WAPIC INSURANCE PLC.

Enterprise Risk Management Framework

Version	2
Approval date	July 28, 2017

Document History

Prepared By	Reviewed By	Date/Year	Version
Onyeka Halim	Tariela Adebiyi	July 2017	2

Version Control

Revision Date	Version	Description	Amendments Made	Owner
27/06/2017	2.0	Review of Enterprise Risk Management	This is the second version of the policy updated to meet Solvency II requirements	Chief Risk Officer

Approval Table

Version	Designation	Name	Signature	Date Approved
	Chief Compliance Officer	Muyiwa Oke		5/7/17
	Chief Risk Officer	Peter Ehimhen		05/07/17
	Executive Director	Bode Ojeniyi		08/07/17
	Managing Director	Yinka Adekoya		08/07/17

Table of Content

Glossary

ACRONYMS	MEANING
BACC	Board Audit and Compliance Committee
Board	Board of Directors
BRMGC	Board Enterprise Risk Management and Governance Committee
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CEO	Chief Executive Officer
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
ERMGC	Enterprise Risk Management and Governance Committee
EVA	Economic Value Added
EXCO	Executive Committee
IT	Information technology
KRI	Key Risk Indicators
MCR	Minimum Capital Requirement
MD	Managing Director
NAICOM	National Insurance Commission Nigeria
RAPM	Risk Adjusted Performance Measure
RAROC	Risk Adjusted Return on Capital
RMF	Risk Management Framework
RM	Risk Management
UCMC	Underwriting and Claims Management Committee
Wapic Insurance PLC	"Wapic" or "the Company"

About the Framework

Purpose of the Framework

This document describes the Enterprise Risk Management (ERM) Framework of Wapic Insurance Plc. ("Wapic" or "the Company"). The major focus of the ERM framework is to ensure the Company complies with sound risk management practices in achieving its business goals and objectives, and to focus on material risks in an integrated manner, rather than in isolation.

With the increasing complexities of transactions, global economic issues, the sophistication of customers, expansion of the insurance business to the global frontiers and the uncertainties in the operating environment; risk management remains a critical success factor for achieving insurance goals and strategies.

The primary role of risk management is to minimize the divergence between expectations and outcomes, thus ensuring the realization of more predictable results. This can only be achieved through a robust framework and clearly defined and transparent processes for the:

- identification of all factors that may lead to the said divergences ("Risk Identification")
- estimation of the likelihood of their occurrence and the extent or severity of their impact in the event of occurrence ("Risk Assessment/Measurement")
- design of effective controls to minimize both the likelihood and the impact of risk events ("Risk Mitigation/Control")
- establishment of procedures to ensure that these controls are effective and are being complied with ("Risk Monitoring")
- regular reporting of risk events and controls ("Risk Reporting")
- provision of sufficient capital to absorb the adverse impact of expected and unexpected losses

This document lays out the ERM framework for the development and institutionalization of processes that enables Wapic to:

- Identify and understand the full spectrum of risks facing it
- Define its appetite for risk, based on its strategic objectives
- Assess, measure and quantify the risks identified
- Develop risk mitigation and control techniques
- Enhance the overall performance of the Company
- Comply with all regulatory requirements with respect to risk management practices, including Solvency II guidelines and domestic regulatory guidelines on risk management practices

Scope and Coverage

ERM framework will cover all the risks facing the Company and its insurance subsidiaries irrespective of whether they arise at exposure level or at firm level. It covers the most significant risks to the Company as listed below:

- Underwriting Risk
- Reinsurance Risk
- Investment Risk
- Operational Risk
- Reputational Risk

Ownership of this Framework

The ownership of the ERM framework rests with the Chief Risk Officer (CRO), who shall be responsible for the implementation of the framework in the Company, under the supervision of the Board Enterprise Risk Management and Governance Committee ("BERMGC").

Approval, Review and Update

The ERM framework shall be approved by the Board of Directors ("Board") who may delegate the responsibility to the Board Enterprise Risk Management and Governance Committee.
The CRO shall monitor and ensure the continued relevance of the framework in light of the changing strategy, macroeconomic and regulatory environment and make recommendations to the BERMGC required.

Users of the Framework

The ERM Framework is intended for the use of all units and staff within Wapic.

1 Definition of Enterprise Risk Management, Risk Management Philosophy, Culture, Objective

1.1 Definition of Enterprise Risk Management

The Committee of Sponsoring Organizations of the Treadway Commission, widely known as COSO, defines ERM as:
"a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

The ultimate objective for implementing ERM is to assist the Board and Management to align the Company's risk appetite to its business strategy, enhance risk response decisions, reduce operational losses, identify and manage interdepartmental risks, allow for more informed risk decisions and improve capital management.

The following are the key points of COSO's ERM definition that will guide Wapic in its adoption of the framework:

- ERM is aimed at achieving organizational objectives: ERM plays a significant role in helping an organisation achieve its organizational objectives and goals
- ERM is applied in strategy setting: An effective ERM should play a major role in helping to establish strategies with its associated risks
- Linked to risk appetite: Risk appetite is the amount of risk that an organisation is willing to accept in pursuit of achieving core purpose, mission and vision
- ERM provides only reasonable assurance: However well-conceived and implemented, ERM cannot provide management or other stakeholders with 100% assurance of outcomes, i.e., with the implementation of ERM framework, possibility of achievement of organisational objectives will improve significantly but no absolute assurance of achievement of organisational objectives is possible. Depending on the sophistication of ERM system, the level of assurance will differ.

1.2 Risk Management Philosophy and Culture

Wapic considers risk management philosophy and culture as the set of shared beliefs, values, attitudes and practices characterising how the firm considers risk in everything it does, from strategy development and implementation to its day-to-day activities.

In this regard, Wapic's risk management philosophy is that moderate and guarded risk attitude will ensure sustainable growth in shareholder value and reputation. The Company believes that ERM will provide the superior capabilities to identify and assess the full spectrum of risks and to enable staff at all levels to better understand and manage risks. This will ensure that:

- Risk acceptance is done in a responsible manner
- The executive and the board of the firm have adequate risk management support
- Uncertain outcomes are better anticipated
- Accountability is strengthened
- Stewardship is enhanced

Wapic has identified the following attributes as guiding principles for its risk culture:

- The Board and Executive shall demonstrate their commitment to risk management and foster a sound risk management environment
- All forms of risk and their impact in business transactions and processes shall be considered in decision-making
- The Company shall avoid products, investments, projects which it cannot reasonably and objectively measure and manage their returns and/or associated risks
- Business-unit and firm-wide risk profiles shall be created and evaluated, to consider what is best for individual business units and the organisation as a whole
- The ownership and accountability for risk and risk management shall be the responsibility of all staff
- The Company shall strive to achieve leading practices in ERM
- The Company shall document and report all significant risks and ERM deficiencies
- Adopt a holistic and integrated approach to risk management and bring all risks together under one or a limited number of oversight functions;
- Risk officers shall be empowered to perform their duties professionally and independently without undue interference
- The Company shall ensure clear segregation of duties between market facing business units and risk management and control functions

1.3 Risk Management Objectives

In line with Wapic's adoption of COSO's ERM framework, the core and supporting objectives for managing ERM are as below:

1.3.1 Core Objectives

Core objective of ERM is to provide a reasonable degree of assurance to the Board that the risks threatening Wapic's achievement of its vision '**To transform and illuminate the insurance industry for the benefit of our customers and other stakeholders**' are identified, measured, monitored and controlled through an effective integrated risk management system covering credit, market, operational, investment risk, underwriting risk, claims management risk, reinsurance risk, provisioning and reserving risk, liquidity risk and other material risks.

1.3.2 Supporting Objectives

- To formalize and communicate Wapic's commitment to achieving information objectives of timely provision of information for decision making
- To formalize and communicate Wapic's commitment to achieving compliance objectives of remaining fully compliant with regulatory requirements of the National Insurance Commission Nigeria (NAICOM) and other regulatory and legal requirements that are relevant and applicable to the Company
- To formalize and communicate Wapic's commitment to aligning risk strategies to support business objectives
- To communicate Wapic's commitment to adopt Solvency II, COSO's ERM framework and international best practices in relation to risk management in a planned manner over time
- To protect against unexpected losses and reduce earnings volatility
- To ensure that the business plans are consistent with the risk appetite and supported with an effective and efficient risk management function
- To maximise stakeholder's value, opportunities and earning potential
- To promote a risk awareness culture

1.4 Risk Management Strategy

The Company shall adopt the following strategies to manage its risks:

- Empower all staff to proactively identify, control, monitor, and regularly report risk issues to management
- Strengthen the risk management framework to fully support the strategic business units and the overall business strategy, the Risk management strategy is to develop an integrated approach to risk assessments, measurement, monitoring and control that captures all risks in all aspects of the firm's activities
- Drive overall corporate objective with emphasis on protecting the organisation from risks while increasing its market share
- Ensure the existence and appropriate implementation of a risk management process that is well articulated to identify/assess measure, monitor and control all the identified risk elements
- Develop detailed policies and guidelines to guide the management of claims risks, operations risk, market risks, investment risks, liquidity risks and other identified risk types

1.5 Risk Appetite

Risk Appetite involves definition by the insurer, the extent to which risks should be acceptable to it in pursuance of its business strategies. The Risk Appetite process aims at balancing positive (sizeable improvement in returns) and negative (large losses) aspects of risk-taking by an insurer.

The Company's risk appetite shall be expressed both quantitatively and qualitatively by identifying its key stakeholder objectives and translating them into measurable Key Performance Indicators (KPIs). These KPIs shall be considered to be core risk appetite metrics and they shall form the basis upon which specific risk level appetite and limits shall be articulated.

