	RISK MANAGEMENT SECTION	**Revision**	1st Edition
		Date Published	21 November, 2014

ZELAN BERHAD 27676-V

ENTERPRISE RISK MANAGEMENT POLICY AND FRAMEWORK

1.0 INTRODUCTION

Risk management is a part of Zelan Berhad Group of Companies' ("ZB") strategy to promote accountability through good governance and robust business practices, to support our 4 strategic objectives:

i. Maximise Shareholder Value;
ii. Service Excellence to Stakeholders;
iii. Lead in Value Innovation; and
iv. Be the Preferred Employer.

The Enterprise Risk Management ("ERM") Policy and Framework set out the process for managing risks across the ZB. This document outlines how the organization ensures risks are managed effectively and efficiently. It illustrates how risk management is embedded in our organisational systems to ensure that it is integrated at all levels and work contexts. It describes the key principles, elements and processes to guide staff in effectively managing risks, making it part of our day-to-day decision-making and business practices.

ZB applies risk management across the entire organisation — ZB Head Office and Operating Companies as well as specific functions, programs, projects and activities. Implementation of the policy and framework strengthens management practices, decision making and resource allocation process, while at the same time protects stakeholders' interests and maintains trust and confidence.

This Policy shall be presented to the Audit Committee and be recommended for approval to the Board of the ZB before it is adopted.

2.0 POLICY STATEMENT

ZB is committed to embed risk management principles and practices into its organisational culture, governance, planning, reporting, performance review, business transformation and improvement processes. ZB will establish and communicate its risk appetite to guide staff in their actions relating to the organization's risk acceptance level. To position ZB as a risk-aware, responsive and resilient organisation, our risk management approach is directed through:

i. Keeping abreast with external and internal developments and risks which can have an effect on the organization.

ii. Effective identification and management of risks at all levels in the organization.

iii. Compliance with relevant legislations, policies and procedures.

iv. Alignment with standards and best practices to soundly support decision making and continuous improvement of our risk management practices.

Effective risk management practice is modelled by:

i. Leadership demonstrated by the Board of Directors, Managing Director and Management Teams.

ii. Staff in all work contexts through their identification, analysis, evaluation, treatment, monitoring and review of risks that may impact on achieving our organisational purpose and objectives.

3.0 OBJECTIVES

The objectives of the Enterprise Risk Management Policy and Framework are as follows:-

i. Provide a policy and organizational structure for the management of risks within the Group.

ii. Define risk management roles and responsibilities within the Group and outlining procedures to mitigate risks.

iii. Ensure consistent and acceptable risk management practices throughout the Group.

iv. Define the reporting framework to ensure clear communication on all risk management activities and reporting.

v. Accommodate the changing risk management needs of the Group while maintaining control of the overall risks.

vi. Detail the approved methodology for risk assessment.

vii. Provide centralized consolidation of risk management data and reporting.

