POLICY ON RISK MANAGEMENT AND INTERNAL CONTROLS

Table of Contents

1. Objective

The Objective of the policy is to provide a framework for the management of risk and increase overall awareness of risk throughout Softlogic Capital PLC.

The policy will help for risks to be prudently identified, analysed and managed in accordance with the principles for managing risks set out at Softlogic Capital PLC.

This document also sets the context in which Enterprise Risk Management is applied at Softlogic Capital PLC and provides information on the risk architecture, processes and procedures, standards, roles, responsibilities, tools, facilities and documentation to be produced in this regard.

2. Establishing the Context

Before we consider risk management, it is necessary to identify the strategic and organisational context under which Softlogic Capital PLC operates. This will enable to:

- Articulate the Company's organisational objectives.
- Define external and internal parameters to be taken into account when managing risk.

Context for risk management at Softlogic Capital PLC is set, but not limited to the following basis;

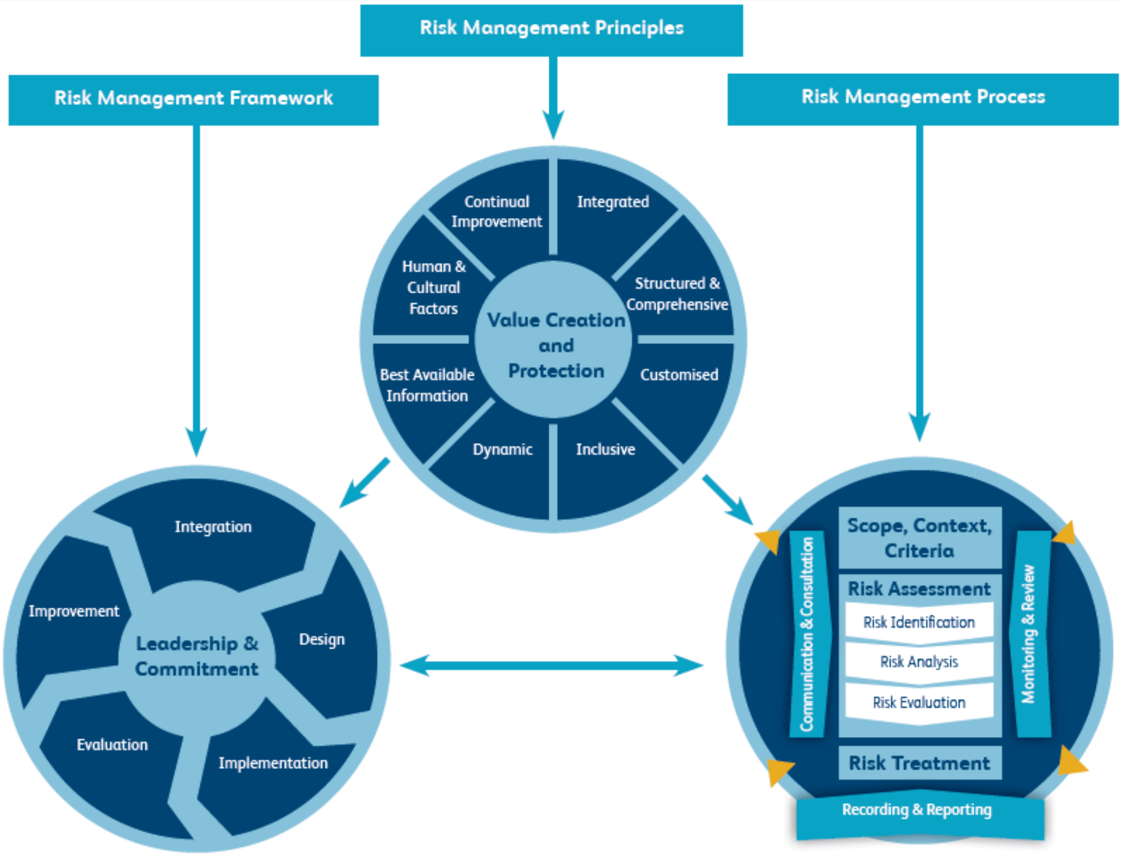
Environment	Definition	Consideration
Idiosyncratic Environment	Anything within Softlogic Capital that can influence the way in which risk will be managed.	• Organizational structure, roles and accountabilities • Vision, Mission and Values of the Company • Governance Structure • Distribution Channels • Product Composition • Demography of Customer Base • Geographic Dispersion of Branch Network • IT Infrastructure • Organizational Culture • Human Capital • Third Party Vendors Agreements/ Relationships
Systematic Environment	External environment in which Softlogic Capital seeks to achieve its objectives	• Impact from Global economic scenarios • Economic environment • Political Environment • Technological changes • Industry changes • Competitor threats • Legal and regulatory requirements • Social, cultural and demographical changes • Relationship with, perceptions, concerns and values of external stakeholders (e.g. Suppliers, Partners, etc)

