by conducting capital adequacy assessments and Stress Tests under various scenarios, and measuring their relative impact on assets and/or liabilities, and actual and future capital levels;

6. Developing risk assessment and management policies and controls relevant to actuarial matters or the financial condition of the Company;

7. Ensuring the fair treatment of policyholders with regard to distribution of profits awarded to them, when their policies contain elements of bonus/dividend.

8. Ensuring the adequacy and soundness of underwriting policies, which must at least include conclusions on the following matters:

    a. Sufficiency of the premiums to be earned to cover future claims and expenses, taking into consideration the underlying risks (including underwriting risks), and the impact of options and guarantees included in insurance and reinsurance contracts;

    b. The effect of inflation, legal risk, change in the composition of the Company's portfolio, and of systems which adjust the premiums policy-holders pay upwards or downwards depending on their claims history (bonus-malus systems) or similar systems, implemented in specific homogeneous risk groups; and

    c. The progressive tendency of a portfolio of insurance contracts to attract or retain insured persons with a higher risk profile (anti-selection).

9. The development, pricing and assessment of the adequacy of reinsurance arrangements must include analysis of the following matters:

    a. The Company's risk profile and underwriting policy;

b. Reinsurance providers, taking into account their credit standing;

c. The expected cover under stress scenarios in relation to the underwriting policy; and

d. The calculation of the amounts recoverable from reinsurance contracts and special purpose vehicles, if any.

10. Product development and design, including the terms and conditions of insurance contracts and pricing, along with estimation of the capital required to underwrite the product;

11. Ensuring the sufficiency, accuracy and quality of data, the methods and the assumptions used in the calculation of technical provisions and ensure that any limitations of data used to calculate technical provisions are properly dealt with;

12. Comparing best estimates against experience, review the quality of past best estimates and use the insights gained from this assessment to improve the quality of current calculations. The comparison of best estimates against experience shall include comparisons between observed values and the estimates underlying the calculation of the best estimate, in order to draw conclusions on the appropriateness, accuracy and completeness of the data and assumptions used as well as on the methodologies applied in their calculation.

13. Reporting to the Board and Senior Management on the calculation of the Company's insurance liabilities which must include at least a reasoned analysis on the reliability and adequacy of their calculation and on the sources and the degree of uncertainty of the estimates. That reasoned analysis shall be supported by a sensitivity analysis that includes an investigation of the sensitivity to each of the major risks underlying the obligations which are covered in the Company's liabilities. The actuarial function shall clearly state and explain any concerns it may have concerning the adequacy of Company's liabilities.

14. The actuarial function must produce a written report to be submitted to the Board, at least annually. This report must document all of the tasks that have been undertaken by the actuarial function and a summary of their results, and must clearly identify any deficiencies and give recommendations as to how such deficiencies must be remedied.

15. Any other actuarial or financial matters determined by the Board.

11. INTERNAL AUDIT FUNCTION

The internal audit function must be responsible for the following matters, at a minimum:

1. Establishing, implementing and maintaining an audit plan, setting out the audit work to be undertaken in the upcoming years, taking into account all activities and the Company's complete system of governance. The plan must be developed taking a risk-based approach in deciding its priorities and the audit plan must be presented to the Board for approval. Where necessary, the internal audit function may carry out audits which are not included in the audit plan.

2. Disclosing any adverse matters affecting the function's independence.

3. Disclosing any material findings, and the extent of management's compliance with agreed upon corrective measures.

4. Conducting risk-based audits to assess the Company's alignment with the Company's Risk Culture, Risk Appetite, Risk Profile and Risk Limits.

5. Assessing the Company's processes, policies and the documentation thereof on an entity and Group-wide basis and on an individual Subsidiary and business unit basis.

6. Assessing the employees' and business units' compliance with applicable Central Bank Laws, Regulations and internal controls.

7. Assessing the reliability of management information systems and processes.

8. Evaluating the methods of safeguarding Company and policyholder assets and, as appropriate, verifying the existence of such assets and the required level of segregation in respect of Company and policyholder assets;

9. Monitoring and evaluating the effectiveness of the Company's other Control Functions, particularly the Risk Management, actuarial and compliance functions.