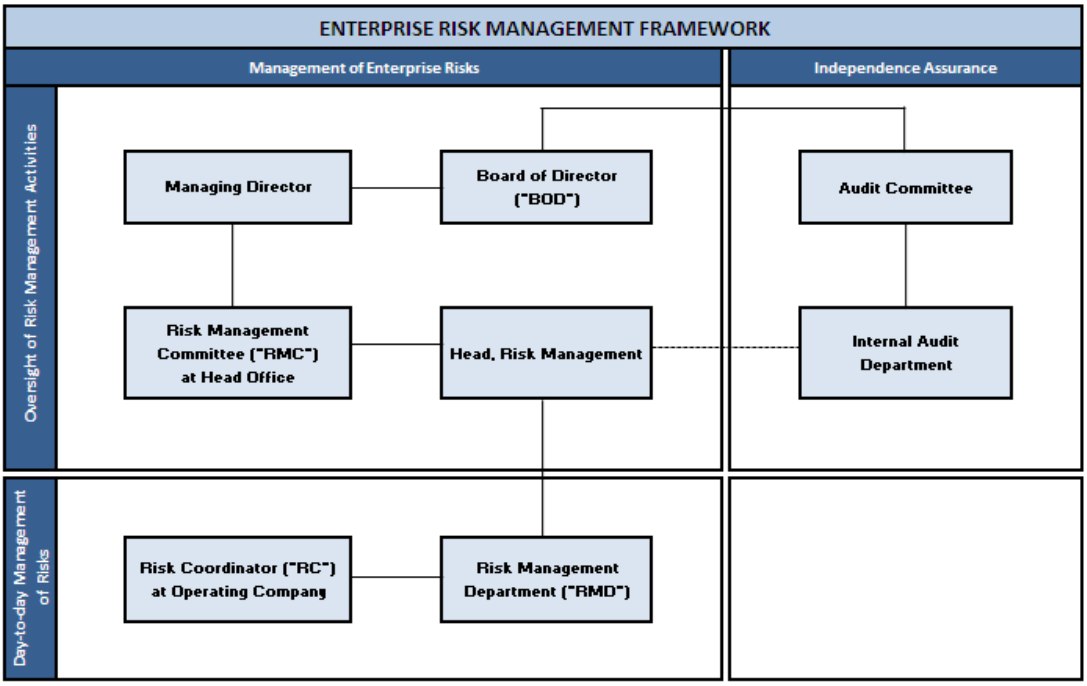
4.0 ENTERPRISE RISK MANAGEMENT ("ERM") FRAMEWORK

ERM is a process adopted by the Board, Management and all personnel. It is applied in a strategy setting across the organisation (including for projects and by subsidiaries) to assist to identify risks and manage it effectively. This is to provide reasonable assurance on the achievement of business objectives.

The ERM Framework helps to ensure that risks are managed across the Group in a holistic manner, is integrated into our culture, business practices and business plans, is inclusive of all levels of staff and is applied in a consistent manner.

ERM supports the needs of the Group at both the Operating Companies and ZB Head Office. The most important element of this structure is the clear definition and communication of the roles, responsibilities and accountabilities for managing risks within the organization.

An overview of the Framework is provided in the diagram below. The diagram illustrates the key elements necessary for managing risk and the integration of these elements at all levels and in all work contexts.



5.0 REPORTING REQUIREMENT

The establishment and implementation of the ERM framework requires Operating Companies and ZB Head Office to submit quarterly risk management reports or as and when required based on the emergence of new risks following the Group's risk management organization structure via an enterprise risk management system.

6.0 ENTERPRISE RISK MANAGEMENT PROCESS

Figure 1 below illustrates the 7 steps of risk management process. The detailed process is set out in ***Appendix 1***.

