I-Berhad

RISK MANAGEMENT POLICY

SOURCE	: RISK MANAGEMENT COMMITTEE
APPLICATION TO	: I-Berhad and Subsidiaries
SUBJECT	: RISK MANAGEMENT POLICY

CONTENTS

Approved by the Board on 24 November 2021.

Reviewed and updated by the Board on 28 November 2023.

1.0 INTRODUCTION

Risk management is a key discipline in today's business environment to manage the business and its growth in order to:

- Optimise the return and to protect the interest of stakeholders (including shareholders, customers and employees).
- Safeguard the organisation's assets and maintain its reputation.
- Improve organisation's performance.
- Fulfil the organisation's strategic objectives.

2.0 RISK, RISK MANAGEMENT POLICY AND OBJECTIVE OF RISK MANAGEMENT POLICY

2.1 DEFINITION OF RISK

The enterprise risk management framework of I-Berhad ("the Company) and its subsidiary companies ("I-Berhad Group") and this policy adopt a broad definition of risk, which is as follows:

The negative effect of uncertainty on I-Berhad Group's business objectives. Business risk arises as much from the possibility that threats will materialise or that errors will be made as it does from the possibility that opportunities will not be realised.

This definition is not meant to limit risk management thinking only to ensure avoidance of possible losses. I-Berhad Group will consider its priority, financial position as well as the adequacy of its resources and timing in determining its risk appetite, it is because the future is uncertain, any business activity is associated with risks and rewards, and its objectives are to identify and reap rewards and opportunities, as well as to manage and control the resulting risks.

2.2 RISK MANAGEMENT POLICY

A statement of the overall intentions and direction of I-Berhad related to risk management. It addresses key elements of the risk management framework to be implemented and maintained by I-Berhad Group which will allow for the management of risks within defined risk/return parameters, risk tolerances and risk management standards. As such, it provides a framework for the effective identification, evaluation, management and reporting of I-Berhad Group's risks. Accordingly, this is established with the aim of setting and providing references of the intents and fundamentals of risk management practices.

2.3   OBJECTIVE OF RISK MANAGEMENT POLICY

The objective of this policy is to define the ongoing and consistent process for identifying, assessing, monitoring and reporting significant risks faced by the business units, departments, executives and ultimately, I-Berhad Group.

The primary goals of I-Berhad Group's Risk Management Policy are to support the overall business objectives of I-Berhad Group by:

- Providing a policy and organisational structure for the management of risks that I-Berhad Group assumes in carrying out its activities.

- Outlining I-Berhad Group's risk context which comprises philosophies, strategies and policies, and operating system so as to better manage the business risks faced by I-Berhad Group.

- Providing guidance for the formation of management practices, procedures, processes, responsibilities and actions on risk management.

- Implementing and maintaining a sound risk management framework which identifies, assesses, manages and monitors the business risks.

- Defining risk management roles and responsibilities within the organisation and outlining procedure to mitigate risks.

- Embedding consistent and acceptable management of risk throughout all the business units within the I-Berhad Group.

- Defining a reporting framework to ensure the communication of necessary risk management information to the Board of Directors, Management and personnel engaged in risk management activities.

- Remaining flexible to accommodate the changing risk management needs of the organisation while maintaining control of the overall risk position.

- Providing reasonable assurance to the Group's stakeholders that a sound risk management system is in place and in accordance with the regulatory bodies' requirements.

- Supporting the risk management framework and strategy with an appropriate organisational structure and ensuring that associated responsibilities are clearly defined and communicated at all levels.

- Setting out the appropriate methods for risk assessment to be adopted by the Group.

- Providing a system to accommodate the central accumulation of risk data which can form part of each department's operational procedures.

- Ensuring that adequate disclosure of risk management activities of the Group is made in the Company's annual report in compliance with the provisions of Bursa's Listing Requirements.

3.0 ACCOUNTABILITY FOR RISK MANAGEMENT

3.1 THE BOARD OF DIRECTORS

The Board of Directors ("the Board") of I-Berhad act as an oversight body for risk management process within I-Berhad Group to ensure the Group identifies all of its risks, recorded in risk register and adequate / effective mitigation or action plans to be taken by the risk owners to mitigate the possibility / impact of the risk happening.