10. Coordinating with the external auditors and, to the extent requested by the Board and consistent with applicable law, evaluating the quality of performance of the external auditors.

11. Issuing recommendations based on the result of work carried out in accordance with the audit plan and submit a written report on the findings and recommendations to the Board on at least an annual basis;

12. Verifying compliance of Senior Management with the decisions taken by the Board on the basis of those recommendations referred to in the internal audit report.

12. OUTSOURCING

1. The Risk Governance System must, at a minimum, provide for the following with respect to Outsourcing:

   a. A Board-approved policy that sets out how the materiality of a proposed Outsourcing arrangement is assessed and requiring any material Outsourcing arrangements to be approved by the Board, or the risk/audit committee of the Board;

   b. Policies and procedures to ensure that potential Conflicts of Interest are identified, managed and appropriately mitigated, or avoided;

   c. Policies and procedures that clearly identify and assign to the Company's departments, committees, Internal Controls functions, and other individuals, the roles and responsibilities with regard to Outsourcing and determine in which cases and at which stage, they must be involved;

d. Policies and procedures to ensure that all material risks related to Outsourcing are identified, assessed, measured, monitored, controlled, mitigated, and reported to the Board in a timely and comprehensive manner;

e. Ensure that any outsourced critical business functions are covered in their disaster recovery and business continuity plans, that Outsourcing service providers are fully prepared to implement them and that Outsourcing service providers have their own disaster recovery and business continuity plans to resolve disruptions at their end.

2. All outsourced activity must be governed by written contracts that state the parties' rights and obligations. The Board and Senior Management must consider the effects on the Company's Risk Profile, and assess the service provider's expertise, knowledge, governance, Risk Management, Internal Controls, and financial viability along with the succession issues upon the ending of the contractual relationship with the service provider. The Company must conduct the following:
   a. Perform a detailed examination to ensure that the potential service provider has the ability, the capacity and any authorisation required by law to deliver the required functions or activities satisfactorily, taking into account the Company's objectives and needs;

   b. Ensure The service provider has adopted all means to ensure that no explicit or potential Conflict of Interests jeopardise the fulfilment of the deliverables of the outsourcing Company;

   c. Execute a written contract with the service provider which clearly defines the respective rights and obligations of the Company and the service provider;

   d. Ensure that the general terms and conditions of the outsourcing contract are clearly explained to the Company's Board and authorised by them;

   e. Ensure that the outsourcing agreement does not entail the breaching of any law in particular with regard to rules on data protection; and

   f. Ensure that the service provider is subject to the same provisions on the safety and confidentiality of information relating to the Company or to its policyholders or beneficiaries that are applicable to the Company.

3. A Company must have an outsourcing register that contains key information for each Outsourcing arrangement, and includes at a minimum:
   a. Key non-risk related data, such as the details of the Outsourcing service provider, start and end date of the arrangement, and a brief description of the services being provided.

   b. Whether the Outsourcing arrangement involves any Confidential Data; and

   c. Whether the Outsourcing arrangement is considered Material Business Activity.

4. a. Companies must ensure compliance with all the applicable State legislation and regulations in managing and processing data, when using Outsourcing services.

   b. Companies must ensure that they retain ownership of all data provided to an Outsourcing service provider, and that their customers retain ownership of their data, including but not limited to, Confidential Data, and can effectively exercise their rights and duties in this regard.

c. Where the Outsourcing service provider subcontracts elements of the service which involve Confidential Data, Companies must ensure that the subcontractor fully complies with the applicable requirements as established by law and under this and other applicable regulations.

d. Companies must ensure their data is secured from unauthorised access, including unauthorised access and/or use by the Outsourcing service provider or its Staff.

