CONFIDENTIAL

SARAWAK CONSOLIDATED INDUSTRIES BERHAD

RISK MANAGEMENT FRAMEWORK

(Approved by the Board of Directors on 17 June 2020)

THE CONTENT

1. INTRODUCTION

a. Purpose of the Policy

All activities undertaken by Sarawak Consolidated Industries Berhad ("SCIB") carry an element of risk. The exposure to these risks is managed through the practice of Risk Management. In managing risk, it is SCIB's practice to take advantage of potential opportunities while managing potential adverse effects. Managing risk is the responsibility of everyone in SCIB.

The objectives of this policy are:

- Ensure going business concern by avoiding and mitigating losses;
- Improve business performance by informing and improving decision making and planning;
- Promote a more innovative, less risk averse culture in which the taking of calculated risks in pursuit of opportunities to benefit SCIB is encouraged; and
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance.

This policy outlines SCIB's risk management process and sets out the responsibilities of the Board of Directors ("Board"), Group Managing Diretor / Chief Executive Officer / Executive Director ("GMD / CEO / ED") and Risk Management Committee ("RMC"), the senior management and others within SCIB in relation to risk management.

b. Policy Owner

The GMD / CEO / ED is the policy owner of the Risk Management Policy for SCIB.

2. DEFINITIONS

The key definitions for this policy are as follows:

- Risk

The chance of something happening that will have an impact on the achievement of SCIB's Vision, Mission and Objectives.

- Risk Assessment

The overall process of risk analysis and evaluation.

- Risk Management

The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects within SCIB.

3. GENERAL PRINCIPLE

- All risk management activity is to align to corporate Vision, Mission and Objectives and SCIB priorities, and aims to protect and enhance the reputation and standing of SCIB.
- Risk analysis is to form part of SCIB strategic planning, business planning and investment/project appraisal procedures.
- Risk management is to be founded on a risk-based approach to internal control which is embedded in day to day operations of SCIB.
- Our risk management approach is to inform and direct our work to gain an assurance on the reliability of SCIB systems and will form the key means by which the Board gains its direct assurance.
- Risk management can be applied at many levels in an organisation. It can be applied at a strategic level and operational level. It may be applied to specific projects, to assist with specific decisions or to manage specific recognised risk areas.

4. PRINCIPLE FOR MANAGING SPECIFIC RISKS

- Risk management in the organisation should be proactive and reasoned. Principal risks should be identified, objectively assessed, and, where this is the appropriate response, actively managed.
- The aim is to anticipate, and where possible, avoid risks rather than dealing with the consequences. However, for some key areas where the likelihood of a risk occurring is relatively small, but the impact on SCIB is high, the risk may be covered by developing contingency plans.
- In determining an appropriate response, the cost of control/risk management, and the impact of risks occurring is to balance with the benefits of reducing risk. It is not necessary to set up and monitor controls to counter risks where the cost and effort are disproportionate to the impact or expected benefits.

5. UNDERSTANDING RISK MANAGEMENT

Risks have been described in terms of combination of the consequences of an event occurring and its likelihood of occurring.

Risk is the chance of something happening that will have an impact on objectives and risk management can be described as the culture, processes and structures that are directed towards realizing potential opportunities whilst managing an adverse effect.

SCIB's risk management system is designed to identify the risks it faces and has measures in place to keep those risks to an acceptable minimum. The existence of risk presents both threats and opportunities to SCIB.

Risk owners have been assigned responsibility for the identified risks in the Risk Register. SCIB's risk assessment matrix is used as the benchmark in planning and implementing the risk management measures. It takes into consideration the nature, scale and complexity of the business.

The risk management process consists of the following main elements:

- Identify

  Identify a risk (threats or opportunities) and document the risks captured by the risk register owner.

- Assess

  The primary goal is to document the net effect of all identified threats and opportunities, by assessing:

  - Likelihood of threats and opportunities(risks);
  - Impact of each risk;
  - Proximity of threats; and
  - Prioritization based on scales.

- Plan

  Preparation of management responses to mitigate threats and maximize opportunities.

- Implement

  Risk responses are actioned.

- Monitor and review

  Monitor and review the performance of the risk management system and changes to business initiatives.

- Communicate

  Provide regular reports to Management team / Audit and Risk Committee at agreed times.