3.2 RISK MANAGEMENT COMMITTEE ("RMC")

The RMC is responsible for, amongst others, reviewing and overseeing the risk management function of I-Berhad Group, on behalf of the Board, which includes, amongst others, the following:-

- to review the risk management policies of I-Berhad Group which addresses key elements of the enterprise wide risk management framework, risk appetite, strategy, processes and methodology and recommend any necessary changes relating thereto to the Board in line with the changing operating and economic environment, prevailing best practices in risk management and any relevant regulatory requirements.

- to oversee, evaluate and monitor the adequacy and effectiveness of I-Berhad Group's risk management framework and the risk management system put in place by the Management in tandem with the changing business circumstances to safeguard shareholders' interests and the Group's assets.

- to report to the Board on the Group's major risk exposures, including the review on the risk assessment framework used to monitor the risk exposures and the Management's views on the acceptable and appropriate level of risks faced by respective business units/division of the Group.

- to review the Statement on Risk Management and Internal Control, as well as other disclosure concerning the risk management activities of I-Berhad Group, for inclusion in the Company's Annual Report and recommend the same for approval by the Board.

- to review the Anti-Bribery and Anti-Corruption Policy and Procedures of the I-Berhad Group.

3.3   RISK MANAGEMENT TEAM

The Risk Management Team ("RM Team"), comprising members of the Management, as nominated by the Group Chief Executive Officer is responsible for the overall risk management activities of I-Berhad Group, whilst direct responsibility for managing risk lies with the respective risk owners. The RM Team is entrusted to carry out the following:-

• Setting up an enterprise-wide risk management system for identifying, assessing, managing (by elimination, mitigation, transfer and/or acceptance) and reviewing risks throughout the I-Berhad Group.

• Increasing awareness, providing guidance and training and educating all employees of I-Berhad Group in understanding and appreciating the relevance and importance of enterprise-wide risk management.

• Continuously overseeing and monitoring the implementation of the risk management system activities to ensure the risk management system is functioning effectively in line with the Board's policies, strategies and risk appetite.

• Ensuring infrastructure, resources and systems are in place for risk management; ensuring that the staff responsible for implementing risk management systems perform those duties independently of the business units' risk taking activities.

• Continuously review risk, risk evaluations and risk management strategies identified, proposed and/or implemented pursuant to the risk management system, including to review and analyse risk reports from the respective risk owners to assess the effectiveness of action taken to address/manage the risks identified.

• Periodically reviewing and continuously improving upon the enterprise-wide risk management system (then) being implemented.

• Periodically reporting to the RMC and Board on the Group's risk exposures, including the review on the risk assessment framework used to monitor the risk exposures and the Management's views on the acceptable and appropriate level of risks faced by respective business units/division of the Group.
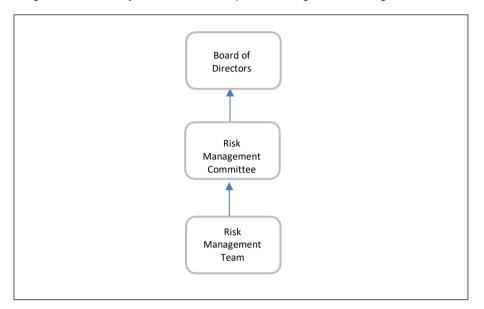
• The RMT reports to the RMC.

Diagram 1 – Summary of I-Berhad's Group Risk Management Oversight Structure

3.4   RESPONSIBILITIES OF RISK OWNER, CONTROL OWNER AND ACTION PLAN OWNER

Risk Owner is a person or entity with the accountability and authority to manage risk. Each risk identified would be recorded in risk register (please refer to Appendix 1) whereby name/ designation of Risk Owner, Control Owner and Action Plan Owner MUST be clearly stated in the document to ensure their responsibility towards the risk, control and action plan.