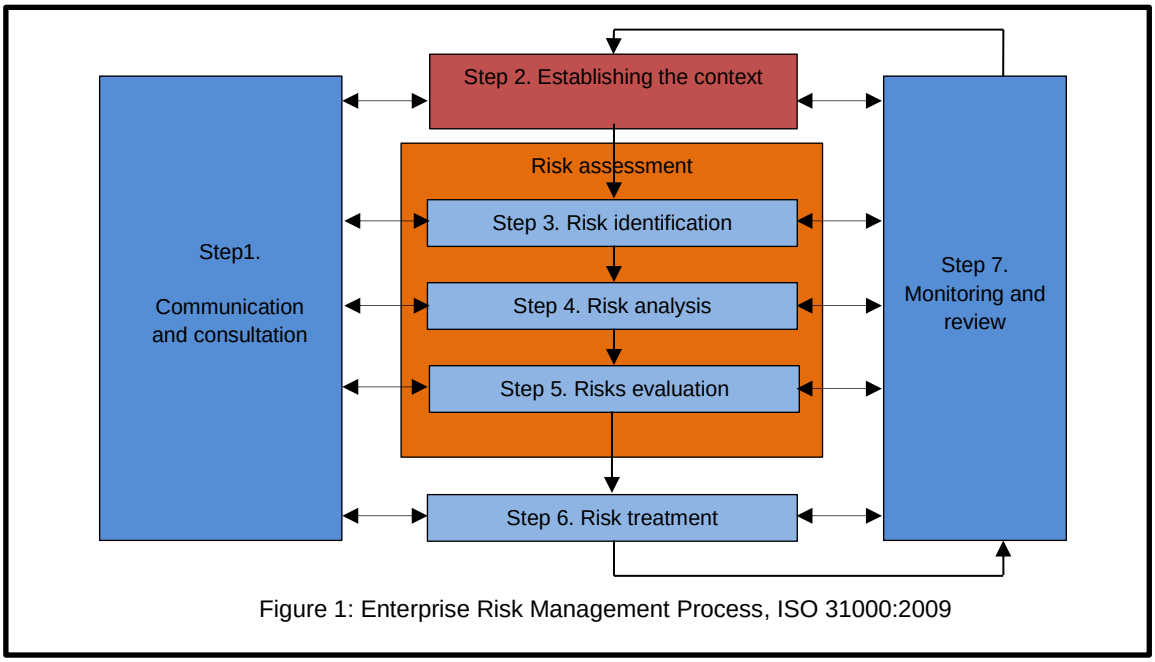


Figure 1: Enterprise Risk Management Process, ISO 31000:2009

7.0 ROLES AND RESPONSIBILITIES

7.1 Board of Directors

The Board of Directors is ultimately responsible for all elements of risk management and internal control in the ZB Group of Companies. This is consistent with the principal responsibilities of the Board of Directors as set out under the Malaysian Code of Corporate Governance.

The Board of Directors shall:

i. Satisfy themselves that significant risks faced by the Group are being managed appropriately and that the system of risk management within the Group is robust enough to respond to changes in the business environment.

ii. Ensure that an appropriate organization and reporting structure as well as system are established to support the delivery and communication on this policy on an ongoing basis.

iii. Adequately discuss and provide challenge on issues of risk and opportunity, their treatment and the overall risk appetite and risk portfolio of the Group.

The Board of Directors, who is responsible for the system of risk management and internal control throughout the Group, has delegated the above responsibility to the Risk Management Committee.

7.2 Risk Management Committee (RMC)

The RMC is responsible to assist the Board of Directors to oversee the establishment and implementation of an enterprise risk management system. The Committee is also responsible to review the effectiveness of the system annually.

The Terms of Reference for RMC are attached in ***Appendix 2.***

7.3 Risk Management Department (RMD)

RMD is responsible to assist the RMC in carrying out the implementation of risk management in the respective Operating Companies/ ZB Head Office.

The RMD roles and responsibilities are:-

i. Lead, direct, coordinate and ensure application of Enterprise Risk Management (ERM) in the ZB Group of Companies.

ii. Ensure that the principles and requirements of managing risk are consistently adopted throughout the Group, and to establish an ERM framework with appropriate resource to assist the Group in its realisation of business objectives and continual development.

iii. Ensure that risk identification and assessment activities carried across the Group are reviewed and challenged where necessary and appropriate escalation procedures are in place at the highest level.

iv. Provide consolidated reporting, inclusive of an overall risk profiles and ensure that major risks are identified and reported to the Board.

v. Produce the Quarterly Group Risk Management Reports and Annual Statement on Risk Management and Internal Control for the RMC and BOD.

vi. Monitor the overall risk management performance at Group level and to ensure the effective and timely reporting of risk management information within the Group's operating divisions, subsidiaries and support functions.

vii. Support senior management with any aspect of risk management development and oversee key risk management training initiatives.

7.4 Risk Coordinator (RC)

Operating Companies and ZB Head Office are responsible for the appointment of a RC who will be responsible for risk reporting, risk monitoring, risk advisory and risk communication for their company and departments in their company.

The RC roles and responsibilities are to be incorporated into the RC's Job Descriptions.

The RC plays an important role together with the RMD in ensuring the successful establishment and implementation of the ERM framework throughout ZB Group of Companies. The detailed roles and responsibilities of the Risk Coordinator are as per ***Appendix 3.***

7.5 Risk Owner (RO)

RO is a named individual accountable for all aspects of the risk including identification, assessment, evaluation, monitoring and reporting for the area under their purview. He/she is the best person to take appropriate decisions and adequate control to manage the risk in question.

The detailed roles and responsibilities of the RO are attached in ***Appendix 4.***

7.6 Management and Head of Division/Department

The Management and Head of Division/Department has a front line responsibility for identifying and evaluating risks within their area of responsibility, implementing agreed actions to manage risk and for reporting any activity or circumstance that may give rise to new or changed risks.