Risks are effectively managed by SCIB through the effective implementation of various controls, which include:

- Board approved risk management framework;
- Documented policies and procedures;
- Maintenance of registers;
- Implementation of risk-based systems and processes;
- Ongoing monitoring of regulatory obligations;
- Checklists to guide activities and project plans to record actions; and
- Internal and external reporting.

6. RESPONSIBILITY

a. Board

The Board of SCIB, through RMC, has responsibility to review and ensure that:

- the Committee has quarterly meeting to review SCIB's risk management framework to satisfy itself that it continues to be sound and effectively identifies all areas of potential risk;
- adequate all policies and processes have been designed and implemented to manage identified risks; and
- Proper remedial action is undertaken to redress areas of weakness.

b. GMD / CEO / ED

The GMD / CEO / ED of SCIB has responsibility under this policy for:

- Monitoring compliance with this policy;
- Reporting to the Board on compliance with this policy;
- Developing, implementing and monitoring systems, management of policies and procedures relevant to the business, including facilitating review by the Executive on a regular basis; and
- Review the Risk Register and Maintaining the risk register.

c. Risk Management Committee

- Ensure the implementation of the risk management policy.
- Identify, evaluate and manage principal risks faced by SCIB (Appendix 1).
- Update the Board via RMC on the status of risks and controls.
- Status update of the Management action on Risk (Risk Owner / Litigation).

d. Risk Owner

The risk owner is identifying new risk (as noted in the Risk Register) is responsible for ensuring on a daily basis that the relevant operational procedures and controls implemented to treat each risk area are adequate and effective. If a control or procedure is not adequate and effective in treating the risk, the risk owner should report this, with a recommendation for an alternative risk treatment, to the Risk Working Committee and ultimately approval from the GMD / CEO / ED.

e. General Responsibilities

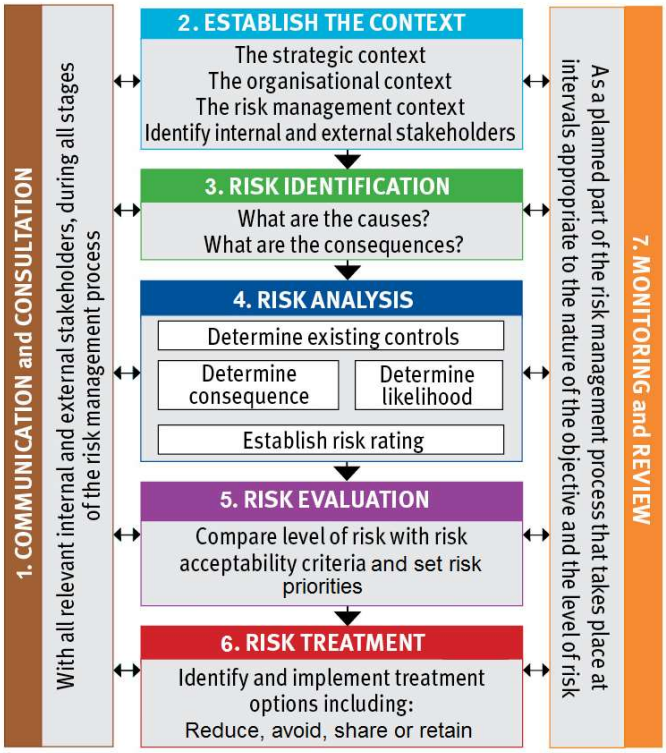
Every SCIB staff member is responsible for effective management of risk including the identification of potential risks. Management is responsible for the development of risk mitigation plans and the implementation of risk reduction strategies. Risk management processes should be integrated with other planning processes and management activities.

Where there is legislation in place for the management of specific risks (such as Occupational Health and Safety) this Risk Management policy does not relieve SCIB of its responsibility to comply with that legislation.

Managers are accountable for strategic risk management within areas under their control, including the promotion and training of the risk management process to staff.

7. RISK MANAGEMENT PROCEDURE

a. Summary of Process



b. Risk Management Process

The risk management system is dynamic and is designed to adapt to SCIB's developments and any changes in the risk profile over time.

The risk management system is based on a structured and systemic process which takes into account SCIB's internal and external risks.

