Document Title	***Risk & Compliance Policy document***
Effective Date	2018
Policy No.	ARC-POL-001
Version	Ver.2
Document status	Final

1. COMPLIANCE POLICY

The Compliance Policy pursues our objectives in ensuring sustainability of our business by embedding governance, risk and compliance management into everything we do.

This policy and the wider risk management framework are designed to encourage a risk culture whereby outputs/compensation from the commercial activities are balanced against the risks in achieving them.

It also recognises the need for compliance with both internal and external compliance obligations and to ensure that a culture of compliance exists throughout the company.

The Compliance policy defines the lawful and proper conduct of the company's business including behaviour standards that Car & General Employees will observe as they carry out their work.

1.1. Scope

This policy applies to all employees (including internal contractors and consultants) and activities of Car & General.

1.2. Principles

- Promote a performance culture where we focus on our objectives and accept responsibility for recognising, communicating and managing the uncertainty (opportunities and threats);
- Promote an organisational focus on Governance, Risk and Compliance to support the business in effectively integrating governance, risk and compliance into business decision making and business processes.
- Understand and comply with our legal, regulatory and other obligations;
- Understand those risks that threaten the ongoing operation of Car & General, and have in place strategies to minimise business disruption.
- Meet the expectations of shareholders and stakeholders, through open and transparent communication;
- Execute timely decisions which create and protect business value having considered the best available information and taking account of uncertainty

1.3. Objective

Each employee is obligated to obey all applicable laws and corporate guidelines within their respective tasks and duties in his /her work for Car & General. This will include but not limited to;-

Comply with applicable laws and regulations; conform to internal rules

1. Conduct business fairly and in good faith, in keeping with laws, regulations, Car & General internal rules, policies, standard operating procedures and social norms.
2. Conduct work in keeping with internationally accepted norms to ensure our growth as a growing enterprise.
3. Comply strictly with domestic and foreign laws including laws regarding bribery and competition laws.
4. Keep corporate and personal interests separate (*and mandatory declaration)* to avoid conflict of interest.

Commitment to Company Values & Culture

1. Alignment of business operations and individual performance and goals to the company values.
2. Respect to basic rights, protection to employee health and treating each other fairly and without discrimination.
3. Organization commitment to providing a safe and enriching work environment for all employees.

Responsibilities of Top Management

1. The top management of Car & General Group shall take the lead to ensure that the business operates and is administered with the highest form of integrity and standards.
2. Cultivate the Car & General corporate culture where employees are empowered to innovate and foster excellence in their outputs including service delivery to stakeholders.

1.4. Reporting

All incidents and breaches of the law are to be reported to management and the Group Audit, Risk & Compliance Officer. These include:

- Breaches and non-compliances - where it is suspected or confirmed that Car & General has failed to comply with a requirement of a law or regulation; and,
- Non-conformances - where there are defects in systems, procedures and/or practices such that failure to rectify the situation could lead to a breach or non-compliance.

1.5. Risk Management

The Risk management function is responsible for providing guidance and tools to enable business units to manage their risk. In addition, report to the Audit & Risk Committee (ARC) and Board of Directors the company's risk & compliance practices.

Part of the reporting and assurance involves conveying the results of monitoring undertaken on business unit progress in implementing agreed treatments for key risks.

1.6. Internal Audit

Internal Audit facilitates good governance by reviewing the suitability and effectiveness of the Risk & Compliance framework, with findings and recommendations for improvement provided to the Management and ARC.

Internal Audit also conducts ongoing audits of compliance performance and programs established throughout the business.

2. RISK MANAGEMENT OPERATING PROCEDURE

2.1. Purpose

This Standard Operating Procedure has been developed to ensure robust processes in respect to the management of risk registers across the organisation.

2.2. Scope

A risk register is a management tool that enables an organisation, executive and or team to understand their comprehensive risk profile. It is a repository for all risk information. This repository is the hub of the internal control system, given that it should contain the objectives, risks and controls for the whole organisation.