Management and the Head of Division/Department shall ensure that appropriate controls are in place to manage identified risks including the formulation of preventive and contingency plans where necessary by performing monthly compliance and assessment in the ERM risk register.

7.7 Employees

All employees have a general duty of care and are responsible to comply with the ERM Policy and Framework. It is the duty of all ZB Group of Companies' employees to be conscious of the risks related to their actions and decisions.

8.0 CONFIDENTIALITY

The information contained within any document dealing with ZB's business risks is to be treated as highly CONFIDENTIAL and should not be released to any outside parties without the prior consent of the Board of Directors.

9.0 DOCUMENT CHANGES

This document is authorized by the RMC. It is a controlled document and is subject to update and if copied, must be marked "Uncontrolled Copy".

Changes are only be authorized by the RMC. Any change to this Policy will result in a change to the revision status and complete reissuance of the Policy.

Records of all changes made to the Policy shall be maintained by the RMD.

APPENDIX 1

ENTERPRISE RISK MANAGEMENT PROCESS

Step 1: Communication and Consultation

Communication and consultation with internal and external stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage.

These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

Step 2: Establishing the Context

By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.

i. Establishing the external context

The external context is the external environment in which the organization seeks to achieve its objectives.

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

a. The social and cultural, political, legal, regulatory, financial, technological, economic, natural

b. Competitive environment, whether international, national, regional or local;

c. Key drivers and trends having impact on the objectives of the organization

d. Relationships with perceptions and values of external stakeholders.

ii. Establishing the internal context

The internal context is the internal environment in which the organization seeks to achieve its objectives.

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way in which an organization will manage risks.

It is necessary to understand the internal context. This can include, but is not limited to:

a. Governance, organizational structure, roles and accountabilities;

b. Policies, objectives, and the strategies that are in place to achieve them;

c. Capabilities, understood in terms of resources and knowledge (e.g. Capital, time, people, processes, systems and technologies);

d. The relationships with and perceptions and values of internal stakeholders;

e. The organization's culture;

f. Information systems, information flows and decision making processes (both formal and informal);

g. Standards, guidelines and models adopted by the organization; and

h. Form and extent of contractual relationships.

iii. Establishing the context of the risk management process

The objectives, strategies, scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. The management of risks should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified.

The context of the risk management process will vary according to the needs of an organization. It can involve, but is not limited to:

a. Defining the goals and objectives of the risk management activities;

b. Defining responsibilities for and within the risk management process;

c. Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;

d. Defining the activity, process, function, project, product, service or asset in terms of time and location;

e. Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organization;

f. Defining the risk assessment methodologies;

g. Defining the way performance and effectiveness is evaluated in the management of risk;

h. Identifying and specifying the decisions that have to be made; and

i. Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

Attention to these and other relevant factors should help ensure that the risk management approach adopted is appropriate to the circumstances, to the organization and to the risks affecting the achievement of its objectives.

iv. Defining risk criteria

The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy, be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered should include the following:

a. The nature and types of causes and consequences that can occur and how they will be measured;

b. How likelihood will be defined;

c. The timeframe(s) of the likelihood and/or consequence(s);

d. How the level of risk is to be determined;

e. The views of stakeholders;

f. The level at which risk becomes acceptable or tolerable; and

g. Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

Risk Assessment

Risk Assessment is the overall process of risk identification, risk analysis and risk evaluation.

Step 3: Risk Identification

i. Risk identification is a line management's responsibility. All risks identified will be evaluated and documented, together with the controls, action plans and a Risk Owner (RO) who is accountable for the risks.

ii. For each risk, accountability is assigned to the person best able to take appropriate decisions to manage the risk in question.

iii. RO is a named individual accountable for all aspects of the risk including assessment, evaluation, monitoring and reporting.

iv. The responsibility of the adequacy of control of each risk rests with the assigned RO.

v. RO may delegate tasks of managing the risks to others. However, the responsibilities over the risks still remain with the RO. The delegated task owner would then report the progress back to the RO.