The main elements of the risk management process are as follows:

- Communicate and consult

  Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

- Establish the context

  Establish the external, internal and risk management context in which the rest of the process will take place – the criteria against which risk will be evaluated should be established and the structure of the analysis defined.

- Identify Risks

  Identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of SCIB's objectives.

- Record Risks

  Document the risks that have been identified in the Risk Register.

- Analyze Risks

  Identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk by analyzing the range of potential consequences and how these could occur.

- Evaluate Risks

  compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.

- Treat risks

  Develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.

- Monitor and review

  It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and effectiveness of treatment measures need to be monitored so that changing circumstances do not alter priorities.

SCIB's risks may come from any internal or external event which, if it occurs, may affect the ability to efficiently and effectively of SCIB operation:

- Internal Risks (Operational Risks)

  Those risks that specifically relate to SCIB's business itself and as such as generally within its control. They include risks such as employee related risks, strategic risks, and financial risks.

- External Risks (Business Risk)

  Those risks that are outside the control of SCIB. They include risks such as market conditions and legislative change.

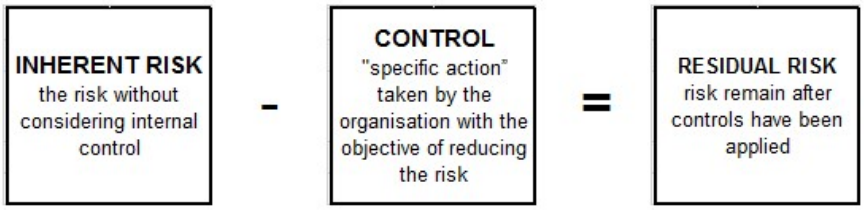
The risks are defined in two types:

- Inherent Risks

  Commonly defined as "the risk without considering internal control" or alternatively "a raw risk that has no mitigation factor or treatment applied to it".

- Residual risks

  Commonly defined as "the level or risk remaining after controls have been applied. An exposure to loss remaining, after other known risk have been countered or eliminated.



Risks are effectively managed by SCIB through the effective implementation of various controls, which include:

- Board approved risk management framework;
- Maintenance of risk register; and
- Regular review of risks and controls, particularly as the business changes.

c. Risk Management Methodology

The methodology adopted by SCIB for managing and treating its risks can be defined as follows:

- Document a risk management framework (i.e. the context)
- Identify the general activities involved in running the business (i.e. risk categories)
- Identify the risks involved in undertaking the specific business activity by asking the questions:
  - What could happen?
  - How and why could it happen?
- Rate the likelihood of the business activity not being properly performed. Likelihood is assessed to the assumption that there are no existing risk management and compliance processes in place. It is assessed as either **Very High, High, Medium, Low** or **Very Low.**

- Rate the consequence of not properly performing the business activity - damage can be quantified in terms of financial and reputation loss to investors or SCIB itself. It is assessed as **Very Significant, Major, Moderate, Minor** and **Insignificant**.
- Assign the inherent risk rating based on a combination of the risk rating. Low and medium risks may be considered acceptable and therefore minimal further work on these risks may be required. The rating may be assessed as **Critical, High, Medium** and **Low.**
- Identify the Implication of the risk which would be e.g. in aspects of financial, reputation, noncompliance, operations.
- Decide the Actions Plans to control or mitigate the risk by What, How, Who and When.
- Assess whether the existing controls are adequate and allocate the responsibility of monitoring the control to treat the risk. This will integrate risk management and compliance to daily activities and facilitate appropriate control of operational risk.
- Raise awareness about managing risks across the organization through communicating the policy and responsibilities.
- Routinely monitor and review ongoing risks so can risk can be effectively managed The Risk. Any change on the risk scoring or effectiveness of the control shall be recorded in Remarks.

d. Risk Rating Definition

- Critical

  These are classed as primary risks requiring immediate attention. They may have a high or low likelihood of occurrence, but their potential consequences are such that they must be treated as a high priority. This may mean that mitigation strategies should be developed and put in place to reduce or eliminate the risks, and the risks monitored regularly. Consideration should be given to planning being specific to the risk rather than generic.

- High

  These risks are classed as significant. They may have a high or medium likelihood of occurrence, but their potential consequences are sufficiently serious to warrant consideration after those risks classified as 'very high'. Consideration should be given to developing strategies to reduce or eliminate the risks, and the risks monitored regularly.