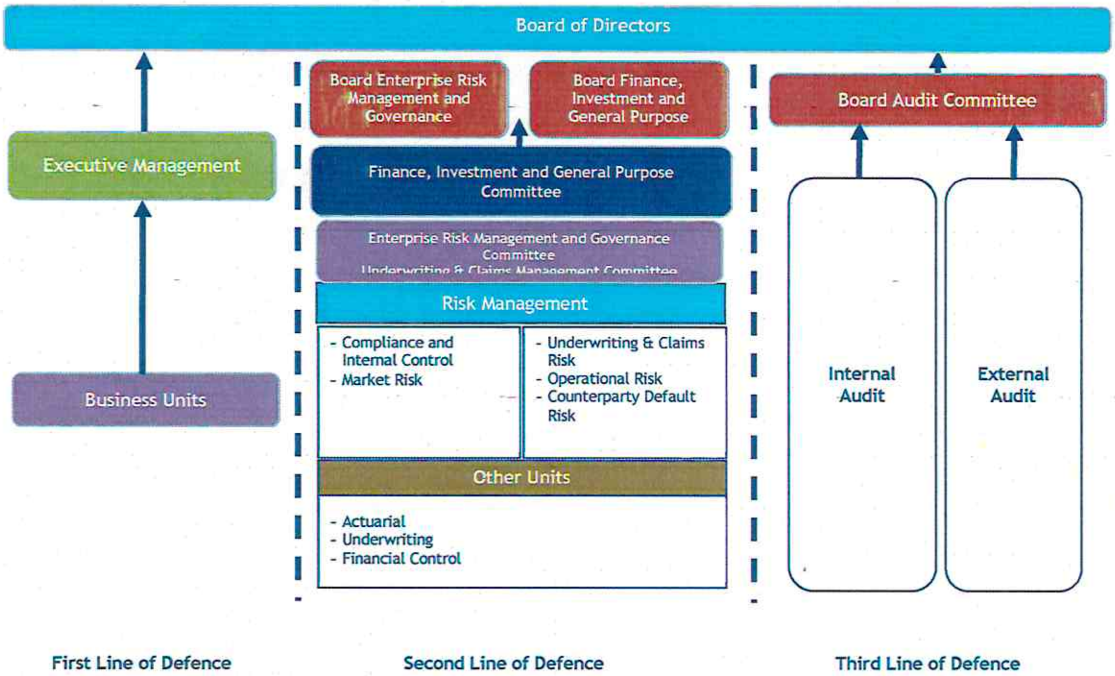
The risk profile of the Company shall be monitored against the risk appetite to monitor any deviations which would require mitigation actions to realign the risk profile with the risk appetite.

The Board shall be responsible for setting and reviewing the risk appetite at least annually to ensure that it is consistent with Wapic's strategy, business environment and the stakeholder requirements.

2 Risk Governance Structure and Responsibilities

2.1 Risk Governance Structure

Below is the governance structure for ERM in Wapic based on the three lines of defence:



2.1.1 First line of defence

This consists of business units and support functions with primary responsibility for risk management. The process for assessing, evaluating and measuring risk is integrated in their daily activities. The primary responsibilities and objectives of the first line of defence include:

- identifying, reporting and prioritising existing and emerging risks
- implementing the Company's policies and managing daily risk exposures by using appropriate procedures and internal controls
- identifying risk events and losses, reporting and escalating material risks and implementing remedial actions to address these issues

2.1.2 Second line of defence

The second line of defence comprises all business units and functions responsible for providing independent risk oversight, monitoring and challenge of the effectiveness of the Company's risk management processes. They provide support, training and counsel to business units in relation to risk management and report on risk management activities to the various risk committees.

The primary responsibilities and objectives of the second line of defence are to:

- establish risk policy, standards and limits and monitor adherence
- provide risk oversight and independent reporting to Executive Management and the Board
- assist the first line of defence in implementing the Company's risk management framework and policy
- establish a measurable and systematic process for risk assessment and governance reporting
- ensure the effectiveness of risk management activities and allocate resources to execute risk management initiatives
- provide analytics, guidance and coordination among diverse business units
- provide independent review and report on the effectiveness of the risk management policy as implemented by the first line of defence

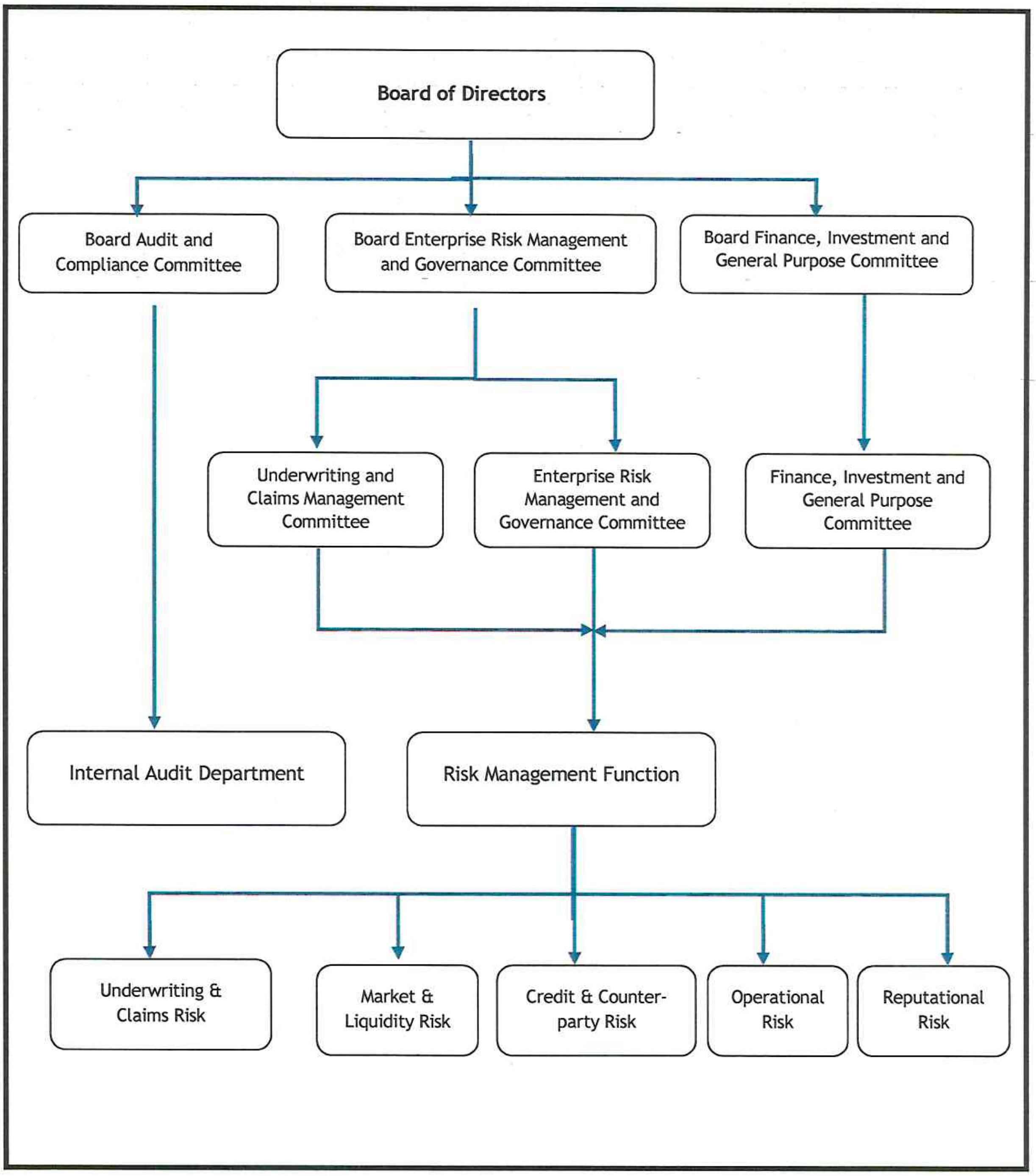
2.1.3 Third line of defence

The third line of defence comprises functions with primary responsibility for assessing and providing independent assurance on the adequacy, appropriateness and effectiveness of the Company's overall risk management framework, policy and actions. Specifically, this line of defence shall perform the following functions:

- assess the adequacy and effectiveness of the Company's risk management and control framework
- monitor compliance of business units and support functions with the risk policies and procedures

2.2 Functional Structure for Enterprise Risk Management

Below is the functional structure of ERM in Wapic:



2.3 Roles and Responsibilities

This section of the framework deals with the roles and responsibilities of the Board, Board Enterprise Risk Management and Governance Committee (BERMGC) Risk Committees and Risk Management Department.

Roles and Responsibilities are at defined at three levels:

- Level 1 – Policy and Strategy Level
  - ✓ The Board, Board Audit and Compliance Committee (BAAC) and BERMGC are responsible for approval of Policies and its implementation throughout Wapic
- Level 2 – Risk Monitoring and Control Level
  - ✓ Finance, Investment and General Purpose Committee (FI&GP), Enterprise Risk Management and Governance Committee (ERMC) and Underwriting and Claims Management Committee (UCMC) are responsible for assisting the Board and BERMGC in monitoring the implementation of risk policies
- Level 3 – Risk Coordination and Operation Level
  - ✓ The Risk Management function shall be responsible for implementing the operational aspects of the risk management policies Business Units for respective risks are responsible for Operational aspects of implementing risk policies. Chief Risk Officer (CRO) shall head the Risk Management Department

2.3.1 Board of Directors

The Board representing the interests of stakeholders, has the ultimate responsibility for risk management. The Board has the primary responsibility for:

- Establishment of the governance structure (board subcommittees, executive responsibilities and risk management and assurance functions)
- Approval of risk policies to mandate a set of standards for risk management throughout Wapic that include risk identification, measurement, setting of exposure and risk limits, monitoring and control and risk reporting
- Forming a view of the risk culture in the Company, and the extent to which that culture supports its ability to operate consistently within its risk appetite, identifying any desirable changes to the risk culture and ensuring the institution takes steps to address those business risks
- Overseeing the ERM framework and its operationalization by management
- Setting appetite for risk taking at the firm level and at various levels in consistent with business strategies
- Approving the Company's risk management strategy

- Ensuring effectiveness, independence and integrity of risk management system through internal control & audit
- Periodically (at least annually) reviewing the risk strategy and significant risk policies of Wapic

The Board of Director's risk management oversight roles and responsibilities shall be delegated to the BERMGC and Board Audit and Compliance Committee (BACC) as applicable. Without prejudice to the roles of these committees, the Board shall retain the ultimate responsibility for risk management.