vi. Risk Register

The Risk Register records details of all the risks identified, their grading in terms of likelihood of occurring and seriousness of impact to ZB's, existing controls on identified risk, plans for mitigating the risk, the costs and responsibilities of the prescribed mitigation strategies and subsequent results.

vii. The sample risk register to be used consist of the following:

Part 1: Risk Identification & Measurement

a. Risk title

b. Risk ID

c. Risk Category

d. Risk Description

e. Risk Owner (a person)

f. Internal/External Causes

g. Consequences

h. Gross Risk Rating (without any control) as per established risk parameter

Part 2: Risk Evaluation and Analysis

a. Current control - the existing internal controls that may minimise the likelihood of the risk occurring

b. Residual Risk Rating, Current Quarter (with current control in place) as per established risk parameter

c. Control Effectiveness – Very good/Good/ Satisfactory/ Some Weaknesses/ Weak

Part 3: Risk Treatment

a. Target Residual Rating as per established risk parameter

b. Additional control – if the current control is not sufficient

Part 4: Risk Mitigation Plan

a. Summary of Mitigation Plan Status

b. Mitigation Plan

c. Plan Owner

d. Plan Co-Owner

e. Start date

f. Target Completion date

g. Quarterly status – Completed/ Due/ Postpone/ In Progress as Planned/ Not yet started

h. Remark

viii. A grading of each risk according to a risk assessment matrix is tabulated below. A table is used to calculate the IMPACT + LIKELIHOOD of risk occurrence. Scoring is then given to provide an indication on the magnitude of the risk to ZB's.

Risk Matrix Table

IMPACT / LIKELIHOOD	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	6	7	8	9	10
Likely	5	6	7	8	9
Possible	4	5	6	7	8
Unlikely	3	4	5	6	7
Rare	2	3	4	5	6

Legend

RISK SCORE
EXTREME (8-10)
HIGH (6-7)
MODERATE (4-5)
LOW (2-3)

ix. Risk Categories

The **9** categories of risks are defined below: -

No.	Risk Category	Description
1	Financial Risk	Exposure related to loss of monetary resources or incurring unacceptable liabilities.
2	Business & Strategic Risk	• Exposure to uncertainty arising from long-term or short-term policy decisions based on current strategy of operating unit. • Exposure to uncertainty due to competition and/or fiscal policy changes. Risks that are external to the operating unit and beyond the control of the organization.
3	Operational Risk	Exposure to uncertainty arising from daily tactical business activities related to Business Processes & Technology.
4	Reputation Risk	Exposure to uncertainty arising from organization brand or image.
5	Information Risk	Exposure to uncertainty arising from loss or inaccuracy of data, IT systems or reported information.

No.	Risk Category	Description
6	Organizational Risk	• Risks arising from poor communication systems property/casualty insurance. • Risk associated with organizational structure, employees (skills, competency, etc.) and management.
7	Regulatory Risk	Exposure to uncertainty arising from inadequacy in compliance to required mandatory or established regulations and policies.
8	Fraud Risk	Exposure to uncertainty arising from dishonest act with intend to cheat in a corporation whereby certain parties may unlawfully benefit from the act/deal.
9	Market Risk	Exposure to uncertainty arising from economic factors such as FOREX, commodity prices etc.

x. Type of Controls:

a. **Preventive**
Reduce or eliminate LIKELIHOOD of risk

b. **Detective**
Identify impending risks which are about to take place – reduce LIKELIHOOD; or identify events which may further deteriorate – reduce IMPACT

c. **Corrective**
Minimise losses and enable prompt recovery – reduce IMPACT

Step 4: Risk Analysis

i. Risk analysis allows an entity to consider the extent to which the potential events might have an impact on the achievement of the company's objectives.

ii. "Risk Score" is an assessment of the risk's seriousness and is based on the **LIKELIHOOD** or **PROBABILITY** of the risk actually arising; and the IMPACT or **CONSEQUENCES** on the ZB if a risk does actually arise.

iii. The Risk Likelihood measurement below is a default measurement based on the expected frequency of risk occurring every quarter. This measurement may be adjusted based on the company's performance.