4.0   RISK IDENTIFICATION ANDTOLERANCE

4.1   RISK IDENTIFICATION

Risk Owners will be required to consider and assess the risk implications of all actions they undertake in relation to both existing and proposed activities, systems and procedures. A Risk Owner is a named individual accountable for all aspects of the risk including identification, assessment, evaluation, monitoring and reporting. All risks identified will be evaluated and documented, together with the controls which mitigate those risks, and personnel accountable for them. Comprehensive identification is critical since any unidentified risks at this stage will not be included in further analysis.

The techniques used to help identify risks include interviews, discussion with employees, review of financial statements and previous risk management reports. To help with risk identification, risks should be considered within main risk categories such as strategic, financial, operational and compliance risks.

Risk identification is a line management responsibility. On recognising a risk, the employee should contact his/her immediate superior illustrating the risk identified and explaining to the line manager his/her understanding of the potential consequences of such risk materialising.

For each risk, accountability is assigned to the person best able to take appropriate decisions to manage the risk in question. Heads of Departments / Head of Projects will make this decision. The determination of best ability will take into consideration the individual's competence, authority, responsibility and available resources.

The responsibility for the adequate control of each risk rests with the assigned Risk Owner. The control and monitoring of each business risk exercised by the Group Management through Risk Management Policies & Procedures, does not relieve Risk Owners of that responsibility.

Risk Owners may delegate tasks to others when managing risks. However, this does not resolve them of ultimate responsibility for the risk. The delegated task owner would then report to the risk owner on the progress of the treatment for the risk.

The risk identification process should be kept up to date.

4.2   RISK CATEGORISATION

Identified risk would be generally categorised into two (2) broad categories i.e. internal and external and then sub-categorised under one (1) of the following categories (according to the Risk Areas):

▪ Strategic ▪ Business environment ▪ Customer ▪ New business ▪ Governance	▪ Reputation ▪ Financial ▪ Marketing ▪ Regulatory and legal ▪ Operational	▪ Product and service ▪ Supplier and sub-contractor ▪ People and culture ▪ Information management ▪ Sustainability ▪ Climate-related

In assessing which category the risk should be placed under, the Risk Owner should take into account the area from which the risk originated. For example, if the identified risk is the threat of rising interest rates, then this risk should be categorised under financial, as it affects the company financially

4.3 MAXIMUM RISK EXPOSURE / RISK TOLERANCE

I-Berhad Group will accept a commercial level of risk such that the long-term profitability and survival of the business are reasonably assured. Where new risks arise, they will be:

- Evaluated (refer to section 5.0 below).

- Immediately reported to the Immediate Superior and Line Manager, and ultimately to the Chief Executive Officer (to develop control strategies/ action plans).

- Monitored through the risk management system.

- Promptly reported to the RMC, together with the mitigations to manage the identified risk.

5.0 RISK EVALUATION

5.1 RISK ASSESSMENT / RISK PARAMETERS

Risk is to be assessed by considering estimates of both likelihood and impact. Risks should be scored relative to each other and against a fixed scale in order to ascertain their relevance to the business.

Risk is to be further assessed by considering I-Berhad Group's vulnerability to the risk after taking into consideration the efficiency of treatments identified, proposed and/or currently implemented (see Section 5.2 below).

Gross likelihood of occurrence measures the expected frequency of a risk occurring or materializing before taking into consideration current control strategies or risk management in place.

Score	Likelihood	Description
5	Almost certain	Happening now or will occur at least monthly.
4	Likely	May occur at least once every 6 to 12 months.
3	Possible	May occur at least once every 1 to 2 years.
2	Unlikely	May occur at least once every 2 to 3 years.
1	Rare	May occur at least once in > 3 years.

Table 1 – Qualitative measures for Likelihood of Occurrence

Gross magnitude of impact measures the expected effect of a risk occurring *before* taking into consideration current control strategies or risk management in place.