Refer to the Board charter for the composition of the Board.

2.3.2 Board Enterprise Risk Management and Governance Committee

The committee has the full responsibility of assisting the Board in formulating strategies for enterprise-wide risk management, evaluating overall risks faced by Wapic, aligning risk policies with business strategies and determining the level of risks which will be in the best interest of the Company.

The following are the roles and responsibilities of the BERMGC:

- Primary role of the BERMGC is to effectively coordinate the efforts of management risk committees to provide an integrated view of risks faced by Wapic to the Board at regular intervals and to effectively implement the Board's strategy for risk management
- Review reports on the Company's risk profile, the action plans in place to manage high risks, and monitor progress against plans to achieve these actions
- Based on the reports received, BERMGC will take decisions and provide guidance / mandate to management risk committees and relevant functions of the Company on the management of risks
- Make suitable recommendations to the Board as it sees fit and examine any other matters referred to it by the Board.
- BERMGC will review issues raised by Internal Audit that impact the risk management and make suitable recommendations to the Boar.
- The Committee, by virtue of powers delegated to it by the Board, will approve any changes in risk policies. Changes to the policy approved by BERMGC have to be ratified by the Board within an acceptable timeframe set by the Board
- Approval of exceptions to the risk policies upon thorough enquiry into circumstances leading to exceptions, nature, size and genuineness of exceptions. Repetition of exceptions of similar nature should lead to changes in the policy of permanent nature
- BERMGC will review issues raised by Internal Audit that impact risk management and make suitable recommendations to the Board

- Make suitable recommendations to the Board as it sees fit and examine any other matters referred to it by the Board

  Refer to the BERMGC charter for the composition of the BERMGC.

2.3.3 Enterprise Risk Management and Governance Committee

The following are the roles of the ERMGC:

- Address all categories of key risks, and their components, to which the Company is exposed
- Manage significant/material risk exposures (individually or in the aggregate) at a much higher level than the individual business units
- ensure the adequacy of controls with respect to the management of risks
- Place the interests of what is best for the firm ahead of individual business unit interests;
- Provide for and champion enterprise-wide risk management and achievement of Wapic's risk philosophy, culture and objectives
- Provide for formal interaction between business units and the sharing of specialised knowledge/research for the mutual benefit of all and the promotion of risk management and corporate governance
- Provide assurance to shareholders, policy holders, investors, rating agencies, analysts, regulators and others that sound corporate governance and effective risk management prevail throughout the organization

Refer to charter for ERMGC for the composition of ERMGC

2.3.4 Finance, Investment and General Purpose Committee (FI&GPC)

The FI&GPC shall be responsible for the following tasks:

- Endorse the Contingency Funding Plan
- Management of all the risks emanating from use of funds by the Company
- Establish significant funding source limits and review exposure reports
- Approve course of action for rectifying any breach of liquidity limits
- Review liquidity reports for reasonableness, consistency and completeness
- The FI&GPC shall be responsible for management of all the risks emanating from use of funds by the firm

2.3.5 Underwriting and Claims Management Committee (UCMC)

The UCMC shall have the responsibility to:

- Evaluate the adequacy of premiums being charged for risk exposures being taken by the Company
- Evaluate and approve the reinsurance strategy of the firm which is a proxy for the risk appetite of the firm with respect to underwriting risks
- Address all the key risks related with underwriting exposures taken by the firm
- Evaluate and approve for modification existing products and introduction of new products where appropriate
- Make decisions related to claims management

2.3.6 Risk Management Function

The following are the responsibilities of the Risk Management Function:

- Understanding the business strategy of the firm and use necessary measures to influence both the board and the managers and employees responsible for making day-to-day decisions
- Providing overall direction for the enterprise-wide risk management framework across the Company, for the management of risks e.g. reputation risk, legal and compliance risk, credit risk, investment risk and operational risk etc.
- Defining policies, process and strategy for the management of risks, including risk philosophy, appetite, tolerance limits
- Extending risk principles into wider business strategy
- Enabling the Company to make decisions based on a better appreciation of the relationship between risk and reward
- Identifying and monitoring emerging risks that may be material for Wapic in future due to changes in the risk environment

- Reviewing and performing analysis of the Company's business and investment proposals to ensure that risks have been adequately identified and mitigating factors put in place
- Ensuring business continuity, defined as the ability to sustain operations in the event of major losses and have crisis management policies in place

2.3.6.1 Market and Liquidity Risk Management Function

The following are the roles and responsibilities of the market and liquidity risk management function:

- Establish liquidity and funding limits and identify exceptions to limits
- Perform stress tests and establish action plans
- Receive notification of limit excesses and approve corrective actions
- Maintain independent market and liquidity risk-reporting
- Prepare and circulate liquidity reports to management

2.3.6.2 Counterparty and Credit Risk Management Function

The following are the responsibilities of the counterparty and credit risk management function:

- Review the process for selection of financial institutions, reinsurance and insurance brokers/agents
- Preparation of reports showing the reinsurance counterparty risk
- Review of the credit limits set for financial institutions, insurance and reinsurance brokers
- Decide the process for selection and monitoring of reinsurance program

2.3.6.3 Operational Risk Management

The following are the responsibilities of the operational risk management function

- Capturing data on risk events and integrating those data from a multitude of systems to build a clear and accurate view of risks across the business
- Ensuring development and implementation of appropriate information systems for risk measurement and reporting, which identify losses, key risks to be managed, incidents etc.
- Monitoring compliance with the Company's risk policies and limits
- Informing the Board and Management of significant risk issues in the firm and risk transfer strategies taken in order to achieve mitigation of such risks

2.3.6.4 Reputational Risk Management

The following are the responsibilities of the reputational risk management function

- Ensure that the zero tolerance for non-compliance with laws and regulatory guidelines of the Management is communicated to all stakeholders and employees
- Ensure transparency, ethical behaviour and professionalism is ingrained in the risk culture of the organization
- Ensuring that there is full compliance with the Code of conduct and other internal policies

2.3.7 Internal Audit

Internal Audit is an independent appraisal function established within the Company to examine and evaluate its internal control systems, improve the effectiveness of risk management, control, and governance processes. Internal Audit's core role with regard to ERM shall be to provide objective assurance to the Board on the effectiveness of Wapic's ERM activities, to help ensure key business risks are being managed appropriately and that the system of internal control is operating effectively.

It is the responsibility of the Internal Audit to report the findings of their review to the Audit committee of Wapic for corrective actions to be taken. Internal Audit shall also follow up on the corrective actions taken for the findings already submitted.

2.3.8 Internal Control and Compliance

The internal control and compliance function shall be responsible for the:

- Examination and evaluation of the adequacy and effectiveness of the internal control systems
- Independent investigation of risk management related issues
- Review of the application and effectiveness of risk management policies, procedures and risk assessment methodologies
- Evaluation of risk management processes and reporting of key risks
- Review of the management and financial information systems, including the electronic information system
- Review of the accuracy and reliability of the accounting records and financial reports
- Review of the means of safeguarding assets
- Review of the processes/systems established to ensure compliance with legal and regulatory requirements, codes of conduct and the implementation of policies and procedures
- Provision of independent quality assurance to the Board

2.4 Underwriting and Claims Units

The underwriting function which is decentralized across business divisions plays the key role of executing decisions taken by the ERMGC. The function shall assist the ERMGC in decision making by updating the Committee on the various risks identified in the underwriting process and drawing up a suitable action plan for the future. The roles and responsibilities of the function includes:

- Ensuring that the Underwriting Risk Policy is strictly adhered to in the underwriting process
- Implementation of strategic plans for general insurance underwriting
- Product pricing and preparation of quotes for insurance proposals
- Developing new insurance products and modifications to existing products and their testing for market acceptability
- Selection and monitoring of loss adjusters and other technical professionals for conducting on site examination and loss estimation for claims
- Frequent review and updating of risk registers and control assessments for underwriting
- Processing of claims and interfacing with customers, actuaries and other stakeholders for any issues of concern
- Record keeping of all the proposals and claims transactions

2.5 Reinsurance Unit

The Reinsurance unit plays a key role of executing decisions relating to reinsurance taken by the ERMGC. The unit shall assist the ERMGC in establishing robust reinsurance management program and related processes. Its function shall include:

- Development and implementation of the reinsurance risk decisions taken by the ERMGC
- Ensuring that an effective reinsurance arrangement is entered into with a reinsurance firm(s)
- Preparation of reinsurance advise based on Company's treaty with the reinsurance firm
- Generation of reinsurance listing and processing from the system
- Scrutiny of quarterly reinsurance reports with what is ceded to reinsurance firm
- Completion of reinsurance certificate for ceding to reinsurance firm
- Streamlining and improvement of processes through reinsurance program management
- Complying with the reinsurance norms set by the ERMGC

2.6 Other Business Units

The management of risk in the business units shall be in line with Company's policies and principles. Business units shall have the following responsibilities:

- Adhere to the Company's process for identifying and managing risks to which they are exposed
- Carry out day-to-day identification, mitigation and monitoring of risks within their business units
- Ensure implementation of the Company's risk management strategies
- Manage the daily risk exposures by utilising appropriate procedures and controls in line with the Company's risk management framework
- Remediate and report all material risk issues to the CRO

3 Enterprise Risk Management Process

The ERM process defines the sequence of activities and tasks that must be performed to execute the risk management framework with the objective of achieving and maintaining the desired level of risk response for the Company. It includes requirements for the identification, assessment, measurement, mitigation/control, monitoring and reporting of facing the Company.