Scales	Probability	Description
Almost Certain	> 75%	Almost certain to occur
Likely	51% – 75%	More likely to occur than not
Possible	26% - 50%	Fairly likely to occur
Unlikely	6% - 25%	Unlikely to occur
Rare	0% - 5%	Extremely unlikely

iv. The parameters on setting the impact is tabulated below.

FACTOR	CONSEQUENCES (FINANCIAL & NON-FINANCIAL)				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
1. Revenue against Budget for the FY	< 1%	< 3%	< 5%	< 10%	> 10%
2. Impact on PBT against budget for the FY	< 1%	< 3%	< 5%	< 10%	> 10%
3. Investment income budget for the FY (Dividend at MMC level)	< 1%	< 3%	< 5%	< 10%	> 10%
4. Shortfall of new businesses / projects against budget for the FY	< 10%	< 20%	< 30%	< 40%	> 40%
5. Impairment of Asset / Investment against value / cost	< 1%	< 3%	< 5%	< 10%	> 10%
6. Funds Availability	Sustainable more than 4 months	Sustainable less than 4 months	Sustainable less than 3 months	Sustainable less than 2 months	Sustainable less than 1 month
7. Project Management	Project delay < 1% of budgeted timeline. or Cost overrun of < 1% of contract value (by project type).	Project delay < 3% of budgeted timeline. or Cost overrun of < 3% of contract value (by project type).	Project delay < 5% of budgeted timeline. or Cost overrun of < 5% of contract value (by project type).	Project delay < 10% of budgeted timeline. or Cost overrun of < 10% of contract value (by project type).	Project delay > 10% of budgeted timeline. or Cost overrun of > 10% of contract value (by project type).
8. Occupational, Health & Safety	First Aid only required.	Minor medical treatment with or without potential for lost time.	Significant injury involving medical treatment or hospitalisation and lost time.	Individual fatality or serious long term injury.	Multiple fatalities or extensive long term injury.
9. Image & Reputation	Isolated, internal or minimal adverse attention or complaint.	Heightened local community concern or criticism.	Significant public criticism with or without media attention.	Serious public or media outcry; broad media attention.	Extensive public outcry; potential national media attention.
10. Environmental & Natural Hazards	Minimal physical or environmental impact; isolated hazards only; dealt with through normal operations.	Minor physical or environmental impact; hazards immediately controlled with local resources.	Significant physical or environmental impact; hazards contained with assistance of external resources.	Major physical or environmental impact; hazard extending off-site; external services required to manage.	Extensive physical or environmental impact extending off-site; managed by external services; long term remediation required.

FACTOR	CONSEQUENCES (FINANCIAL & NON-FINANCIAL)				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
11 Regulatory & Governance	Isolated non-compliance or breach; minimal failure of internal controls managed by normal operations.	Contained non-compliance or breach with short term significance; some impact on normal operations.	Serious breach involving statutory authority or investigation; significant failure of internal controls; adverse publicity at local level.	Major breach with formal inquiry; critical failure of internal controls; widespread adverse publicity.	Extensive breach involving multiple individuals; potential litigation; viability of organisation threatened.
12. Contractual & Legal	Isolated non-compliance or breach; negligible financial and non-financial impact. (Non-financial impact can include loss of reputation, goodwill, customer confidence, opportunities, loss of employee morale etc.)	Contained non-compliance or breach with short term significance and minor financial and non-financial impact.	Serious breach and non-compliance including prosecution by relevant statutory authority/authorities with some adverse financial and non-financial impact.	Major breach and non-compliance leading to major fines/penalty and legal claims; with long term significance and major adverse financial and non-financial impact.	Massive fines/ penalty and legal claims with possible threat to viability of project or company leading to massive adverse financial and non-financial impact.
13. Human Resource	<3% of overall staff turnover	<7% of overall staff turnover	<10% of overall staff turnover	<15% of overall staff turnover	More than 15% of overall staff turnover
	One(1) Key Staff (HOD/GM and above) left	Two(2) Key Staff (HOD/GM and above) left	Three(3) Key Staff (HOD/GM and above) left	Four(4) Key Staff (HOD/GM and above) left	More than 4 Key Staff (HOD/GM and above) left
	Employees Satisfaction Index >80%	Employees Satisfaction Index <80%	Employees Satisfaction Index <72%	Employees Satisfaction Index <65%	Employees Satisfaction Index <50%

v. Three assessments of risk status are needed:

a. **Gross Risk**

Risk status before existing mitigation – an assessment of the risk happening and its impact if no action is taken.