- Medium

  These risks are less significant, but may cause upset and inconvenience in the short term. These risks should be monitored to ensure that they are being appropriately managed and consideration given to their being managed under generic planning arrangements.

- Low

  These risks are both unlikely to occur and not significant in their impact. They should be managed using normal or generic planning arrangements and require minimal monitoring and control unless subsequent risk assessments show a substantial change, prompting a move to another risk category.

Risk Rating Matrix and Risk Register format are shown in Appendix A.

8. RISK CATEGORY

a. Environment

- Risks associated with protection and enhancement of the environment, as well as risks arising from natural disasters such as floods, earthquakes, landslides, tsunamis, hurricanes, adverse weather conditions, etc.
- This also includes the risk of disruption to business activities due to the spread of pandemics/ epidemics.

b. Financial

- Risks relating to financial management or transactions, such as fraud, theft, conflict of interest, duplicated payments, etc. Includes risks relating to financial budgets and factors affecting budgets, insufficient cash flows, and improper controls over financial operations or processes.

c. Human Resources

- Risks arising from ineffective organizational capabilities, work environment, and other relating to human resource issues and competencies within the Corporation such as relating to recruitment, engagement, training and staff development.

d. Information Technology

- Risks arising from the use and reliance on information by the Corporation or other external entities, which may impact operations, such as internal systems, external service provider's systems, business / internet.
- Risks relating to the protection of corporate and private information.
- Risks relating to the security, function or management of technological systems and processes.
- Risks relating to IT implementation, including mismatch or lack of adequate technology, IT applications and capabilities.

e. Legal & Regulatory or Compliance

- Risks resulting from non-compliance with internal and external policies, procedures, standards and laws.
- Risks relating to service and/or product delivery or information or breach of contracts or defaults that result in legal proceedings.

f. Operational

- Risks associated with a lack of defined policies, processes, procedures or delegations of authority at a functional or business unit level.
- Risks associated with culture, organizational structure and communication including supporting system, processes and procedures.
- Risks resulting from the ineffectiveness of operational processes, legal and/or financial impacts and other shortfalls.

g. Stakeholder Management

- Risks associated with the identification of individuals and organizations with a direct influence on and/or interest in the Corporation's operations.
- Risks associated with the need to ensure ongoing and effective communication and consultation with key stakeholders.

h. Market

- Risks due to changes or volatility in the market forces affecting the business operation and the Corporation's competitive position or advantage.
- Risks relating to the incomplete or total absence or ineffective strategies to position the Corporation's products and services in the market.

i. Corruption

- Risk which is equated with the set of institutional vulnerabilities within a system or process which might favor or facilitate corrupt practices.

9. MANAGEMENT OF CHANGE

Where any changes to systems of work and planned changes in process, substances, equipment, procedures, people and information, a review of existing risk assessments and procedures shall be required.

10. RISK MANAGEMENT ASSURANCE AND REVIEW

a. Risk Management Assurance and Review

- Assurance on the integrity of the control and recovery barriers shall be established through regular review and inspection depending on:
  - Criticality
  - Magnitude of the risk
  - Performance of the control barriers
- Risk Management studies shall be reviewed and updated when there are changes within the organization, which call into question the validity of the existing assessments. Such changes can include the following elements but not limited to:
  - Changes in any legislation and other requirements or SCIB policy and concern from interested party.
  - Expansion, construction or modification of plant or work area.
  - Changes to the operation.
  - Audit findings.
  - To incorporate the findings subsequent to the incident investigations findings.

b. Period of Policy Review

The review shall take place at least once every two (2) years if there are no changes occurred.

c. Procedure of Changes

The changes resulting from this review shall be managed according to SCIB policy.