3.1 Risk Identification

Risk identification is an integral part of an insurer's risk management framework. The objective of the risk identification activity is to generate a comprehensive list of known and emerging risks and sources of risk facing the Company. These risks may prevent, degrade, delay or enhance the achievement of our strategic objectives.

A sound process of risk identification would typically be comprehensive and systematic and include a mechanism for regularly updating and re-assessing risks and identifying new risks.

In identifying risk, the Company shall provide answers to questions similar to the following:

- What are our goals and objectives?
- What could prevent us from achieving our goals and objectives?
- How is our performance measured and what could contribute to variability in the results of those measures?
- What are the business issues that keep our senior management and shareholders awake at night?

Refer to the individual risk management policies for more clarification on risk identification.

3.1.1 Techniques to be adopted in identifying Risk

The techniques used by Wapic to enable identification of risks and their impact shall include:

- **Self / risk assessment** — the Company will assess its operations and activities against a menu of potential risk vulnerabilities. This process will be facilitated through a workshop and may incorporate checklists or the use of other risk identification tools to identify the strengths and weaknesses of the risk management environment
- **Risk register** — during this process, various business units, organisational functions, process flows and interdependencies are mapped by risk type. This exercise typically reveals areas of weakness and helps prioritise subsequent management action
- **Risk indicators** — risk indicators are statistics and/or metrics (often financial) which can provide insight into the Company's risk position. These risk indicators will be reviewed on a regular basis (such as monthly or quarterly) to alert the Board and Management to changes that may indicate risk concerns.

These techniques are not mutually exclusive and may be utilized in conjunction with each other. The Chief Risk Officer shall coordinate all risk identification activities.

3.2 Risk Assessment

The risk assessment activity involves different methods of grading risks in order to assess the possibility of their occurrence and the extent of damage to the Company in the event they occur. The activities involved include establishing ways of measuring the risk (risk rating) and ranking the risks based on the outcome of this measurement (risk prioritization).

3.2.1 Risk Assessment Approach

The following approaches shall be used to conduct the risk assessment activity.

- **Facilitated workshop** – This will involve holding workshops with key stakeholders within the Company to discuss and evaluate the likelihood and impact of the occurrence of the identified risks. The workshops shall be attended by risk champions within the business units, Head of Units and may include participants from Internal Audit or other functions vital to the Company's activities
- **Interviews** – This will involve holding stakeholder interviews to obtain their opinions on risk categories being assessed. This approach is desirable where it is difficult to get all the required personnel into a workshop session
- **Questionnaires** – This involves developing and administering structured questionnaires to key individuals to obtain their opinions on the level of risk exposure affecting their business unit

3.2.2 Likelihood of Risk Occurrence

The likelihood of occurrence is the measure of the probability that a risk event will occur. The factors that should be taken into account in the determination of likelihood are: the source of the threat, capability of the source, nature of the vulnerability and existence and effectiveness of current controls. Likelihood can be described as high, medium and low.

Likelihood and Frequency Matrix

Rating	Scale	Likelihood	Frequency
Rare	1	May occur in exceptional circumstances	Once in 10 years
Unlikely	2	May occur at some time	Once in every 5 years
Possible	3	Should occur at some time	Annually

Rating	Scale	Likelihood	Frequency
Likely	4	Probably occur in most circumstances	Once in a quarter
Almost Certain	5	Will occur in most circumstances	At least monthly

3.2.3 Magnitude of Impact

The magnitude of impact is the potential effect that a risk could have on the Company if the risk crystallises. It is worth mentioning that not all threats will have the same impact as each system in the organization is worth differently.

Magnitude of Impact

Impact	Financial	Non-Financial			
		Customer	Staff	Regulatory	Reputation
Catastrophic (5)	Above 20% impact on Shareholders' Funds (SHF)*	Significant impact to most/all of customer base, channels, regions or portfolios	Widespread industrial action or significant impact to most/all of our people	Suspension or loss of licence	National adverse media attention and/or substantial long term damage
Major (4)	Between 10% and 20% of SHF*	Impacts to most customers channels, regions or portfolio	Loss of key specialists team (s) or significant adverse impact to our people in more than one business unit	Sustained regulator scrutiny and/or significant fines and/or formal undertaking	Sustained local media attention and/or substantial medium to long term damage
Moderate (3)	Between 5% and 10% of SHF*	Impacts some part of customer base, channel, region or portfolio	Some impact to our people in more than one business unit	Targeted regulatory scrutiny or investigation	Local adverse local media attention and/or substantial short to medium term damage
Minor (2)	Between 1% and 5% of SHF*	Impacts small part of customer base, channel, region or portfolio	Some impact to our people in more than one team within one business unit	Routine regulatory finding	Limited adverse media attention and/or some short term damage and/or complaints to industry complaints body
Insignificant (1)	Less than 1% of SHF*	Minimal impact to part of customer base, channel, region or portfolio	Minimal impact to our people and limited to local team	Little or no impact	No publicity and/or minor short term damage

3.2.4 Risk Rating Grid

The risk factor or risk rating is determined by a combination of the magnitude of impact and the likelihood of risk occurrence. A matrix categorised as high, medium and low, is formed by this combination as shown in figure below:

Risk Rating Grid		Impact				
		1	2	3	4	5
Likelihood	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Legend		
Low	Medium	High

- **High risks**: are risks that may materially influence the attainment of the business objectives. Risks in this category should be prevented at source. They threaten the achievement of strategic objectives and should be mitigated or eliminated with preventive controls. These risks require the active attention and involvement of the Board and Management to ensure they are mitigated appropriately
- **Medium risks**: are risks that may influence the achievement of short-term business objectives. Risks in this category should be detected and monitored. They need to be monitored to ensure that they are properly managed and do not increase in level of impact. Detective controls should be put in place to ensure that these risks are detected before they occur
- **Low risks**: are risks which occur in the normal course of business. These risk typically have no material influence on the achievement of business objectives and require minimal monitoring unless a subsequent risk assessment shows a material change

3.2.5 Control Assessment

This is any element within a process which has been developed to facilitate action or reduce or eliminate either the likelihood or the impact of a risk event in the business. It can be preventive, detective, corrective or directive. Controls are assessed on the effectiveness and adequacy.

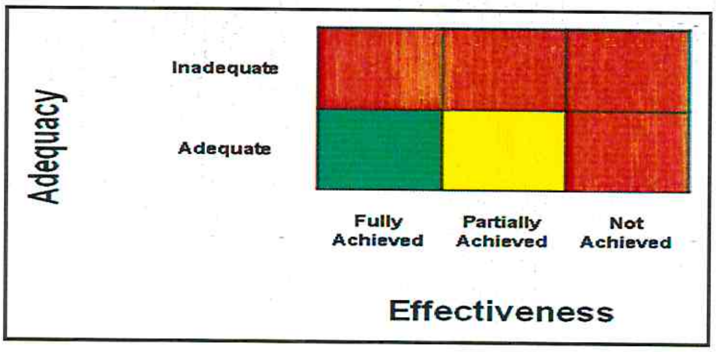
- **Control Effectiveness**

  The effectiveness of the control is determined by considering how successful the control is in producing the desired or intended result.

- **Control Adequacy**

  The adequacy of the control is determined by considering the design of the control and how well the control should work in theory if it is always applied as intended.

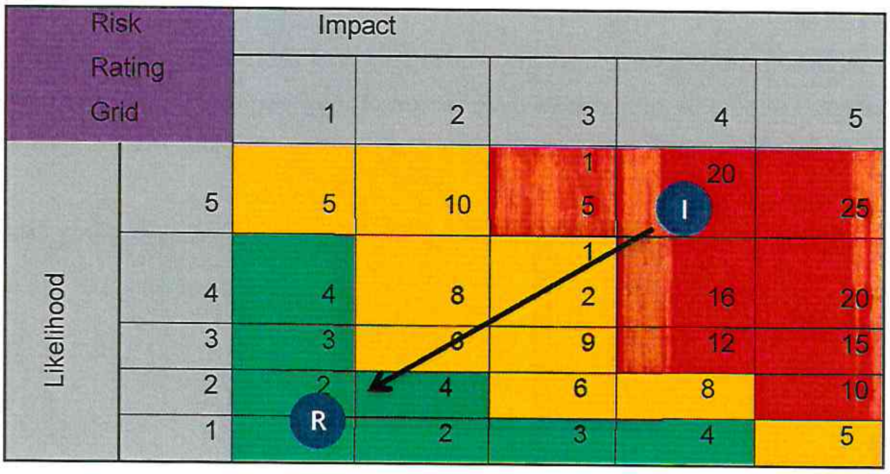
The table below shows the control rating scale:



3.2.6 Residual Risk Assessment

Identification of controls and assessment of their effectiveness shall be required in determining the Residual Risk Level. This is because risks that are not subject to effective controls may result in more catastrophic consequences.

The matrix below shows how residual risk level shall be determined from the relationship between the inherent risk level (level of risks determined prior to control assessment) and the control rating:



3.3 Risk Measurement

Risk Measurement involves application of estimation standards of risks across the business including but not limited to; Underwriting, Credit, Reinsurance, Investment, Operational and Reputation Risks. The Company shall quantify its risks by employing techniques such as risk assessments, scenario analysis etc. Wherever measurement of risk is not possible due to complexity and non-availability of adequate data, qualitative approaches must be used with a view to transitioning to advanced approaches over time. The Company shall develop risk management policies with the view to ensure that at a minimum the above mentioned risks are efficiently managed.