It is through this process that risks are managed and is the process by which the organisation identifies, assesses and takes action to manage their risks. It is the responsibility of all staff throughout the organization to ensure that they fulfil their role in risk management

2.3. Terms and Definition

Standard operating procedure (SOP): An "SOP" is a set of written step-by-step instructions on how to enact each policy or perform each different activity in the work place.
Risk management: Risk management refers to the culture, processes and structures developed to effectively manage adverse effects and potential opportunities for any activity, function or process undertaken by the organization.

Risk: An event or set of circumstances, with an uncertain likelihood or outcome, which would have a negative impact. Any threat of an action/in action or event to our industry or activities that has the potential to threaten the achievement of our business and or departmental objectives.

Opportunity: An event or set of circumstances, with an uncertain likelihood or outcome, which would have a positive impact.

Likelihood: Likelihood measures the expected frequency of a risk occurring.

Consequence: Consequence measures the expected level of impact on the organization and its objectives, should the risk occur.

Risk owner: Risk owners are individuals within the company with primary responsibility for managing a particular risk.

Risk Assessment: A summary of the causes and consequences of a risk which include an initial risk rating, and potential courses of action.

Risk Register: Document recording identified risks.

Controls: Those measures already in place to manage risk.

2.4. Roles and Responsibilities

Roles	Responsibility
Board Audit, Risk & Compliance Committee (BARC)	• Enable oversight of the different Business Units • Manage enterprise risks from a country perspective and any country specific risk. • Meet quarterly as per the Audit Committee charter and complement the work of the Risk Governance Management Meeting (RGMM)
Head Audit, Risk & Compliance **Designate; Risk & Compliance Officer (RCO)**	• Ensure that RGMM meetings are held. • Accountable for the risk management process within the organization • Process owner for overall business risk process • Ensures annual review of risks • Ensures both Management Monitoring (Internal audits) and *Independent Business Monitoring (external audits)* schedule is in place and in use • Reviews findings for all audits within the businesses in scope and ensures that the appropriate Corrective and Preventive Actions (CAPAs) are in place and that the said CAPAs are closed in a timely manner
Head of Business (CEO – Group MDs – Per Country)	• Establish an appropriate risk management and compliance infrastructure within the business unit • Chair the RGMM Meeting • Appoint risk management process owner • Ensures timely and appropriate reporting and escalation of risks to the BARC
Head of Department (HOD) / Risk Owner(RO) - BLs	• Identify risks within their area of responsibility • Accountable for individually identified risks and their overall mitigation • Create and implement risk mitigation plan and ensure internal controls are implemented • Assess risk mitigation plan for effectiveness, at least once a quarter • Manage and ensure risk mitigation plans are completed by due date
Risk Governance Management Meeting (RGMM)	• Ensure appropriate risk management and implementation of internal controls for relevant Principal Risks within their scope of accountability. • Assign risk owners for each applicable Principal Risk and align their activities to support enterprise risk strategies. • Review each applicable Principal Risk at least once a year.

	• Meet at least quarterly to review mitigation of applicable risks and discuss emerging risks in the external or internal environment.
	• Establish a framework for ensuring risk management is embedded throughout the organization, i.e.
	  o Supported by other RGMM's as appropriate e.g. within other Local Operating Companies and Branches.
	  o The framework includes a mechanism to ensure that employees take accountability for identifying and escalating encountered risks so they can be appropriately managed.
	• Consider business environment and discuss potential new risks
	• Enter significant risks into business unit risk register
	• To support implementation of Enterprise Risk Strategies
	• Prioritize risks for review / mitigation
	• Review risk scorings
	• Review departmental registers and progress of mitigation plans versus priority list
	• Agrees on Audit schedules for both Management Monitoring (Internal audits) and *Independent Business Monitoring (external audits)* schedule
	• Reviews findings from all audits
	• Tracks the closure of CAPAs arising from audits conducted on the businesses in scope
	• Implementing organization's internal control framework