Score	Impact	Implication
5	Critical	Extremely high financial loss and significant irreparable impact on stakeholders' prospects. Impact to organization and staff morale severe.
4	Major	High financial loss, projects, projects, services or clients curtailed due to failure to deliver outcomes, serious external criticism (e.g. key stakeholders, high profile media, severely adverse audit report). Substantial impact on overall staff and morale with performance affected. Measurable increase in stress related issues.
3	Moderate	Medium financial loss, substantial impact on overall program or functional outcomes (e.g. many projects, products, services or clients), some external criticism directed at executive, Board (e.g. by customers and stakeholders, low key media, moderately adverse audit report). Impact on staff noticeable, degree of change in morale.
2	Minor	Small financial loss, small impact on overall program or functional outcomes (e.g. confined to a substantial minority or projects, products, services or clients), criticism by directly affected managers or clients, minimal impact on staff or overall morale.
1	Insignificant	Minimal financial loss, no impact on overall program or functional outcomes (e.g. confined to very small number of projects, products, services or clients), no adverse external criticism or publicity, no impact on staff.

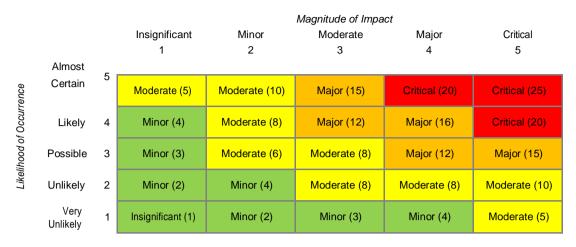*Table 2 – Qualitative measure for Magnitude of Impact / Consequences*

Magnitude of Impact

		Insignificant 1	Minor 2	Moderate 3	Major 4	Critical 5
Almost Certain	5	Moderate (5)	Moderate (10)	Major (15)	Critical (20)	Critical (25)
Likely	4	Minor (4)	Moderate (8)	Major (12)	Major (16)	Critical (20)
Possible	3	Minor (3)	Moderate (6)	Moderate (8)	Major (12)	Major (15)
Unlikely	2	Minor (2)	Minor (4)	Moderate (8)	Moderate (8)	Moderate (10)
Very Unlikely	1	Insignificant (1)	Minor (2)	Minor (3)	Minor (4)	Moderate (5)

Likelihood of Occurrence

Table 3 – Qualitative Risk Matrix / Likelihood and Impact Matrix

Level of Acceptance	Score	Classification	Required Action
Unacceptable Level	20 – 25	Critical	RM Team, RMC and Board attention required.
	12 - 16	Major	Attention, time and resources required.
Acceptable Level	5 – 10	Moderate	Specific risk management required to monitor and review.
	2 - 4	Minor	Standard operating procedures / policies to handle.
	1	Insignificant	Acceptable.

Table 4 – Risk Rating Classification and Level of Acceptance

5.2 IDENTIFYING KEY CONTROL

Risk Owners must identify the present and existing key control or risk treatment methodology (system / procedures / policies) that have been put in place to address / mitigate the gross risk and to review the effectiveness of the existing key controls to manage these risks.

Key control could be in form of:

a. Preventive Control

Designed to STOP the consequences or damages arising from undesirable transactions, items, events, errors or incidents from occurring so that to reduce the likelihood of the risk. These include but not limited to policies & procedures, organisation structure, segregation of duties, delegated authorities, training and dual control.

b. Defective Control

Designed to promptly REVEAL undesirable transactions, items, events errors or incidents so that the appropriate action can be taken. These include but not limited to secondary checks, control self-assessment, reconciliation and validation checks.

c. Corrective Control

Designed to REDUCE the consequences or damages arising from crystallisation of an individual significant incident or a significant number of transactions, items events, errors or incidents and to mitigate the full impact of consequences. These include but not limited to change/improve operational control / system and redesign procedural process.

5.3 DETERMINING CONTROL EFFECTIVENESS

This process involved the assessment of the effectiveness of each identified control to reduce the likelihood of risk and / or reduction of the impact.

Risk Mitigation Action (Control Effectiveness) – it is something that already exists and is not merely on someone's wish list. It may be an existing management policy and procedure, or some technical system, or some training program which reduce the risk.

Levels of control effectiveness are as follow:-

Ranking	Score	Description	Action Status
High (H)	3	The control is highly effective because it reduces the likelihood of the risk occurring and/or reduces the consequences if the risk does occur.	Acceptable level of risk - no action is currently needed.
Medium (M)	2	The control is moderately effective because it only partially reduces the likelihood of the risk occurring and /or partially reduces the consequences if the risk does occur. The control needs to be reviewed, abolished, amended, or replaced to make it a highly effective control.	Some reduction in risk level required - monitor position and action plan.
Low (L)	1	The control is ineffective because it does not reduce the likelihood of the risk occurring and/or it does not reduce the consequences if the risk does occur. The control needs to be reviewed, abolished, amended or replaced to make it a highly effective control.	Unacceptable risk level - action required.