3.4 Risk Mitigation and Control

As part of its risk management framework, Wapic would consider various control mechanisms to mitigate identified risks and to ensure compliance. Principal elements of the business operations will include:

- Clearly defined management responsibilities and accountabilities including documentation for approvals, setting limits, delegations and authorisations
- Activity and procedural controls for each division or department (e.g. segregation of duties)
- Policies to document such controls
- A system for monitoring compliance with controls
- Policies and procedures for treating and resolving non-compliance issues
- Mechanisms to ensure that all personnel have appropriate performance objectives, expertise and training with regard to relevant risks
- Regular verification and reconciliation of transactions and accounts
- Security of staff, premises, access to, and use of, the Company's assets and records (physical and electronic controls)

Risk control involves initiating corrective steps to address deviations from policy stipulations.

3.4.1 Risk Mitigation

Wapic shall cope with all the identified risks through effective risk decision to prevent further escalation of severity/frequency of the losses. The choice of the risk decision shall essentially depend on the effectiveness of the measure in reducing the probability and impact of a given risk and the cost and time involved in implementing the measure. The risk decision should be any one of the following or a combination that will result in an effective measure.

Selecting the most appropriate option involves balancing costs of implementing each treatment option against the benefits derived from it. Risk decision shall consider the values and perceptions of stakeholders and the most appropriate ways to communicate them. Risk decision may itself introduce new risks that need to be identified, assessed, treated and monitored.

3.4.2 Approaches to Risk Mitigation

3.4.2.1 Tolerate/Accept Risk

The decision to accept a risk should be based on the cost benefit analysis justification wherein the estimated risk (frequency & severity) could be less than the cost of risk mitigation. Acceptance of residual risks has to take place at the Management of the Company. Management shall monitor the severity of these risks on a yearly basis and revise their risk decision appropriately.

3.4.2.2 Transfer Risk

Risk transfer is critical tool for managing exposure to non-controllable sources of risk. Risk transfer is a means of exchanging unknown financial impact of specified events to a third party for a known financial cost. High risks which cannot be managed through internal controls could be transferred primarily through the following:

- Co-insurance
- Reinsurance
- Outsourcing

The risk appetite of Wapic shall be taken into account while implementing the risk transfer through insurance and outsourcing. The relevant business units with the assistance of the risk management function shall be responsible for identifying and incorporating the risks arising from such risk transfer arrangements in their risk registers. The business units shall also be responsible for managing the resultant risks and reviewing the risk transfer arrangement to ensure that it is still capable of mitigating the initial risk.

3.4.2.3 Treat Risk

All possible controls that will enable prevention of losses or reduction in the impact/probability of loss occurrence shall be implemented as part of risk treatment for the identified risks. New/additional internal controls shall meet the desired objective and shall be approved by the ERMC. The Risk Management function shall review and ensure adequacy of process documentation and shall conduct regular tests to ensure effectiveness of the controls.

3.4.2.4 Avoid Risk

In the event where the cost-benefit analysis proves that the benefit margin is less than the risk cost considering all types of risk, Wapic shall opt for avoiding such risks. However, the decision to discontinue the activity shall be approved by ERMC taking into account the strategic objectives of the Company.

3.5 Risk Monitoring and Reporting

3.5.1 Risk Reviews

A risk review involves the re-examination of all risks recorded on the risk treatment plan to ensure that the current assessment remain valid and to review the progress of risk reduction actions. Risk reviews shall form part of normal management reviews. Internal Audit and External Auditors shall carry out regular reviews of the risk management process to evaluate the risk identification and assessment process, evaluate the effectiveness of implemented controls and the quality and appropriateness of all risk mitigation action plans. This will form part of the updates into the risk treatment plan. Risk actions and any associated risk budget should be reviewed every financial year and updated in the risk treatment plan.

3.5.2 Risk Reporting

The ERM reporting system will provide the reporting of enterprise-wide risks, along with drilldown capabilities so that all key risks can be monitored simultaneously. The ERM reporting system will include the following attributes:

- Provide a single point of access to all critical risk information that arises from various risk streams and business units across the insurer
- Timely delivery of accurate risk information to the top management
- Integration of quantitative KRIs, qualitative risk assessments, policy documents, and external market data

To ensure an effective risk management process, reports containing information on the risk profile of the firm, adherence to risk policies, changes in the external environment and their impact on the Company's strategy and risk management practices shall be communicated by the CRO to Management on a monthly basis and to the Board quarterly.

3.6 Structure of Risk Reports

Structure of Risk Reports shall include the following:

- Description of reports
- Contents and coverage of reports
- Function/ Division responsible for production of reports
- Recipients of reports
- Periodicity of reporting

3.7 Coverage of Risk Reporting

Risk Reporting shall cover the following:

- Risk Aggregation and Identification
- Risk Monitoring and Control
- Deviation and Exception

No.	Report Description	Contents of the report	Coverage of the Report	Function/ division responsible for generating of reports	Recipient of reports	Periodicity of Reports
I	• Risk Aggregation					
1.	Integrated Risk status Report	Report on summary of all risks assumed by Wapic in comparison to capital available, risk appetite and limits	This report will give the sum of unexpected loss faced by Wapic in all the risk streams and also highlight the material risks. (It will reflect both individual and aggregate risks)	CRO / Risk Management	BERMGC /Board	Monthly
2.	Trend Analysis Report	Report on the direction of movement of risks assumed by Wapic as compared to the previous reporting period	This report will present the trend analysis of all risks faced by Wapic. Comparison will be done on a monthly basis. (During every quarter, half year and year end – report will furnish quarterly, half yearly and annual trend along with the monthly trend)	CRO / Risk Management	BERMGC /Board	Monthly
II	Risk Monitoring and Control					
1.	Integrated Risk monitoring and control Report	Report on summary of risk monitoring and control activities of Wapic	This report will give the details of significant risk monitoring and control activities of Wapic (significant risk issues in Wapic and risk transfer strategies) from all the risk streams.	CRO / Risk Management	BERMGC /Board	Quarterly
2.	Report on response to issues raised by internal audit	Recommendations/ response by Board Audit & Compliance Committee (BACC) / BERMGC	This report will give the response and recommendations of BERMGC for the comments given by Internal audit on risk management	BACC / BERMGC	Board	Quarterly
III	Deviation and exception					
3.	Deviation and exception reports	Report on summary of deviations and exceptions to the	This report will give the details of significant deviations and exceptions to the	CRO / Risk Management Units	BERMGC /Board	Monthly

No.	Report Description	Contents of the report	Coverage of the Report	Function/ division responsible for generating of reports	Recipient of reports	Periodicity of Reports
		policy guidelines along with details of approval authority	policy guidelines (from all the risk streams) and action taken by the Risk Management unit during the reporting period			
4.	Deviation and exception reports – Cumulative	Report on summary of deviations and exceptions to the policy guidelines along with details of approval authority	This report will give the details of significant deviations and exceptions to the policy guidelines (from all the risk streams) and action taken by the Risk Management unit cumulative since the beginning of the financial year till the reporting period	CRO / Risk Management Units	BERMGC /Board	Monthly
IV	Integrated Stress Testing					
5.	Plausible Scenarios for stress testing.	1. Plausible Scenarios chosen. 2. Impact of scenarios on Risk measures at Portfolio level.	This report will contain consolidated details of stress testing scenarios simulated by the Risk Management Unit	CRO / Risk Management	BERMGC /Board	Quarterly
6.	Remedial Actions (Stress Testing)	Remedial actions taken against identified stress scenarios.	The report shall list out the remedial actions against the identified stress scenario for all the risks faced across Wapic	CRO / Risk Management	BERMGC /Board	Quarterly
V	Capital Allocation & Risk Adjusted performance					
7.	Report on capital allocation and Risk Adjusted performance	Report on current level capital allocated and Risk adjusted return on capital (RAROC) from business units	This report will contain the details of current level capital allocated and Risk adjusted return on capital (RAROC) from business units for the reporting period	CFO / FINCON	ERMC / BERMGC	Monthly/Quarterly

4 Insurance Risk Management

4.1 Definition

Insurance risk is the risk of loss arising out of inadequate or failed re-insurance program, inefficient claims management or weak underwriting system.

Insurance risks are the risks inherent in the systems and controls in the management of an insurance business.

Insurance risk types include but not limited to:

Underwriting risk: The risk inherent in the systems and controls surrounding the underwriting process which may bring about an unexpected loss that threatens the solvency of the Company

Claims risk management: This is the risk of failure of the claims settlement process. It is the risk that the Company may be unable to manage the claims settlement process by which it fulfil its contractual obligations to policy holders

Reinsurance risk: This is the risk of inadequate reinsurance cover which may be triggered by insolvency of a re-insurer or exhaustion of reinsurance cover through multiple losses

Reserve risk: This is the risk that insurance liabilities will be inadequate to meet the claim amount payable when such liabilities crystallize

4.2 Objectives of Insurance Risk Management

The objectives of insurance risk management at Wapic are as follows:

- Avoid potentially large or catastrophic risk losses and or reduce other losses arising from inadequate or failed internal processes, people, systems and external events associated with insurance underwriting, claims management and reinsurance
- Enhance controls of insurance management process through improved understanding of risk activities within various business units
- Provide early warning signals of any deterioration in the Company's internal control system in underwriting, claims, and reinsurance departments
- Enable an improved performance measurement system through appropriate allocation of risks and capital

4.3 Insurance Risk Management Process

To effectively manage its insurance risk, Wapic shall establish and follow the process of identifying, assessing, mitigating, controlling, monitoring and reporting insurance risk.