Risk Champions (BL or his assignee)	• Provide a status update on the Department Risk Register at monthly review with Risk & Compliance officer or Designate • Supports their respective HODs in updating the departmental risk registers and following up on risk mitigation plans • Support identification, assessment, verification and management of Risk Registers

2.5. Internal Control Framework

The Internal Control Framework (ICF) is a reference point that will enable the organizations to effectively and efficiently adapt to changing business and operating environments, mitigate and manage risks to acceptable levels, and support sound decision making and governance of the organization.

Elements of the framework are as follows:

1. **Risk Assessment:** Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. It is a pre-requisite to establish a reference point for controls. It identifies all reasonable areas of scope and then assesses the impact and likelihood of potential risks.

2. **Written Standards** are formal company policies, standard operation procedures, and guidelines (collectively called 'control documents') that communicate the ideas, rules, controls and expectations of the organisation. The objective is to establish in-process controls to ensure a process is actually happening as intended.

3. **Training** is provided to ensure staffs operate competently in whatever activity they undertake.

4. **Communication:** Managers need to be able to articulate to their teams the importance of each part of the framework in a relevant and engaging way aligned to our Values and encourage an open culture. Managers must also implement a process to receive complaints or questions and protect whistle-blowers from retaliation.

5. **Management Monitoring (Internal Audit):** The departmental managers are accountable for the controls in their area. Management monitoring is an ongoing process of assessing that the controls are in place, in use and effective. Monitoring can be conducted in many ways including but not limited to workplace observation of tasks, checklist activity inspection, and desktop review of data or documentation.

6. **Responding to Problems:** Failures and problems offer an important opportunity for learning and improvement. By understanding and correcting the root cause, they should not recur and thus the overall control framework is strengthened. Deliberate violation of policy, law or ethical codes threaten the Company's reputation and these need to be investigated.

   Detected issues that are not properly addressed can result in a range of undesirable outcomes, including reputational and/or legal risk, as well as fines and penalties. As a result, it is imperative that managers have a process in place to investigate items on a timely basis to establish if a violation has occurred.

   Additionally, investigative activity should be thoroughly designed to ensure that the root cause of the problem is determined. If the investigation concludes that a violation has occurred, an appropriate action plan should be put in place to remediate the issue.

7. **Discipline and enforcement:** generally refers to undertaking appropriate and consistent disciplinary action across the company for violations of policy or code of conduct.

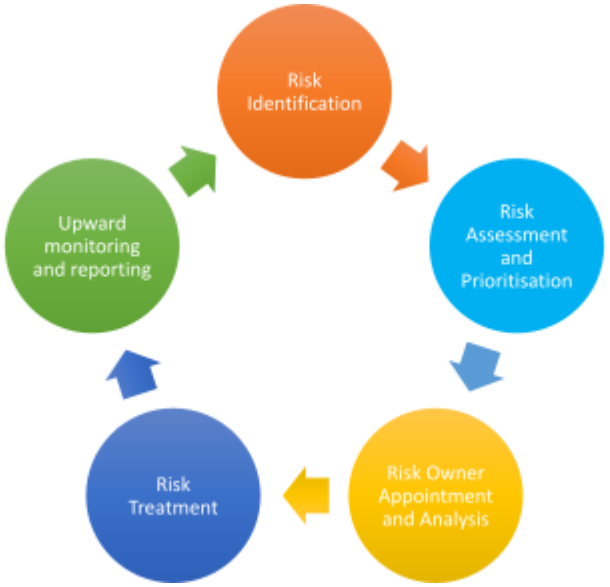
8. ***Independent Business Monitoring (External Audits):*** This activity is to be performed by a person or group independent of the activity being monitored, e.g. external auditors and or managers conducting regular reviews of activities, and deviations in order to continuously improve the operations, systems and processes. This review gives leadership objective evidence that the overall set of controls are effective, based on an understanding of current information.