Table 5 – Measurement of Effectiveness of Risk Mitigation

5.4 DETERMINING RESIDUAL / NETT RISK

Residual/ nett risk is mitigated by risk action plan (as mentioned in Item 5.2) after considering the risk appetite (acceptable risk).

Likelihood x Impact	= Initial / Gross Risk Rating
(Likelihood x Impact) – Risk Mitigation Action	= Residual / Nett Risk Rating

Table 6 - Vulnerability Table

5.5 RISK TREATMENT

All I-Berhad Group managers are primarily responsible for the treatment of risk exposures within their business operations. Risk treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing those plans.

The range of options includes (but not limited to) the following categories:

- Avoidance, eliminate – prevent / withdrawal from / not involved.
- Reduction, optimise – mitigate.
- Transfer - pass-on to others / insure.
- Retention, accept - budget.
- Sharing - outsource / joint-venture.

The selection and implementation of appropriate options for dealing with risk is the responsibility of the Risk Owner, subject to their respective Head of Departments approving or amending the proposed action plans. The risk profile enables the Board and/ or Management to make conscious and visible risk management decisions. Management should identify and agree on the key risks which should be addressed first after considering the risk profile.

Where current controls are deemed ineffective and therefore warrant action, appropriate control improvements and action plans will be developed by Management. Included in each control plan will be the allocation of accountabilities and action dates for the implementation of the control improvement plan.

Management of individual risks is somewhat subjective; however, the following guidelines should be followed:

- The annual cost of risk control should not exceed the estimated gross annual risk cost.
- I-Berhad Group does not seek to eliminate risk nor be a high-risk taker – moderate level of risk is acceptable ("calculated risks") is acceptable.
- The resources allocated to risk treatment should be given priority in the arears of employee safety, customer service and financial impact.

I-Berhad Group is committed to identifying and mitigating risk and not seeking to eliminate the risk.

6.0 RISK MONITORING

6.1 ESCALATION PROCESS

Risks and risk response activities would be monitored by the respective Head of Departments to ensure that significant risks remain within acceptable risk levels, that emerging risks and gaps are identified and that risk response and control activities are adequate and appropriate.

There is no restriction on what may be escalated for action, but the key criteria is where intervention is required from higher management. This may be because:

- Actions are urgently required and cannot be executed at the current level.
- A decision must be made involving several groups.
- There is doubt as to whether accountability should be retained at the lower level.

The overriding principle for escalating risks for action is – if in doubt, escalate and it is the individual staff's responsibility to highlight risks, which he/she believes require action by higher authority.

Although there is no requirement as to whether individual risks should be escalated for action to a higher authority, management is required to complete an assertion that risks are managed within the business, as set out in Appendix 2. The urgency of escalation for action will vary depending on the nature, and the business area.

6.2 REPORTING FREQUENCY AND FORMAT

Regular risk reporting is essential for information management and business planning. Formal reporting has been instituted at various levels of the organisation (including the Board) to highlight the significant risks identified by the individual departments and I-Berhad Group as a whole during the previous period and business planning cycles.

Risk reporting should be continuous and embedded into existing management reporting processes and structures. The frequency, format and level of reporting should be formalised, with a system to allow red flags or high risk areas to be immediately escalated to the appropriate level for action.

All new risks and changes to existing risks should be timely escalated to the RMC. The RMC will then report to the Board all significant risks identified on a quarterly basis including the current risk profile and a summary of any major changes since the last report.

The RMC will brief the Board, summarising the significant risks facing the I-Berhad Group and the action plans put in place to mitigate the risks.

7.0   MONITORING / REVIEW

The Board and the RMC shall regularly evaluate contribution of risk management to the overall business performance, and the RMC will coordinate periodic reviews of the effectiveness and continued relevance of the risk management system and this policy. Proposed amendments to this policy and/or the risk management system will be subject to the provisions set out in Section 10.1 and Section 10.2 below respectively.