4.3.1 Underwriting Risk Management Process

Underwriting is the process by which the Company makes an assessment of the risks to be accepted and determines the terms on which the risks would be acceptable to the insurer.

4.3.1.1 Risk Identification and Measurement

Wapic shall consider the implications associated with selecting, accepting and retaining risks which may deviate from what was envisaged during the product development and pricing stages. Such risks may include:

- accepting risks without imposing adequate loading or conditions
- accepting risks which should have been declined given the Company's risk tolerance
- accepting and retaining risks in excess of the resources available to Wapic (risk accumulation)
- accepting lives/risks whose experience is worse than that envisaged when pricing the product

4.3.1.2 Underwriting Risk Control and Mitigation

Wapic shall have clearly documented underwriting guidelines for each of the key types of products it underwrites so as to provide sufficient guidance to the Underwriting Unit. The guidelines will also include when Underwriters should refer to the Reinsurer for underwriting support.
The guidelines shall include but not limited to:

- business objectives
- risks selection criteria
- rating factors
- declined risks
- reinsurance limits

4.3.1.3 Underwriting Risk Monitoring and Reporting

Wapic shall conduct regular reviews to ensure that the Underwriters continue to be competent in the area of their delegated authority and the quality of the underwriting decisions made remains satisfactory.

The Risk Management function shall develop an approach to monitor the risks across product types so that the overall risks underwritten by the Company are always within its retaining protection limits and risk appetite.

The function shall conduct spot checks of underwriting files regularly. These reviews should be conducted with clear and pre-defined terms of reference – for example, to check for adherence to underwriting guidelines or underwriting authorities. There should also be an appropriate system to select the files to be reviewed. In addition, the risk function shall also monitor risk indicators and periodically report to the Board and Management

4.3.2 Claims Risk Management Process

4.3.2.1 Claims Risk Identification and Measurement

The Company shall put in place measures to identify the risk associated with poor claims handling and claims reserving, which may include:

- making claim settlement decisions which are not in accordance with the policy terms and conditions, thereby either incurring liability that is not considered in the pricing or failing to fulfil its contractual obligations to policyholders
- inefficient handling of claims leading to slow responses or higher cost overheads, thereby impeding its market competitiveness
- setting inadequate reserves, or delay in revising claims reserves for reported claims resulting in under provision of claims liabilities and time lag in adjusting premiums for new policies in the case of general business

4.3.2.2 Risk Control and Mitigation

Wapic shall have a clear process in place for the notification of claims by the intermediaries or the policyholders. The process shall ensure that all claims are reported to the Company at the earliest opportunity and that relevant information is captured in the in a timely manner.

4.3.2.3 Risk Monitoring and Reporting

The Risk Management function shall conduct regular reviews to ensure that the personnel responsible for claims continue to be competent in their field. The function shall also conduct reviews of claim files regularly. These reviews shall be conducted with clear and pre-defined objectives – for example, to check for adherence to claims settlement authority limits or to assess the adequacy of the claims reserves set, or that case reserves are reviewed and revised on a timely basis.

Wapic shall have in place regular claims reporting to Management and Board so as to raise awareness of key claim exposures and losses, especially where a single claim, loss event or series of losses could in aggregate have an impact on its balance sheet.

4.3.3 Reinsurance Risk Management

4.3.3.1 Reinsurance Risk Identification

Wapic shall analyse its risk profile in conjunction with the legal, economic, social and political environment in which it operates, to identify the potential sources of risk and estimate the probability and consequence of each risk. The risks include but not limited to:

- **Underwriting Risk**

The Company shall decide on what and how much risks to retain, taking into consideration its risk appetite, and the availability and cost of reinsurance. It shall identify the source and magnitude of concentration of risks and assess the impact of likely adverse events.

- **Legal Risk**

Another material risk faced by the Company, is the risk that the contract wordings do not accurately reflect the intent for the purchase of the reinsurance cover or the contract is not legally enforceable.

- **Credit Risk**

The Company also faces credit risk arising from potential defaults by its reinsurers as it is contractually obligated to pay all claims in respect of the underlying policies in full.

- **Liquidity Risk**

Wapic is exposed to liquidity risk in the event of large losses whereby it may have to pay the claims prior to receiving all the reinsurance recoverables.

4.3.3.2 Reinsurance Risk Assessment

The Company shall assess the impact of likely adverse events through stress testing and realistic disaster scenario analysis to ensure that its catastrophe reinsurance cover can be relied upon to reduce the impact of most conceivable calamities to a magnitude that will not threaten its viability.

4.3.3.3 Reinsurance Risk Control and Mitigation

In designing a reinsurance programme to mitigate risk, the insurer shall take into account the following relevant factors:

- business plan and strategies
- underwriting philosophy and capabilities

- size and profile of each line of business
- frequency and size of loss by line of business
- financial strength

Wapic shall ensure its reinsurance contracts cover applicable lines of business and the limits of cover are adequate for the size of its business operations. The terms, conditions and exclusions stipulated in the reinsurance contracts shall also be aligned with those of the underlying business.

The Reinsurance unit shall put in place appropriate systems and processes to facilitate achieving contract certainty, including prompt commencement of review of the reinsurance programme and vetting of contract wordings.

The Risk Management function shall develop criteria for the selection of reinsurers and outline the information that is required to assess the financial soundness of a reinsurer. In case of exceptional circumstances that merit a deviation from the original approved limits, the endorsement of the appropriate approving authority shall be obtained.

4.3.3.4 Reinsurance Risk Monitoring and Reporting

The Risk Management function shall monitor that only approved reinsurers are used and track aggregate exposures to individual reinsurers against exposure limits established. It shall also monitor the outstanding balances from its reinsurance counterparties and the credit standing of its approved reinsurers on an ongoing basis.

The function shall report to Management and Board on reinsurance performance measures to ascertain the effectiveness of its reinsurance counterparties. Such measures include:

- amount and ageing of reinsurance recoverable
- amount of doubtful debts and write-offs

The Reinsurance unit in collaboration with the Risk Management function shall also review and report on whether its reinsurance programme has, over a period of time, supported its business objectives and strategies, and helped to mitigate its losses to within its risk tolerance level.

5 Operational Risk Management

5.1 Definition

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal and excludes strategic and reputational risks. Examples of these risks and their associated losses include fraud/forgery, poor accounting and lapses in financial control, legal settlements involving significant payments for losses alleged to have been caused by the Company.

Operational risk shall be categorised as follows:

- Internal process risks: are associated with breakdowns in established processes and controls, failure to follow processes and controls, the absence of a process or control or the inadequacy of a process or control within business lines
- People risks: are operational failures driven specifically by factors attributable to the behaviour of staff; for instance, lack of experience, inadequate supervision and a poor control environment. Examples of people risks include: negligence, intentional circumvention of established controls etc.
- System risks: are associated with system failures arising from the breakdown, interruption and/or physical loss or damage to a computerised processing system. Examples of system risks include power failures, slow or failed internet connection that impede trade execution, data theft, theft/damage of hardware/equipment, virus attacks etc.
- External risks: are risk events outside the control of the Company and they include natural disasters, acts of terrorism and other natural and man-made disasters

5.2 Objectives of Operational Risk Management

The objectives of operational risk management at Wapic are as follows:

- Loss reduction : To minimize losses arising from operational risk events
- Process/Control improvements: To improve the design and implementation of controls in business processes

5.3 Operational Risk Management Methodology

This section outlines the Company's operational risk management methodology and procedures to be adopted for operational risk identification, assessment, measurement, control, reporting and monitoring.

5.3.1 Operational Risk Identification

Wapic shall adopt the following qualitative and quantitative techniques for the identification of operational risk events:

- Risk Assessment – this qualitative risk identification technique will be applied in all business functions
- Other sources of operational risk events:
  - ✓ Actual internal loss experiences
  - ✓ Business planning document
  - ✓ External data (where relevant and available)
  - ✓ Scenario analysis by subject matter experts
  - ✓ Internal and external audit reports
- Risk indicators – to monitor the level of risks continuously

The Operational Risk Management function in conjunction with business units shall identify and assess the operational risk inherent in all material products, activities, processes and systems of the Company. The identification process shall specify the nature and types of operational risk, their causes and the likely impact on Wapic.

5.3.1.1 Key Risk Indicators

The Operational Risk Management function shall establish Key Risk Indicators (KRIs) for the Company as a whole and for individual business units. Furthermore, formal escalation triggers shall be defined as appropriate. Where KRIs cannot be established for a significant risk, an exception to this requirement shall be approved by the Chief Risk Officer.

5.3.2 Risk Assessment and Measurement

The Operational Risk Management function, business units and support functions shall assess all risks identified from the risk assessment process, mapping and external event brainstorming sessions to determine the extent to which the identified events may affect the achievement of the Company's objectives.

The risks identified shall be evaluated and rated for significance based on a combination of probability of occurrence and potential impact or severity. Each business unit shall assess the extent of residual operating risks in their business and rate them in line with the criteria established by the Risk Management function.

5.3.3 Risk Mitigation and Control

Appropriate controls shall be designed and documented for all significant risks and actions plans formulated to address weaknesses identified.

5.3.4 Operational Risk Monitoring and Reporting

5.3.4.1 Operational Risk Monitoring

To facilitate the process for monitoring and controlling operational risk within Wapic, results from the risk identification, assessment and measurement exercise shall be summarised and circulated to the relevant stakeholders to improve their understanding of the identified risks.