b. **Residual Risk**

Risk status after existing mitigation – an assessment of the risk happening and its impact, taking account of existing actions aimed at reducing the risk.

c. **Target Residual Risk**

Risk status after future mitigation – an assessment of the risk level we will reach after all the mitigating actions identified have been done.

vi. If after existing mitigation, the risk status is acceptable then the risk should be tolerated; there is nothing more to do. But if the status remains unacceptable (bearing in mind our risk appetite) then further mitigating actions should be identified.

Step 5: Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

i. Implementation of Mitigation Strategies (Action Plans)

It is the responsibility of the relevant operational and functional heads to implement the mitigation strategies identified in the Risk Register developed during the Risk Identification process.

Where current controls are deemed ineffective, appropriate actions plans will be developed by the management to mitigate the risks. Allocation of accountabilities and action dates for the implementation of the action plans need to be established. Risk mitigation strategies involves identifying the range of options for treating risks, assessing those options, preparing action plans and implementing those plans.

ii. The Action Plans must follow the "**SMART**" principles:

Specific	Action Plans must be detailed and exact.
Measurable	Action Plans must be measurable in nature i.e. financial impact.
Achievable	Action Plans must have a targeted objective that is achievable.
Realistic	Action Plans must be realistic where actual results can be produced.
Time-Based	Action Plans must have time-line for execution and targeted achievement results.

Step 6: Risk Treatment

Risk Treatment is the process of selecting and implementing of measures to modify risk. Risk treatment measures can include terminate, reduce, accept, pass and spread the risk (TRAPS).

The treatment plan is how to plan to respond to potential risks. It outlines how risks will be managed whether they are low, high, or acceptable risks. The controls set in the risk management plan will assign team members or stakeholders the task of how they will respond to risk.

Terminate	By deciding not to process or avoid the activity likely to generate risks.
Reduce	Introducing controls or action plans to reduce the significance of the risks.
Accept	Using the abilities of the Group to accept the risks in order to build a competitive edge over other competitors.
Pass	By transferring the consequences of risks to third parties e.g. insurance, hedging, etc.
Spread	By sharing the occurrence of risks with third parties e.g. joint ventures, outsourcing, etc.

Step 7: Monitoring and Review

i. Monitoring

Monitoring and reviewing of risks forms an essential and integral part of the risk management process.

The objectives of monitoring and reviewing the risk management process are:

- To provide reasonable assurance that risks are being managed effectively as expected.
- To ensure that risk profiles anticipated and reflects the changing business conditions and exposures.

The objectives are achieved through the deployment and implementation of the following activities:

- Digital confirmation and sign-off from the MD is to be carried out on a quarterly basis.
- Review on the effectiveness of controls and action plans implemented against established risk appetites.
- Periodic review on the effectiveness of and compliance to the risk management process adopted by ZB by the Group Internal Audit Department.

ii. Reporting

Regular risk reporting is essential for information management and business planning. Formal reporting has been instituted at various levels of the organization (including the Subsidiaries' Board) to highlight the significant risks identified by the business during the previous period and business planning cycles.

On a quarterly basis, the MD and Head of Corporate Divisions/Department will assess and update the relevant risk information via the Enterprise Risk Management Register.

For the purpose of the quarterly risk management reporting to the ZB's Board of Directors, the Risk Management Department should only extracts from the Register the risks that are rated as "**high**" and above (as per ZB's established risk score).

The risks are then compiled into the Group's risk management quarterly reports and submitted to the Risk Management Committee (RMC). The reports are subsequently tabled to the Board of Directors (BOD).

The Board then reviews and approve the reports each quarter so that they are aware of major risks within the Group and ensure that appropriate actions are taken by the management to mitigate the risks.