3. Enterprise Risk Management Principles and Framework

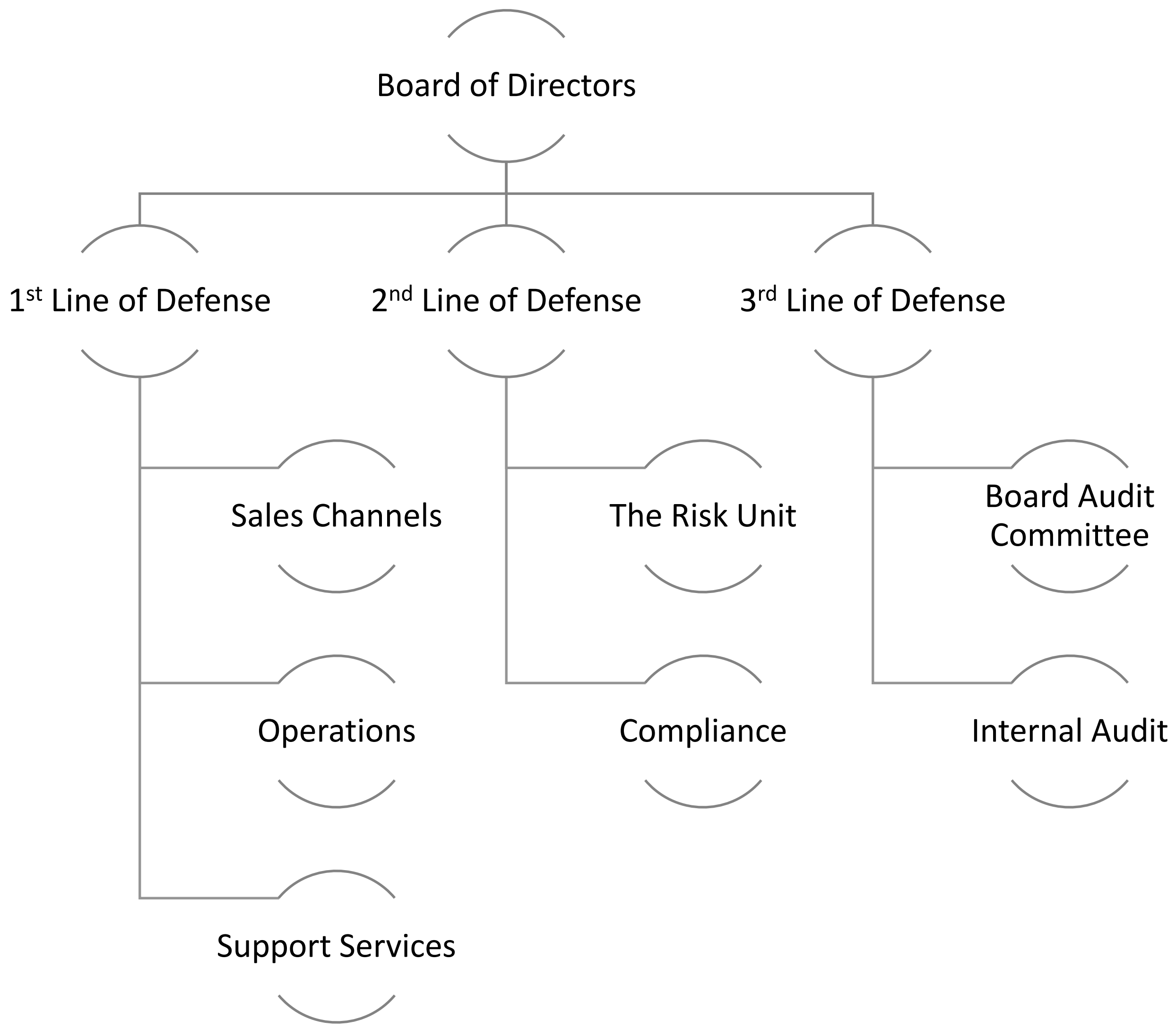
The design of the ERM framework at Softlogic Capital PLC is based on the ISO 31000:2018 International Standard. ISO 31000 states that the purpose of risk management is the creation and protection of value and is based on a total of eight principles as detailed below;