The Risk Management function shall develop policies and procedures on how the significant risks identified will be monitored including their associated indicators and controls. The function shall ensure that:

- there are adequate processes and procedures to control and mitigate the operational risks that have been identified
- control activities for the management of operational risks are an integral part of the regular activities of the Company, business units and support functions
- controls and systems are sufficient to mitigate the identified risk before they become major concerns

The CRO shall maintain a loss database for recording and analysing operational risk losses and near misses. The loss database shall contain the key data elements needed for operational risk measurement, management, and verification.

The monitoring process shall involve the analysis of trends and correlations between indicators, controls and losses. Trends in operational risk metrics using the key risk indicators and thresholds shall be monitored and exceptions reported to the appropriate levels of authority based on predefined escalation procedures.

5.3.4.2 Operational Risk Reporting

The Company's reporting of operational risk events shall incorporate the following:

- Delivery and sharing of relevant operational risk event information between the Risk Management, business units and support functions. This information shall primarily be data such as losses, near misses, key risk indicators and results of self-assessments. It shall be responsibility of business unit heads to ensure that all required operational risk data and information are reported into the loss database
- Business unit specific operational risk reports prepared by the Risk Management function and forwarded to the specific units. The reporting shall reflect aggregate and granular information designed to assist the business units to better understand and manage their operational risks

- Reporting of aggregate operational risk by risk category to the Board and Management to ensure a better understanding and management of operational risk

5.4 Outsourcing

The Company shall establish a policy to guide the outsourcing of functions and help manage the risk exposure in outsourcing contracts. The policy shall cover the following areas:

- Procedures for assessing whether and how identified activities can be appropriately outsourced and establishing the business case for outsourcing
- Scope and nature of services that should be outsourced
- Vendor evaluation and selection
- Procedures for monitoring the outsourced activities and the Risk's relationship with the service provider
- Establishment, monitoring and review of Service Level Agreements (SLAs)
- Roles and responsibilities for managing the outsourcing process
- Grievance resolution process
- Contract termination provisions

5.5 Business Continuity Management

The Business Continuity Management (BCM) plan shall consist of a set of identified policies, actions and processes necessary for the prevention, management and containment of business disruptions and crises.

The purpose of the Plan shall be to:

- Establish direction and accountability for Business continuity management
- Minimise disruption of service to customers
- Ensure the safety of the Company's employees and property
- Minimise financial loss due to disruptions
- Ensure timely resumption of normal operations in the event of a disaster

The Plan shall cover the following areas:

- A process for performing a business impact analysis of events that could lead to a major operational disruption and identifying critical operations and services, key dependencies and the ability of the Company to recover from the events
- Recovery strategies and pre-defined goals for recovering specified business operations and supporting systems to a specified level of service (recovery level) within a defined period following a disruption (recovery time) as well as the plan for ultimately resuming business operations

- A defined process for reporting to the Board and Executive Management on matters related to business continuity and crisis management
- Policies relating to business continuity and crisis management planning including well defined roles, responsibilities and authority to act, as well as succession plans
- Data back-up and recovery procedures
- Procedures for communicating within the Company and with relevant external parties in the event of a major operational disruption and comprehensive emergency communication protocols
- A process for testing the Business Continuity Management Plan (BCP), evaluating its effectiveness and updating it as appropriate
- Process for ensuring awareness, familiarity and understanding among key personnel of their roles and responsibilities in the event of a major operational disruption with respect to the BCP
- Clearly defined triggers and individuals responsible for activating the plan

5.6 Information Security

The Head of Information Technology (IT), in conjunction with the Risk Management function, shall be responsible for developing appropriate information security policies and procedures for the Company. The objectives of the policies and procedures shall be to ensure:

- constant availability of systems and information
- data integrity in the information systems and in the exchange of data internally and externally
- confidentiality of the data internally and externally
- protection of information assets against all risks (viruses, intrusion, theft and information manipulation)

6 **The Head of IT shall be responsible for reviewing and enhancing the Company's information security policies and procedures in line with leading practices for information security. The Risk Management function shall be responsible for testing and evaluating the implementation of the Information Security policies.**

7 Investment Risk Management

7.1 Introduction

Investment risk is the risk of loss (partial or full) of the principal amount and/or expected returns due to changes in the market variables. Wapic shall ensure that investment risk is managed effectively and on a proactive basis by developing and implementing investment risk management strategies policies and processes.

The Company will invest with a view to increasing and sustaining the wealth of its shareholders. The Company shall implement a sound investment risk management framework so as to minimise possible losses to capital and earnings arising from volatilities in market factors.
To ensure that the Company meets its objectives and goals, it shall implement an investment strategy, investment mandate and investment policy to guide the management of its investments.

7.2 Objectives of Investment Risk Management

The following are the objectives of managing investment risk in Wapic:

- Maintaining investment risk within risk limits in line with the Company's risk appetite
- Identify and accurately measure the investment risk to support information and decision analysis
- Mitigate and monitor the investment risk exposures effectively

7.3 Investment Risk Management Process

This section outlines the investment risk identification, measurement, control, monitoring and reporting process.

7.3.1 Investment Risk Identification

The Risk Management function shall review and identify risk factors, inherent in proposed investments that may impact the Company achieving its business objectives. The function in conjunction with the Treasury and Investment Unit shall develop strategies to manage identified risk factors.
The Risk Management function shall also conduct on-going review of investments to identify emerging risks that would impact negatively on the Company's investment objectives.
The risk identification process shall be carried at on an individual investment level and portfolio level. Risks identified shall be categorized based on the categories defined below:

7.3.1.1 Market Risk

Market Risk is the risk to Wapic's financial status arising from the adverse movement in market prices. Market risk involves the exposure to variables such as equity prices, interest rates etc. Market risk incorporates general market risk (on all investments) and specific market risk (on each investment). Market risk includes:

- **Interest Rate Risk**

Interest Rate Risk is defined as the risk of reduction in market value of an interest rate sensitive instrument or portfolio due to changes in interest rates.

- **Equity Risk**

Equity risk is the risk in fall of value of investments on account of changes in equity market prices.

- **Currency Risk**

Currency Risk refers to the risk to earnings and capital arising out of adverse movements in currency exchange rates.

- **Property Risk**

Property Risk is defined as the risk of financial loss to the Company from changes in the level or in the volatility of market prices of property.

7.3.1.2 Concentration Risk

This is the risk from lack of diversification in the asset portfolio, or from large exposure to default risk by a single issuer of securities or a group of related issuers

7.3.1.3 Sovereign Risk

Sovereign Risk is defined as the risk of loss experienced by a financial institution due to changing social, economic, or political factors specific to one country and can range from social or economic deterioration, political turmoil etc. All such events could reduce the Company's earnings or capital.

7.3.1.4 Macroeconomic Risks

Macroeconomic risks including geo-political risk, inflation/deflation risk, regulatory risk, and demographic risk. Macroeconomic risks are external, uncontrollable factors and may impact investment performance. These risks are also not all quantitatively measurable.

7.3.2 Investment Risk Assessment

Identified risks shall be ranked in order of priority using the probability of occurrence and impact rating scale as defined in **Section 3.2**.

7.3.3 Investment Risk Measurement

The Company shall measure its investment risk using a combination of the following techniques:

7.3.3.1 Portfolio Valuation

This involves the estimation of the fair value of the Company's portfolio. Positions with quoted market prices shall be marked to market whilst positions that cannot be marked to market shall be marked to model.

The Risk Management function shall have the responsibility for the valuation of the Company's portfolio.

7.3.3.2 Counterparty Risk Measurement

Counterparty risk is the risk that the counterparty will not perform on its contractual obligations.

7.3.3.3 Foreign Exchange Risk Measurement

The Market Risk Management function shall measure the sensitivity of foreign currency positions to a shift in the foreign currency rate as a means of measuring foreign exchange risk.

7.3.3.4 Interest Rate Gap Analysis

Interest rate gap analysis utilises the maturity or re-pricing schedules of balance sheet items (assets and liabilities) to determine the differences between maturing or re-pricing items within a given tenor. Interest rate sensitive assets and liabilities instruments are assigned to defined time periods on the basis of the earlier of expected re-pricing dates or maturity date.

The Market Risk Management function will measure the rate sensitivity position of the Company monthly, to ensure its long-term interest earning power. In addressing this, the ratio of Rate Sensitive Assets (RSA) to Rate Sensitive Liabilities (RSL) and the attendant gap (RSA minus RSL) to total assets will be reviewed based on the defined tenor buckets.

7.3.3.5 Sensitivity Analysis

The Company shall use sensitivity analysis to determine how much the investment portfolio value would change if there is a small change in one or all of the market risk factors. The market risk impacting the Company include:

- interest rates
- equity prices
- currency rates
- property prices
- other market variables

7.3.3.6 Tracking Error

This is a measurement of how much a portfolio returns deviates from the return on a set benchmark. The Company shall decide on an appropriate benchmark or hurdle rate, whilst the monitoring of portfolio returns vis-à-vis the returns of the rate shall be computed and reported regularly to the FIMC and Board by the Risk Management function.

7.3.3.7 Scenario Analysis

This measurement approach shall be used to assess the reaction of the Company's portfolio to stress events. It measures the impact of a simulation of stress scenarios that may affect several risk factors. The stress scenarios can be based on historical or hypothetical events.

The Risk Management function under the supervision of the CRO, shall be responsible for performing stress tests on the Company's investment portfolio. The appropriateness of the stress tests shall be reviewed annually by the FIMC and BFIC.