APPENDIX 2

Terms of Reference for Risk Management Committee

Objective	Risk Management Committee (RMC) within the company is essential to discuss and manage all the risks related to strategic and operations of the company. The RMC will discuss on risks, formulate strategies in managing such risks and forward the strategies and recommendations to the BOD.
Members	1. Chairman – MD for ZB head office and Head for operating companies. In the absence of the Chairman, the appointed alternate Chairman will chair the meeting. 2. Members - Head of Departments.
Secretary	The Risk Coordinator shall act as the Secretary of the Committee, unless otherwise determined by the Chairman of the Committee.
Quorum	The quorum shall comprise the Chairman and Head of Departments (subject to Chairman approval).
Frequency of Meetings	The committee shall meet every quarter and at such other times as the Chairman of the Committee considers necessary.
Reporting process	ZB Head Office 1. All risk reports must be submitted to the Risk Coordinator one (1) week before the Head Office RMC. 2. The RMC shall determine the key risks that need to be reported to the BOD. Operating Companies 1. All risk reports must be submitted to the Risk Coordinators one (1) week before the Head Office RMC. 2. The RMC shall determine the key risks that need to be reported to their respective BOD. 3. Subsequently the report will be reported to the RMC of Head Office.
Responsibilities	1. Responsible for the continuous development of risk management system in the respective Operating Companies/ZB Head Office and supervise the implementation of risk management in compliance with the ERM Policy and Framework. 2. Conduct RMC meetings on a quarterly basis. 3. Ensure that risks identified are reviewed prior to reporting to the BOD of ZB. 4. Decide on the status and further action on matters arising with regards to the identified risks. 5. Identify key risk at the Operating Companies/ ZB Head Office that need to be escalated to the BOD of ZB.
Responsibilities	6. Review and enhance the company risk management structure to sustain the ERM framework and support the ongoing delivery of risk management objectives. 7. Review and enhance the company Risk Assessment process. 8. To ensure that the ERM Policy and Framework have been adopted accordingly.

APPENDIX 3

Risk Coordinator Roles and Responsibilities

Operating Companies and ZB Head Office are responsible to appointment a Risk Coordinator who will be responsible for the roles defined below.

Risk Reporting and Monitoring	1. Coordinate the quarterly risk reporting and monitoring processes at company level. 2. Facilitate the identification and assessment of risks to business objectives. 3. Identify and reporting the critical risks and its current status. 4. Monitor and reporting the implementation of approved mitigation plans to the Chairman of the RMC. 5. Ensure that appropriate controls are in place by risk owners to manage identified risks including the formulation of preventative and contingency plans where necessary. 6. Check accuracy of information updated in the Enterprise Risk Management System (ERMS). 7. Compile and submit company risk report to the company Risk Management Committee.
Risk Advisory	1. Review, propose and implement an appropriate risk management structure within the company level. 2. Provide support to the senior management of the company in risk issues. 3. Keep abreast of new developments in Group Risk Management. 4. Act as a focal point for all RM support and advice to the company. 5. Ensure that full consideration and commentary on risks are provided to support the business strategy and planning cycle.
Risk Communication	1. Communicate enterprise risk management strategies, policies and processes together with defined responsibilities to all management and staff within the company. 2. Engage in dialogue and discussion with management and staff within the company to promote risk management awareness and its practical implementation.

APPENDIX 4

Risk Owner Roles and Responsibilities

Risk owners identified in each department within the Operating Companies and ZB Head Office are responsible for the roles defined below:-

Risk Reporting and Monitoring	1. Identify and evaluate risks within the area of responsibility. 2. Ensure that appropriate controls and mitigation plans are in place to manage identified risks. 3. Monitor and report the implementation of approved mitigation plans. 4. Perform monthly compliance and assessment in the ERM risk register.
Risk Review	1. Identify and evaluate emerging risks within the area of responsibility. 2. Review the operating division's / department's Internal/external audit reports in order to identify issues related risks. 3. Ensure that full consideration and commentary on risk mitigation plans are provided to support business strategy and the planning cycle. 4. Ensure that sufficient budget is available to carry out the relevant mitigation plans and/or existing controls. 5. Update information into the online MMCB Enterprise Risk Management System (ERMS).