Principle	Description
Integrated	The organization integrates risk management in all of its activities
Structured and Comprehensive	The risk management is established upon a structured and comprehensive approach.
Customised	Risk management is linked to organizational objectives and is tailored to fit the organizations context
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organisation.
Inclusive	Risk Management includes the necessary stakeholders and takes into account their knowledge, views and perceptions
Dynamic	Considering both internal and external changes happen, risk management is able to detect and respond to those changes appropriately
Best Available Information	Risk management accounts for any limitations and uncertainties regarding the provided historical and current information future expectations
Human Cultural Factors	Both human behaviour and culture influence heavily the risk management, therefore these two characteristics are taken into account in all aspects of risk management
Continual Improvement	The organization's risk management is continually improved

Based on the above principles, the framework and process is derived; which works as the foundation of the architecture and processers established at Softlogic Capital PLC.


Risk Management Principles
Risk Management Framework
Risk Management Process
Continual Improvement
Integrated
Human & Cultural Factors
Structured & Comprehensive
Value Creation and Protection
Best Available Information
Customised
Dynamic
Inclusive
Integration
Improvement
Leadership & Commitment
Design
Evaluation
Implementation
Scope, Context, Criteria
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Risk Treatment
Communication & Consultation
Monitoring & Review
Recording & Reporting

4. Risk Governance Structure at Softlogic Capital PLC



5. Architecture of the Risk Management Unit

The Risk Unit comprises dedicated pillars to identify and assess risks pertaining to the areas concerned. The pillars specified are governed by category specific policies, which details the various methodologies and risk limits set in each of these areas.

The Policies governed by the Risk Unit under each pillar of risk are as follows;

Market & Investment Risk	Treasury Middle Office Policy
	Asset and Liability Management Policy
Operational Risk	Operational Risk Policy
	IT Risk Management Framework
	Fraud Risk Policy
Business Continuity	Business Continuity Plan
	IT Disaster Recovery Plan
Strategic Risk	Environmental and Risk Governance Framework
Regulatory Risk	Compliance Policy (by Compliance)
	AML Policy (by Compliance)

