PROGRAM TITLE

COMPLIANCE AND RISK MANAGEMENT

PROCESS TITLE

Risk Assessment and Monitoring

1. SCOPE

This policies and procedures manual establishes policies, systems, procedures and controls on risk assessment and monitoring. All duties and responsibilities stated in this manual are not exclusive to the personnel’s designated responsibilities in this process title.

1. OBJECTIVES

* To provide risk management procedures consistent with and supportive of the Company’s goals and objectives.
* To provide guidelines on the risk management strategies and action steps for building and executing risk management capabilities and improving them continuously.
* To provide clear monitoring of the risks and countermeasures to assist the Company in its decision-making function.
* To clearly define the duties and responsibilities of all personnel involved in this process title.

1. PERSONNEL INVOLVED
   1. Senior management
      1. Discusses with the Department Managers of the risk assessment procedures conducted.
      2. Approves the Risk Assessment Form (RAF) based on the discussions conducted.
      3. Analyzes the risks being presented by the Department Managers and determine necessary response to the identified risks.
   2. Department Managers
      1. Determines the following details, using the risk assessment tools and techniques, for the preparation of the RAF:

* Risk Type
* Risk Owner
* Description of Risk
* Potential Root Cause
* Potential Damages
* Mitigation Measures in Place
* Risk Scores (Severity, Likelihood and Mitigation)
  + 1. Prepares the RAF.
    2. Proposes and discusses with the Senior Management any revision or addition to the existing controls and mitigation measures in place.
    3. Facilitates the implementation of the approved risk controls and mitigation measures.
    4. Conducts constant regular evaluation of the existing controls in place for any possible vulnerabilities and threats.
  1. Compliance Department
     1. Receives and files duly approved RAF.
     2. Updates the Risk Register on the progress of risk assessment procedures being implemented.
     3. Assists in the monitoring and evaluation of controls and mitigation measures currently in place.
     4. Conducts constant regular evaluation of the existing controls in place for any possible vulnerabilities and threats.

1. KEY TERMS
   1. *Risk* – The uncertainty of outcome, within a range of potential exposures, arising from a combination of the impact, the likelihood of potential events and the existing mitigating measures in place. Risks can be opportunities overlooked as well as threats to the achievement of objectives.
   2. *Risk Owner* – The designated personnel with responsibility for the management, monitoring and control of an identified risk, including the implementation of the selected responses.
   3. *Risk Management* – The process of identifying risks, evaluating their potential consequences and determining the most effective methods of controlling them and or responding to them.
   4. *Assurance* – Gaining confirmation that risk assessment and control response is appropriate, adequate and achieving the effects for which it has been designed.
   5. *Risk Appetite* – The range of exposure that is judged tolerable for the Company.
   6. *Vulnerabilities* – These are the weaknesses that has been identified which can result in a potential damaging impact on the business. Vulnerabilities are ‘internal’ to the Company.
   7. *Potential Threats* – These are ‘external’ causes which can exploit vulnerabilities to cause damage.
   8. *Senior Management* – The senior management shall pertain to the Board of Directors, President, Senior Vice Presidents and Vice Presidents.
2. POLICIES
   1. **General Policies**
      1. Risk Assessment Form shall be duly filled-out and signed by designated signatories. Any details/signatories which are not applicable must be duly indicated with “N/A”.
      2. Alterations, if any, on the business forms shall be duly countersigned.
   2. **Control Environment**
      1. The control environment is the set of standards, processes, and structures to provide basis for carrying out internal control across the Company.
      2. The control environment of the Company comprises, at a minimum, the following:

* The Company’s goals and objectives;
* Company integrity and ethical values;
* Markets and geographies in which the Company operates;
* Regulatory and statutory requirements in which the Company is required to comply with;
* The products and services the Company provides to those market, the channels it uses to access those markets and the characteristics by which it differentiates its products and services in the eyes of the customer.
* The process through which the Company converts materials and labor into products and services;
* Current existing activities and projects of the Company;
* On the employees the Company hires, trains and retains;
* On the suppliers and customers in which the Company does business; and
* The shareholders and lenders that supply the Company’s capital.
  1. **Risk Assessment**
     1. Risk assessment involves a dynamic and iterative process of identifying and assessing risks to the achievement of the Company’s objectives. Risks to the achievement of the Company’s objectives are considered relative to establish risk appetites. Thus, this will be the basis for determining how the risks will be managed.
     2. Each level of management (SVP, VP, Managerial) must consider and regularly review the control environment in order to ensure that all relevant risks have been identified.
     3. If necessary, crossing of each management’s area of responsibility may be considered to obtain a more comprehensive risk assessment and for partnership risks to also be considered.
     4. Any new and emerging risks which may become apparent throughout the year must be assessed. Any changes in the existing risks must be reassessed and the Risk Register must be updated accordingly.
     5. The following factors shall be considered when identifying risks:
* Any previous risk assessment which may have been undertaken in relation to the Company’s goals and objectives;
* Any areas which have been subject to significant recent change;
* Any new or innovative practice or business areas;
* Risk register – this will indicate which incidents have occurred in the past, how often they occurred and what the consequences were;
* All key activities of the Company’s business;
* Key Question List *(Appendix A)*
* Type of Risk *(Appendix B)*
  + 1. The following criteria may be considered in the evaluation of identified risks:
* Financial – value for money issues
* Service Delivery – quality of services issues
* Reversibility or realization of the risk
* Quality or reliability of the evidence surrounding the risk
* Impact of the risk on the Company, its clients, partners, and others.
* Defensibility of the realization of the risk
  + 1. When evaluating the risk which have been identified, the **impact** or **severity** of the event if it occurred, the **likelihood** of the event occurring and the existing **mitigating measures** must be considered. *(See Annex D)*
    2. For each risk, a **Risk Magnitude Score (RMS)** must be determined to help rank the identified risks and the causes for the identified risks in order of level of priority.
    3. Risk appetite must be considered by the Company to ensure that risks are managed to an acceptable level. Before any decisions can be made on how to respond to certain risks, the amount of risks which the Company can tolerate must be determined.
    4. The measure of risk appetite must be determined at an overall organizational level and an individual risk level. The Executive Department will determine the maximum overall exposure to risk that should be accepted, based on the benefits and the costs involved. Once the organizational risk appetite has been set, the department managers can then determine the risk appetite for individual projects and activities.
    5. When the risk appetite has been applied by the management, the net risk score must be compared with the risk appetite:
* Net risk score is lower than the determined level of risk appetite, the risk can be tolerated and therefore no further response is required
* Net risk score is higher than the determined level of risk appetite, a response is required in order to bring the level to an acceptable level or as low as reasonable possible.
  1. **Control Activities**
     1. The control activities are the actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out.
     2. Control activities are to be performed at all levels of the Company, at various stages within the business processes, and over the technology environment.
     3. Sample control activities may be taken upon establishment of the RMS:

|  |  |
| --- | --- |
| **Response** | **Description** |
| Transfer | The risk is transferred to a third party (e.g. insurance, IT supplier) |
| Tolerate | The level of risk is thin the risk appetite of the Company |
| The cost of taking any action may be disproportionate to the potential benefit gained |
| Treat (Mitigate) | Actions are taken to contain the risk to an acceptable level (internal controls) |
| Either the likelihood or the impact of the risk may be reduced |
| Terminate | The risk cannot be reduced to a tolerable level and is a threat to the achievement of objectives and must be terminated |

Risks with a high likelihood and impact must be addressed while the lesser risks may be less critical and may therefore be within the risk appetite of the organization.

* + 1. When deciding the response to a risk, cost consideration must be considered in taking the appropriate response in relation to the risk which it is controlling.
    2. The responses to risk must also be in proportion with the risk which they address. Over control of any minor risks must be avoided as well as the under control of serious risks.
    3. Any internal controls which are put in place must be properly documented and also be regularly reviewed to ensure that they remain effective and continue to offer the best value for money response to risk.
    4. Before determining whether any additional internal controls are required to be applied to the risk, the current existing controls must be considered. If the existing controls are ineffective to reduce the net risk score, a further response will be required.
  1. **Information and Communication**
     1. Information is necessary for the entity to carry out mitigating measures to support the achievement of the Company’s goals and objectives. Communication is the continual, iterative process of providing, sharing and obtaining necessary information. It enables the Company’s personnel to receive a clear message from the senior management that control responsibilities must be taken seriously.
     2. The following table shows the relationship of information and communication to the other policies in the manual:

|  |  |  |
| --- | --- | --- |
|  | **Information Component** | **Communication Component** |
| Control Environment | Written manuals and Code of Conduct | Management’s message to employees concerning ethics through their daily words and actions. |
| Risk Assessment | Documentations produced from a risk assessment | A subject matter expert’s description of a process during a risk assessment meeting. |
| Control Activities | Written policies and procedures | A manager’s review of pertinent policies with key employees. |
| Monitoring | A written plan to review a sample of transactions to test a control | A weekly staff debrief after a supervisor’s review of the sample of transactions. |

* + 1. Effective information and communication shall be applied to provide accurate and timely information on risk assessment and monitoring procedures. Effective communication shall also establish quick responses to any changes in the control environment to which the Company operates. Good communication techniques, to name a few, are as follows:

1. **A manager with an “open door” policy**

Managers can create an atmosphere where employees can communicate their concerns easily, without fear of reprisal. To accomplish a true open door policy, managers must be conscious of the subtle cues they send employees and try hard not to associate negative sentiments with the messenger, regardless of the message.