5. a. Outsourcing agreements must ensure that the Company has unfettered access to all of its data for the duration of the contract, including upon termination of the contract.

b. Outsourcing agreements must include appropriate provisions to protect a Company's data, including non-disclosure agreements and provisions related to the destruction of the data and/or transfer to the Company upon termination of the agreement.

c. Outsourcing agreements must specifically establish standards for data protection, including any nationally recognised information assurance and/or data protection and confidentiality of information requirements in the State.

d. Outsourcing agreements must specifically establish that the Outsourcing service provider, or any of its subcontractors must not provide any other party with access to Confidential Data without first obtaining the specific authorisation of the Company, or the customer, as the case may be.

e. Outsourcing agreements must specify to what extent subcontracting is allowed and under what conditions.

f. Outsourcing agreements must include an explicit provision giving the Central Bank, and any agent appointed by the Central Bank, access to the Outsourcing service provider. This provision must include the right to conduct on-site visits at the Outsourcing service provider, if deemed necessary by the Central Bank and require the Outsourcing service provider to provide the Central Bank, or its appointed agent, any data or information required for supervisory purposes.

g. Outsourcing agreements must include an obligation for the Outsourcing service provider to notify the Company without undue delay of any breach of the Company's data and in particular, breaches of Confidential Data.

6. When Outsourcing outside of the State:

a. Any Outsourcing agreement with a party located outside of the State, must stipulate that the Company and the customer retain ownership of the data at all times, and that the Central Bank can access the Company's data upon request.

b. A Company must explicitly consider the possibility that changes in economic, political, social, legal or regulatory conditions may affect the ability of a service provider outside of the State to fulfil the terms of the agreement. This risk must be managed by a careful selection of service providers and jurisdictions, adequate contractual and practical arrangements, and appropriate business continuity planning.

c. A Company must explicitly consider any other relevant risks arising when the service provider is located outside of the State. These must include, but are not limited to:
   1. Higher levels of operational risk due to poor infrastructure in another jurisdiction;

   2. Legal risk due to differing laws and possible shortcomings in the legal system in the countries where the service is provided; and

   3. Reputational risk due to the breach of the service agreement by the service provider.

d. A Company must ensure compliance with all relevant personal data protection legislation and regulations prior to entering into an Outsourcing agreement with an Outsourcing service provider or third party outside of the State.

e. A Company must establish policies, processes and procedures regarding controls and monitoring activities specifically addressing the business relationship of the Company with an Outsourcing service provider, which includes the sharing of Confidential Data outside of the State.

f. For each of its business relationships a Company holds with an Outsourcing service provider, which includes the sharing of Confidential Data outside of the State, the Company must define concrete security requirements and must ensure that its Staff are sufficiently trained in respect of these requirements.

g. Companies must ensure that third parties implement and maintain the appropriate level of information security and service delivery.

h. With regard to Outsourcing service providers located outside of the State, the Central Bank may exercise its powers through collaboration with the relevant authorities of any relevant jurisdiction.

7. Prior to Outsourcing any material activity, including to any related party, Companies must obtain a prior notice of non-objection from the Central Bank. When requesting the non-objection, Companies must provide the Central Bank with the following at a minimum:

   a. A brief explanation of the business activity to be outsourced;

   b. A summary of the materiality assessment;

   c. A summary of the risk assessment;

   d. A summary of the due diligence performed and its outcome;

   e. A confirmation of the agreement of the internal audit function and the compliance function;

   f. An overview of any closely related outsourcing agreements;

   g. Confirmation of compliance with the requirements of the Risk Management and Internal Controls Regulation for Insurance Companies and these Standards.

   h. Evidence of the approval of the proposed Outsourcing by the Board or Board committee.

The Central Bank will either grant the non-objection, request further information, or decline the request. Companies are encouraged to discuss their material Outsourcing plans early and coordinate with the Central Bank to avoid the non-objection process delaying the Outsourcing.