6. The Role of the Risk Management Unit

- Setting the framework, strategy and policy and procedures for Risk Management
- Setting the framework, strategy and policy and procedures for ESG Risk Management
- Building a risk awareness culture and disseminating the culture across the organization
- Establishing a risk framework that defines the ownership and accountability of management of the risks identified.
- Implementation of a rigorous risk assessment process to carry out continuous risk identification, control and mitigation processors
- Establishing the Company's risk appetite and risk limits
- Establishing the Company's ESG Risk appetite and strive to reach specific measurable ESG Goals
- Integrate environmental and social risk management considerations into SLI's business activities and approval and risk management processes and establish an effective reporting framework to track and report ESG issues in relevant areas
- Support the decision-making process of the Company with reliable analysis of risk exposures
- Strengthening systems, policies, processes, and measurement tools as needed to provide robust Risk Mitigation, including specialised operational risk management processes, including business continuity management, occupational health and safety
- Modify mitigation strategies according to changes in internal and external environment
- Ensuring that the BRMC has all the required information to enable it to efficiently exercise its governance function.
- Disseminating information on risk for the Board and other stakeholders
- Disseminating information on ESG risk to the Board Risk Committee
- Monitor developments and emerging best practice on the identification of ESG

and Climate related risk and opportunities and mitigation techniques

- Review annually all policies under purview of Risk Governance Framework
- Liaising with the internal audit function to review the adequacy of internal controls related to risk management and to address audit findings related to risk.

7. Summary of Roles and Responsibilities

	Design and implement an overall risk management process	Identification of Risks	Performing Risk Analysis and Evaluation	Defining Risk Acceptable level	Risk Mitigation and Response	Communicating Risk Acceptance	Risk Monitoring and Reporting
Board of Directors	**I**						
Managing Director	**I**	**I**		**C**	**I**	**C**	**I**
Head of Risk	**R**	**A**	**A**	**A**	**C**	**A**	**A**
Risk Unit	**C**	**R**	**R**	**R**	**C**	**R**	**R**
Business Process Owners		**R**			**R**		**I**

8. Identification of Risks

Identification of risks may occur in one or more ways listed below;

a) Direct Observations
b) Incident Analysis
c) Scenario Analysis
d) Structured What – If Analysis

9. Assessment of Risks

All identified risks are rated according to its likelihood of occurrence and the potential impact on the Business as per the Risk Scoring Matrix below which evaluates the impact and likelihood of occurrence.

The potential impact of a risk is evaluated based on its impact on business continuity, profit, and the loss of business portfolio as detailed below.

Assessment and Measurement of Identified Risks

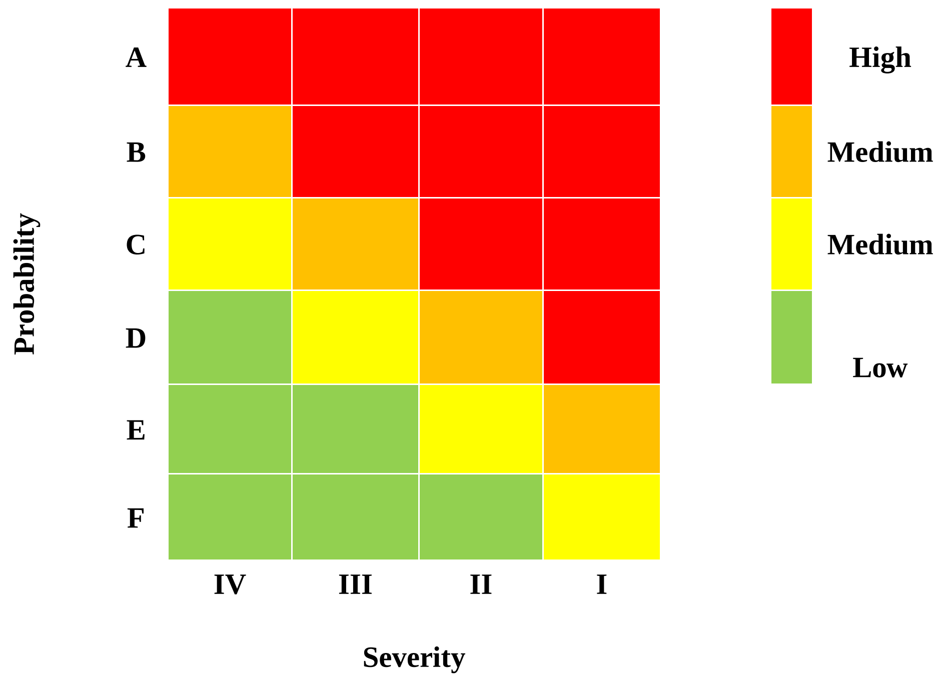
	Risks that affect Business Continuity			
	IV – Marginal	**III – Significant**	**II – Critical**	**I - Catastrophic**
Operations	< 1 Hour	1 Hours < x < 5 Hours	5 hours < x < 1 Day	x > 1 Day
Call Centre	< 5 Minutes	> 5 Minutes < 15 Minutes	> 15 Minutes < 30 Minutes	> 30 Minutes
Other Critical Systems	As defined in the BCP and IT DR Plan			