   It provides an assessment of management effectiveness at risk identification and mitigation. It also assesses the overall effectiveness of the local control framework.

3. RISK MANAGEMENT PROCESS

It is important to recognise the 5 Step Car & General Risk Management process as a continuous cycle, with risks being identified, assessed, prioritised, analysed, and treated, with communication and upward reporting to the appropriate governance meetings, and where necessary escalation to the next level of governance e.g. BARC board.

Risk Management is an ongoing activity with new and emerging risks being identified based on changes in the internal and external environment, and existing risks being managed based on their significance to the business.



3.1. Risk Identification

The objective of Risk Identification in the Risk Management process is to develop a comprehensive list of risks whether or not they are under the direct control of the business or organisation.

Risks can be identified from a number of sources including a review of strategic business plans, audit results, a review of business processes, customer feedback or complaints, and data analysis for trends.

The output is a list of risks and their causes and effects, written in the form of a risk description

3.2. Risk Assessment and Prioritisation

This step requires one to assess the comprehensive list of risks developed in risk identification and prioritise them in a logical manner based on the impact and likelihood of the identified risk occurring. This needs to take into account the current level of control.

The treatment for the risks may also be determined at this step.

3.2.1. Risk Scoring

The identified risk is quantified on the likelihood of the risk occurring and the severity of the consequence of the risk.

To calculate the **Risk Index Value (RIV),** determine what the consequences would be if the risk was to materialise and then think about the likelihood of the risk. The risk score is calculated by multiplying the consequence and likelihood.

Likelihood Index Scoring

Rating	Based on Annual Frequency		Based on Annual Probability of Occurrence	
	Descriptor	Definition	Descriptor	Definition
5	Very frequent	More than twenty times per year	Almost certain	>90% chance of occurrence
4	Frequent	Six to twenty times per year	Likely	65% to 90% chance of occurrence
3	Reasonably frequent	Two to five times per year	Reasonably possible	35% to 65% chance of occurrence
2	Occasional	Once per year	Unlikely	10% to 35% chance of occurrence
1	Rare	Less than once per year	Remote	< 10% chance of occurrence

Consequence Impact scoring

Rating	Descriptor	Definition
5	Catastrophic	· Financial loss to company in excess of Kshs. 1 billion · International and regional long-term media coverage · Widespread employee morale issues and loss of multiple senior leaders · Required to report incident to authorities, resulting in significant sanctions and financial penalties
4	Major	· Financial loss to company between Kshs. 10 million and Kshs. 1 billion · National, long-term media coverage · Widespread employee morale problems and turnover · Required to report incident to authorities, resulting in sanctions against company
3	Moderate	· Financial loss to company between Kshs. 1 million and Kshs. 10 million · Short-term, regional or national media coverage · Widespread employee morale problems · Required to report incident to authorities and take immediate corrective action
2	Minor	· Financial loss to company between Kshs. 100,000 and Kshs. 1 million · Limited, local media coverage · General employee morale problems · Incident is reportable to authorities, but no follow-up
1	Incidental	· Financial loss to company less than Kshs. 100,000 · No media coverage · Isolated employee dissatisfaction

		· Event does not need to be reported to authorities

3.3. Risk Owner Appointment and Risk Analysis

Each risk should have a risk owner appointed. The Risk Owner is accountable for ensuring that the risk is managed in line with any Car & General strategy. The Risk Owner is accountable for:

- Ensuring that the risk is appropriately analysed
- Confirming the causes and effects identified
- Determining the current state of the internal controls and management processes in place.
- To ensure that there is accountability for any specific actions resulting from decisions of how to treat the risk.
- To ensure that the risk treatment plan is carried out according to the plan's timeline.