Appendix A – Risk Rating Matrix and Risk Register

Risk Consequence Severity (Impact)

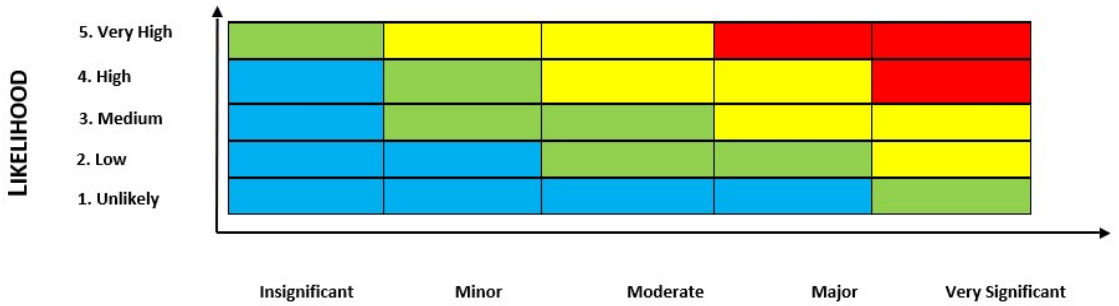
Consequence Type	Insignificant	Minor	Moderate	Major	Very Significant
Financial Loss	<RM100K	Minor loss RM100K - RM250K	Moderate loss RM250K – RM500K	Major loss RM500K – RM1 mil	Significant loss >RM1 mil
Cash Flow Impact	No impact	Minimal impact on cash flow. No external borrowing required / related to SCIB advance required	Cash flow affected. Short term borrowing required (Borrowing of less than 1 year)	Cash flow erosion. Long term borrowing required (Borrowing more than 1 year)	Imminent cash flow erosion. Shareholder borrowing required
Business Objective	Business objective can still be achieved	Business objective can still be achieved	Business objective is threatened	Major threat to business objective	Business objective will most probably not be achieved
Business Interruption	No impact. Business as usual	Up to ½ day	Up to 1 day	More than 1 day but less than 3 days	More than 3 days
Legal & Regulatory Impact	Not applicable	Not applicable	Non-compliance with internal policies and procedures	• Non-compliance with external guidelines • Breach of contracts	Non-compliance with regulations and Acts
Business Process & System	No amendments on planned activities	Minor amendments to certain parts of planned activities	Minor rework on planned activities	Rework on certain parts of planned activities	Significant or total rework on planned activities

Consequence Type	Insignificant	Minor	Moderate	Major	Very Significant
People	No impact	Insignificant level of staff's dissatisfaction	Localized low morale / low staff turnover	Significant spread of low morale / Increasing staff turnover	Group wide low morale / high staff turnover
Reputation	No impact on reputation.	Minor impact on Image. Recoverable. (recovery period up to 1 month)	Any event which may tarnish SCIB's reputation but does not attract published adverse publicity (Recovery period up to 3 months	Any event which may tarnish SCIB reputation with a specific customer, group or 3rd party and adverse publicity published in local media (Recovery period up to 6 months)	Adverse publicity in either the local or national press, which attract a newspaper editorial or feature article. (Recovery period of more than 6 months)
Customer Satisfaction	No impact	Minor shareholder dissatisfaction when ROE is more than 5% but less than 8%	Moderate shareholders dissatisfaction when ROE is between 3% to 5%	Major shareholder dissatisfaction when ROE is less than 3%	Very significant shareholder dissatisfaction due to negative returns

Probability & Frequency (Likelihood)

Likelihood Rating	Description	Probability
Very High	Known to happen often	> 80%
High	Could easily happen	40% - 79%
Medium	Could happen & has occurred before	20% - 39%
Low	Hasn't happened yet but could	5% - 19%
Unlikely	Conceivable, but only in extreme circumstances	< 5%

Risk Rating Matrix



Impact

CATEGORY	DESCRIPTION	RISK SCORE
Critical	Primary risk - Consideration should be given to planning being specific to the risk rather than generic.	20 - 25
High	Significant risk - Consideration should be given to developing strategies to reduce or eliminate the risks, and the risks monitored regularly.	10 - 19
Medium	Less significant risk - but may cause upset and inconvenience in the short term. Consideration given to their being managed under generic planning arrangements.	6 - 9
Low	Unlikely to occur and not significant risk - should be managed using normal or generic planning arrangements and require minimal monitoring and control	1 - 5

Risk Register

No	Risks (Inherent/Control)	Category Business Risk - External Risk Operational Risk - Internal Risk	Residual Risk			Implication	ACTIONS PLANS				Action Status	Remarks
			Possibility	Impact	Risk Score		What	How	Who	When		

Name :
Position :
Department :
Date :
Signature :