	Other Risks			
	IV – Marginal	**III – Significant**	**II – Critical**	**I - Catastrophic**
PBT	x < Rs. 200 Mn	Rs. 200 Mn < x < Rs.450 Mn	Rs. 450 Mn < x < Rs. 750 Mn	x > Rs. 750 Mn
	X < 4.4%	4.4% < x < 10%	10% < x <16.6%	x > 16.6%
Total Equity	X <500 Mn	Rs. 500 Mn < x < Rs. 750 Mn	Rs. 750 Mn < x < Rs. 1.5 Bn	x > Rs. 1.5 Bn
Loss of Market Share	x < 0.5%	0.5% < x < 1.5%	1.5% < x < 2.5%	x > 2.5%
Stakeholder Faith	x < Rs. 2,500 Mn	Rs. 2,500 Mn < x < Rs. 4,500 Mn	Rs. 4,500 Mn ≤ x < Rs. 5,700 Mn	x ≥ Rs. 5,700 Mn

The likelihood of the occurrence of the risk is examined based on the historical experience and probabilities of occurrence under current market and economic conditions. The matrix defines the probability of occurrence as the likelihood of an event occurring in a particular time period. As such we have defined six probabilities of occurrence as given below.

Probability	Description	Definition
A	Very High	< 3 Months
B	High	3 Months < 1 Year
C	Occasional	1 Year < 5 Years
D	Low	5 Years < 15 Years
E	Very Low	15 Years < 100 Years
F	Almost Impossible	>100 Years

These risks once rated according to the above are plotted on the traffic light matrix below.



10. Escalation, Treatment and Reporting of Risks

	Marginal	Significant	Critical/ Catastrophic
Escalation of Risk	Not Required	• Risk Unit • Risk Owner • Owner of Risk Mitigation • Senior Management	• Risk Unit • Risk Owner • Owner of Risk Mitigation • Senior Management • Board of Directors
Treatment Mechanism	Acceptable with continued monitoring or Acceptable after review of operation. Requires continued tracking and recorded action plans	Implement controls immediately to mitigate risks so that risk is controlled. The Risk may also be accepted by the Board of Directors with the recommendation of the Head of Risk.	Immediate risk treatment actions are required since the impact is significant and reported and discussed by the Board of Directors.
Reporting	Board of Directors		

11. Criteria of Risk acceptance

a) Criteria for Risk Acceptance

- Risk acceptance shall be based on the following criteria's:
  - ✓ The cost of controls is significantly higher than the possible benefits gained from implementing such controls.
  - ✓ Acceptance of risk does not violate any legal, statutory and/or regulatory requirements.
  - ✓ Regional, socioeconomic, and environmental aspects that prevent the implementation of controls; and
  - ✓ The possible adverse impacts on business operations due to implementation of the controls and the related stakeholders' concerns and priorities.

b) Communication of Risk Acceptance

a) The Company's Risk register will note the acceptance of the said risk, along with the description of the risk, justification of the risk, the criteria for risk acceptance as per the above methodology and any plans to reduce the risk in future

b) Additionally, the Minutes of the Board Meeting should clearly mention the acceptance of the same.