Risk Analysis includes assessing the effectiveness of the internal control framework against the identified risk and to ensure required controls are effective and are in place.

3.4. Risk Treatment

The purpose of this process is to assign an appropriate risk treatment measure for each identified risk. Treatment options include:

1. **Treat:** Also to **mitigate** the risk involves the implementation of a series of actions designed to reduce the consequence or impact associated with a risk. To reduce the likelihood by improving management controls and procedures. Reduce the consequence by putting in place strategies to minimise adverse consequences, e.g. contingency planning, Business Continuity Plan, liability cover in contracts.

2. **Transfer:** involves transferring the weight or the consequence to another party. Shifting responsibility for a risk to another party. A risk can be transferred as a whole or shared e.g. Insurance or business partnership.

3. **Terminate:** Also to Avoid the risk. This generally involves not doing an activity or preventing the exposure in order to avoid the risk involved, i.e. by deciding not to proceed, to eliminate or not continue with the activity or choosing an alternative approach to achieve the same outcome. The aim is risk management, not aversion.

4. **Tolerate:** Also to **Accept**. It is the decision made to take no action to reduce consequence or likelihood of a risk occurring. Controls are deemed appropriate. These must be monitored and contingency plans developed where appropriate.

3.5. Risk Register

The risk register also referred to as Risk Log will be the master document where all risks shall be managed. All department/functional units will have specific risk registers outlining functional risk. The risk register will be continuously updated and monitored.

4. MONITORING & REVIEW OF RISKS AND RISK REGISTERS

4.1. Monitoring Risk Registers

The objective is to ensure that principal risks are being monitored and all actions and treatment plans are on track and are reviewed and approved by the governance board (RGMM).

- Risk owners to review departmental risk register regularly to ensure completed actions are updated by due date.
- Risk Champion/s to provide an update on new or emerging risks at the monthly review meetings with RCO
- **All risks must remain on the risk registers for 3 years after closure of the risk.**
- RGMM to review the mitigation plans for effectiveness.
- RGMM to review RIV and assign mitigated index value (MIV) after completion of the mitigation plan.
- RGMM to perform an After Action Review on all risks with a RIV >10 to ensure the controls implemented are effective

4.2. Visibility & Procedure for Making Changes

- The Risk Register shall be available for employees to view on a Shared platform/folder
- A Compiled working version of the Risk Registers shall maintained by the RCO
- Any proposed changes to the risk register will be approved by the RGMM. The Risk Owner will notify the RCO or Designate to include it in the agenda for the next RGM meeting discussions.
- The RGMM member of the department initiating the change shall table the proposed change before the meeting and seek the input of other members
- After the RGMM's input, the initiator will make the relevant update on the departmental risk register based on the decision at the RGM meeting.
- The shared folder is to be updated on a regular basis by the Risk & Compliance Officer or Designate

4.3. Escalation of Risk

The Heads of Business is responsible for;

- Attending the respective Board Meeting
- Escalate significant risks in their respective business units to the Audit Board

4.4. Monitoring of Risk Management Process

The RGMM monitors the effectiveness of the risk management processes continually for the purpose of;

- Detecting and managing new risks
- Identifying the significant risks
- Implementing risk mitigation plans
- Monitoring and continually reviewing all risks (both existing and new)
- Keeping managers and stakeholders informed
- Effectiveness of escalation
- Ensure that the risk registers are current
- Reducing reactive behaviour by focusing on proactive anticipation and prevention

Legal Risk

All legal risks must immediately be escalated to the Legal Counsel.

5. TRAINING

All staff will be trained on this procedure. They will include; RGMM members, Country Leads, Business Risk Owners, Risk Champions and other members identified by the RGMM.

Revision History

Date	Version	Authored by	Reviewed and checked by;	Approved by	Reason for revision
05.01.2022	02	Costa Cherutich- Head of Internal Audit			To update the risk scoring methodology