Risk monitoring includes evaluating the effectiveness of the risk treatment plan, reviewing risk strategies and the risk management system which is set up to control implementation.

Regular review of the risk management system should be conducted by the RM Team to identify:

- Simplified and consistent reporting procedures;
- Duplication of risk management activities; and
- Inefficient practices.

8.0   TRAINING AND EDUCATION

It is the policy of I-Berhad Group to provide training to its employees to improve their knowledge, skills and competency, and this includes trainings on risk management with varying degree of emphasis depending on seniority, as and when required.

9.0   CONFIDENTIALITY OF RISK INFORMATION

The information contained within any document dealing with I-Berhad Group's business risks is to be treated as highly confidential and should not be released to any outside parties without the prior written consent of the Board.

10.0   DOCUMENT REVISION

This document is approved and authorised by the Board. This Policy is issued and controlled by the RMC.

10.1   POLICY CHANGE PROCESS

The RMC will periodically review the effectiveness of this policy and as when required by the RMC or the Board. Changes to this Policy may only be made after being authorised by the Board. Any changes to this Policy will result in a change to the revision status and complete reissue of the Policy.

10.2   RISK MANAGEMENT SYSTEM CHANGE

The RMC will periodically review the effectiveness of the risk management system and implement changes and improvements as and when it deems necessary. Changes to the risk management system may only be made upon the recommendation of the RMC and approval of the Board.

10.3   RECORD OF CHANGES

Records of all changes made to this Policy shall be maintained by the Risk Management Department of the Company.

RISK REGISTER

RISK ID	RISK CATEGORY	RISK TITLE & DESCRIPTIONS	ROOT CAUSE	CONSEQUENCE	INITIAL RATING		EXISTING CONTROL					RESIDUAL RATING		RISK TREATMENT	MANAGEMENT ACTION PLAN			STATUS
					LIKELIHOOD	IMPACT	CONTROL TYPE	EXISTING CONTROL DETAILS	CONTROL OWNER	EFFECTIVENESS		LIKELIHOOD	IMPACT		ACTION PLAN DETAILS	CONTROL OWNER	DEADLINE	
					SCORE: RATING							SCORE: RATING						

EXECUTIVE SUMMARY REPORT ON RISK MANAGEMENT

To	: Risk Management Committee (RMC)	Reference :
From	: Project sponsor/ Project Director/ Project Manager/ HOD	Date :
Subject	: Executive Summary Report on Risk Assessment for _____	Period :

MANAGEMENT ASSERTION
(Covering period of assessment_____/_____)

AsProject Sponsor/ Project Director/ Project Manager/ HeadofDepartment _____ (designation or position) of _____(name of subsidiary/project), I have primary accountability for providing reasonable assurance on internal control for my _____(area of responsibility).

In order to provide this assurance for _____(name of subsidiary/area of responsibility), I have ensured that there is an ongoing system of risk identification and assessment.

For the period in question, _____(name of subsidiary/area of responsibility) has assessed all material risks. These material risks will be formally monitored on a routine basis and reported on a quarterly basis. Where exposure is considered acceptable, we will document and validate the control activities are in place and are effective.

Where an individual risk has been assessed as unacceptable, individuals have been identified to develop plans for corrective action to address the risk. These plans for corrective action will be developed and implemented in a timely manner.

To the extent that the individual risk is not perceived to be within my control (either directly or as delegated to my immediate Management team), it will be documented and elevated to the appropriate level of Management within I-Berhad Group.

If any warning signs of material risks or any significant unforeseen events occur, they will be immediately escalated to the appropriate level of Management within I-Berhad Group. Where a breakdown in our controls has occurred, which might result in or could have resulted in a material effect on the business, it will be escalated so that lessons (on the risk and its resolution) can be learnt across the Group, generating improvement in our management of risk.

I also confirm that all employees under my supervision and I, have adopted and complied with the requirements of I-Berhad Group's Risk Management Policy and Risk Management Framework.

Signature :   Date :

Name :

Position :