8. Although all requests for non-objection will be considered on their individual merits, the Central Bank, will in general, not permit the Outsourcing of core insurance activities, and key management and Control Functions, including but not limited to Senior Management oversight and internal audit. The Central Bank may determine adding further requirements in this regard, from time to time

13. COUNTERING FRAUD IN INSURANCE

1. A Company must have policies, procedures and controls to minimise the risk of internal and external fraud in the following areas, at a minimum:
    a. Product development;

    b. Onboarding clients;

    c. Hiring and dismissal Staff;

    d. Outsourcing;

    e. Claims' management and settlements; and

    f. Dealing with practitioners of Insurance Related Professions.

2. Insurance fraud categories include:
    a. Internal fraud, which is committed by a Board member, Senior Manager or other member of Staff on his/her own or in collusion with others who are either internal or external to the Company.

    b. Insurance Related Professions' fraud, which is committed by practitioners against the Company, policyholders or beneficiaries.

    c. Policyholder fraud, which is committed against the Company in the purchase and/or execution of an insurance product by one or more persons by obtaining wrongful coverage or payment.

3. Preventive policies, procedures and controls to manage internal fraud must include:

    a. Creating a culture based on integrity;

    b. Developing and maintaining policy and guidelines on ethical behavior;

    c. Adequate supervision of Staff;

    d. Performing pre-employment and in-employment screening of permanent or temporary Staff;

    e. Documented job descriptions;

f. Periodical job rotation and mandatory vacations for Staff in fraud sensitive positions;

g. Observing the "four eyes" principle.

h. Segregation of duties;

i. Having procedural safeguards over the use, handling and availability of cash;

j. Establishing a transparent policy in dealing with internal fraud by Board members and Staff, including a policy on reporting to the relevant law enforcement agency;

k. Establishing a clear dismissal policy for internal fraud cases in order to deter potential perpetrators.

4. Preventive policies, procedures and controls to manage policyholder fraud must include:

a. Customer due diligence prior to inception.

b. Requesting additional supporting documents to verify the policyholder's sources of wealth.

c. In terms of claims settlement, procedures must include:

1. Using professional judgement based on experience;

2. Identifying red flag lists;

3. Conducting peer reviews;

4. Reviewing internal and/or external databases or other sources;

5. Using information technology tools, such as voice stress analysis, data mining, neural networks and tools to verify the authenticity of documents; and

6. Interviewing claimants.

5. Preventive policies, procedures and controls to manage Insurance Related Professions' fraud must include:

a. Having in place a documented policy and procedure for the appointment of new practitioners of Insurance Related Professions.

b. Having an application form and terms of business agreement that have to be completed and signed by the practitioners of Insurance Related Professions.

c. Ensuring the application form requires applicants to disclose relevant facts about themselves, including qualifications, experience, and qualifying body.

d. Verifying the financial soundness of the applicant and checking references.

e. Having an effective sanction policy in case of non-compliance by the practitioners of Insurance Related Professions.

6. A Company must collect information in respect of insurance fraud from the market and to provide same to the Board and Staff. Such information must be used to evaluate the effectiveness of policies, procedures and controls, and to make changes were necessary.

7. A Company must establish and maintain an independent audit function to test fraud, fraud risk management, procedures and controls.

8. A Company must encourage Staff to report all irregularities and must have a whistle blowing policy in place for this purpose.

9. A Company's fraud management strategy must be aligned with the Risk Profile of the Company. In determining the Risk Profile, the following factors must be taken into consideration:
    1. size of the Company;
    2. organisational structure;
    3. products and services offered;
    4. payment methods used for premiums and claims;
    5. types of policyholder; and
    6. market conditions.

10. A Company must retain records of all reported cases of fraud along with the findings, and must establish standards relating to the turnaround time for the assessment of fraud, documentation of analysis and keeping records of fraud incidents.

11. A Company must have effective reporting systems to the Board in terms of frequency of incidents, along with recommendations to address the issues.

12. A Company must report any suspected or confirmed fraud cases to the proper law enforcement authorities immediately and notify the Central Bank of such reporting.

13. A Company must provide the Board and Staff with guidance on fraud indicators and training on preventing, detecting, reporting and remedying fraud. Such training must be commensurate with the position that the person holds within the Company.