7.4 Investment Risk Mitigation and Control

The CRO shall seek to mitigate the risks in the Company's portfolio through the use of the following:

7.4.1 Limits

The Company shall use limits for setting boundaries for the level of investment risk it is capable of accepting. The limit system shall also ensure that positions that exceed the predetermined levels are escalated to Management for necessary attention. Wapic shall consider the following in developing and setting the limit system:

- Overall risk appetite/tolerance
- Size and complexity of the business
- Capital levels and capital requirements
- Regulatory requirements
- Profitability of business areas
- Liquidity of specific markets
- Volatility of markets
- Adequacy of risk management tools, systems and personnel
- Cash-flows
- Experience in the given sector
- Targeted risk-adjusted return

Wapic shall control its investment risk by establishing the following limits:

7.4.2 Exposure Limit

Exposure Limit (EL) reflects ceiling on a Company's exposure across any dimension such as industry, geography, sector, counterparty etc. to avoid risk of concentration. The Treasury and Investment Unit shall recommend ELs to the Board for approval while the Market Risk Management function shall ensure adherence to the approved ELs.

7.4.3 Risk Limits

Risk Limits shall consider the sensitivity and volatility of risk factors that are important for risk measurement apart from merely considering exposures.

The Market Risk Management function shall set RLs based on the important dimensions such as:

- Capital Market exposures
- Currency exposure
- Asset class level

7.4.4 Stop Loss Limits

Stop loss limits are the most essential for any investment activity. Stop loss limits are defined as limits set on losses in order to cut losses incurred in a security or portfolio. It defines the limit on single period market loss on a portfolio/asset class/security that should not be exceeded. Stop loss limit violation occurs when the single period market loss exceeds the loss limits set.

Risk taking units shall be responsible for ensuring adherence to the limits applicable to them whilst Risk Management function shall be responsible for monitoring adherence to these limits and escalating breaches in a timely manner where they occur.

7.5 Investment Risk Monitoring

Monitoring involves reviewing the effectiveness of the risk control and mitigation measures put in place with the aim of ensuring that activities relating to investment risk are performed as expected and that controls remain valid. The following shall be employed in the monitoring of investment risk:

- Economic and Market Review: The Company shall carry out a review of the economy and the market to ascertain their directions and impact on the performance of its portfolio
- Review of investment performance: The investment portfolio shall be reviewed and analysed in a bid to monitor how investment goals and objectives are being achieved. Any variance from investment goals and objectives shall be reported on a regular basis to the FIMC and Executive Management.
- Monitoring adherence to established limits and risk policies: The Market Risk Management function shall monitor adherence to established limits and risk policies. Unauthorized exceptions to risk policies and limits shall be escalated to the appropriate reporting function
- Monitoring of key risk indicators: The Market Risk Management function shall establish key risk indicators (metrics that indicate changes in the risk profile) based on the type of risk exposures

8.3.1.1 Identification of stakeholders

The divergence between the business conduct of the Company and the expectations of its stakeholders will potentially lead to reputation risk. Thus it is crucial to identify the stakeholders that will be affected by the performance and the conduct of Wapic. The Risk Management function shall identify its stakeholders groups and identify the clusters within each group.

Furthermore, in order to prioritise communications and prevent accidental reputational damage, stakeholders shall be mapped to key business units according to their degree of influence over and in the Company.

8.3.1.2 Identification and mapping of stakeholders expectations

Following the process of stakeholder identification, it is imperative to identify and document their expectations.

Business units shall identify:

- the expectations that the stakeholders have from them
- those parameters and values that make the Company better than its peers and it wants to safe guard

8.3.1.3 Identification of reputational risk drivers

The Company shall seek to identify understand the perception of stakeholders by identifying drivers that may impact its reputation. Examples of reputational risk drivers include:

- **Financial soundness and business viability**: This relates to the Company's financial track record and future prospects
- **Corporate governance and leadership:** This relates to the leadership of the Company (Board and Management) and their capability to run the business and manage risk
- **Management integrity**: This relates to the personal ethics and behaviour of the Company's Management personnel
- **Corporate Culture:** This relates to the collective values systems, beliefs and processes within Wapic
- **Corporate responsibility**: This relates to the Company's social, ethical and environmental impacts
- **Workplace talent and culture:** This relates to Wapic's work place culture, fair treatment of its employees, quality of staff and health and safety standards in place
- **Risk Management and Control environment:** This relates to the existence and effectiveness of the Company's risk management and control environment

9 Compliance Risk Management

9.1 Definition

Compliance risk is the risk of legal or regulatory sanctions, financial loss, or loss to reputation that the Company can suffer as a result of failure to comply with laws, rules and regulations, industry guidelines and codes of conduct applicable to its activities. Wapic is exposed to compliance risk as a result of the regulations it must comply with.

9.2 Compliance Risk Management Strategy

Wapic's strategy for the management of compliance risk is as follows:

- A healthy compliance culture through continuous training and education of staff and management on the statutory and regulatory requirement for the business
- Environmental scanning of the regulatory environment with a view to keeping up to date with regulatory compliance rules relevant to the business. Compliance risk would also be taken into cognizance in the evaluation of potential investments

9.3 Compliance Risk Management Process

9.3.1 Compliance Risk Identification

The Risk Management function shall develop a process of identifying the compliance risk universe, which involves the following:

- Identification and analysis of new laws and regulations
- Environmental scanning of the external regulatory environment

9.3.1.1 Identification and analysis of laws and regulations

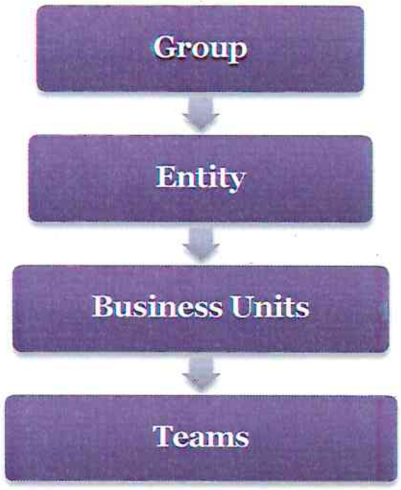
The Company shall facilitate the process of identifying the regulatory universe via building of an exclusive regulatory library (database of laws, regulations and guidelines) representing its compliance risk universe.

9.3.1.2 Environmental scanning of the external regulatory environment

The Risk Management function shall monitor changes in the external regulatory environment through environmental scanning. The main objective of this process is to ensure the early identification of possible changes in existing laws and regulations and devise processes for achieving compliance. Environmental scanning involves searching websites of regulators and actively participating in

12.3 RAPM Level of Application

For the purpose of assessing risk adjusted performance measures of Wapic, the assessment shall be done at the levels below;



12.3.1 Economic Capital

This is the capital the Company is required to have to support the risks it takes on at a specified confidence level. It serves as a cushion against potential large losses. It is a better reflection of actual risks embedded in the Company's business.

12.3.2 Optimizing the RAPM

Wapic shall optimize its RAROC and EVA through a revenue and cost optimization process. This optimization shall form the basis for allocating capital to entities, business units and teams in order to achieve the highest possible returns on all investments.

12.3.3 Internal Use

RAROC and EVA shall be one of the metrics used for performance measurement for employees in Wapic. The Company shall use the RAPM metrics to make strategic decisions on reallocating capital, diversifying its portfolio, adjusting its structure, rewarding employees and phasing out teams.

- **Legal and Regulatory compliance:** This relates to the level of Wapic's compliance with relevant laws and regulations and how proactive it is in anticipating and keeping pace with regulatory developments
- **Communications and crisis management**: This relates to the adequacy of the Company's communication and response during/to crises situation

8.3.2 Reputational Risk Assessment

In assessing reputational risk and its underlying drivers, Wapic shall ensure the assessment is performed based on the following:

- The assessment shall depend on both backward-looking and forward-looking analysis of reputational risk events
- The analysis shall comprise qualitative and quantitative measures, such as results from risk assessment, internal audit reports, media reports, reports from external auditors and reports from credit rating agencies

The Risk Management function shall leverage the output of these sources and assess the reputational impact of such risk occurrences or events.

The Company shall also seek to assess "the gap" between the stakeholder expectation and its performance by evaluating the expectation of the diverse stakeholder groups in relation to the reputational risk drivers.

8.4 Reputational Risk Control

The Company shall ensure that adequate measures (proactive and reactive) are taken to close identified gaps between its performance and stakeholder expectations. The personnel responsible for managing the expectations of the stakeholder group shall be responsible for implementing measures to either improve the performance of the Company or manage the expectation of the stakeholder.

8.5 Reputational Risk Monitoring

The CRO and the Head of Corporate Communications shall monitor the effectiveness of the risk response strategies and ensure that significant risks are:

- Monitored by the business units through risk assessments
- Subject to ongoing monitoring by the Enterprise Risk Management and Governance Committee

Due to the dynamic nature of stakeholder expectations, the Company shall continuously monitor changes in stakeholder expectations. This shall be carried using the following approaches:

8.5.1 Media Monitoring

The Risk Management function shall monitor press coverage of the Company in both the print and electronic media. References and news report on the Company shall be identified and analysed into any of the following categories: negative, positive and neutral rating.

8.5.2 Market Development Monitoring

The Risk Management function shall monitor industry, market, political, legislative or social developments which may have reputational risk implications on the Company.

8.5.3 Periodic Stakeholder Survey

The Risk Management function shall also conduct a systematic stakeholders' survey to assess stakeholder perception of the Company, determine its success in driving its reputation and identify the areas to be improved. This exercise may be performed directly or by proxy. Surveys will include but not limited to the use of the following:

- **Face-to face interviews** – This approach will be adopted where the stakeholder is ranked important, it is practicable to meet one-on-one with the audience, and interviews are considered the most effective way of determining the stakeholder's expectations e.g. major shareholders
- **Questionnaires** –This approach will be adopted where it is impracticable to meet one-on- one with the members of the stakeholder group and a sample of the population is considered a fair representation of the entire population

8.6 Reputational Risk Reporting

The CRO shall be responsible for consistently communicating reputational risk information across Wapic. The Risk Management function shall also be responsible for providing Board and Management with timely and accurate reports on reputational risk management.