1. **Establish and promoted channels for reporting potential wrongdoing**

An infrastructure for free information flow, especially when reporting questionable actions or misconduct is effective in promoting a strong control environment and prevents fraud. It should allow for anonymity and the reporting channels should be separate from management’s reporting structure to prevent any potential barriers to the reporting of wrongdoing.

1. **An established ethics policy**

Establishing clear expectations of employee conduct and fostering a culture where ethical behavior is seen as critical is a fundamental tenet of internal control. One of the ways these ideas are communicated throughout an organization is through an established ethics policy.

1. **Internal control responsibilities are regularly communicated by management**

Effective communication ensures employees understand their internal control responsibilities relative to the larger organization. Management should ensure that all employees understand their control responsibilities.

* 1. **Monitoring Activities**
     1. Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether the controls and mitigating measures established is present and functioning. Findings are evaluated against criteria established by the senior management.
     2. A Risk Assessment Form (RAF) shall be prepared for any new or changed risk which is within the Risk Owner’s area of work. Details included on the form shall include information about the likelihood and impact of risk and the current controls in place to address the risk.
     3. The Risk Register shall be regularly updated for any new and changed risks.
     4. Evaluation of established controls and mitigating measures shall be constantly done. The monitor must be able to determine whether an activity meets, comes close to or fails to meet its goals, and the responsible staff should be able to do the same. If an activity fails, the monitor needs to know the extent of the failure and, if possible, the reason why.
     5. What monitoring steps should be included and how they should be designed and conducted depend on various determinants, including:
* **The number of an activity’s transactions.** The fewer the transactions, the easier the monitoring of the activity becomes.
* **The cost of monitoring** per transaction in money, staffing and other resources.
* **The ease of monitoring.** For example, where management can employ technology to automate and expedite monitoring, this bodes well for the overall process.
* **The risk of non-compliance – both its seriousness and likelihood**. Serious consequences of non-compliance may encourage pre-transaction approval; non-compliance that is more likely to occur can suggest a need for monitoring of more transactions.
* **Motives for operating staff not to comply**. Where staff may benefit from non-compliance, it behooves management to consider more stringent monitoring. For example, if sales staff can earn more commission from increased product dales by bypassing important paperwork, it may be important to monitor and ensure the paperwork’s timely and accurate completion.

1. PROCEDURES

| Risk Management | | | |
| --- | --- | --- | --- |
| Step No. | Activity | Personnel  Involved | Business  Forms |
| 1 | Identifies vulnerabilities in the Company’s control environment. | Department Managers | List of vulnerabilities |
| 2 | Identify possible threats to the Company.  If no risk is determined, reassess on other vulnerabilities in the Company’s control environment. | Department Managers | List of threats |
| 3 | Perform evaluation and assessment of the identified risk. | Department Managers |  |
| 4 | Examine the level of severity of the effect of the event and the corresponding likelihood of the event occurring.  Determine the severity and the likelihood of the risk on a scale of 1-5. The more critical the severity, the higher the rate. The more likelihood the event from happening, the higher the rate. | Department Managers |  |
| 5 | Determine the preventive, detective and mitigating controls in place to address the identified risk.  Determine the rate of the mitigating controls in place on a scale of 1-5. The more ineffective the controls are in place, the higher the mitigating score. | Department Managers |  |
| 6 | After determining the level of severity, likelihood and mitigating measures in place, obtain the Risk Magnitude Score (RMS) by multiplying the three scores. | Department Managers |  |
| 7 | Compare the RMS with the Company’s established risk appetite or tolerance. | Department Managers |  |
| 8 | Discuss and determine the appropriate risk response to the identified risk. The management may opt to:   * Take urgent action / Terminate * Mitigate / Treat * Transfer the risk * Tolerate / Accept | Department Managers |  |
| 9 | Identify the responsible personnel and target date of the controls and mitigating measures to be placed and implemented. | Department Managers |  |
| 10 | Prepares the Risk Assessment Form (RAF) and forwards the same to the senior management. | Department Managers | Duly filled-out RAF |
| 11 | Submits the RAF to the senior management. Present and discuss the determined vulnerabilities, threats, and mitigating measures to the senior management. | Department Managers | Duly filled-out RAF |
| 12 | Reviews the RAF and reviews the details of the risk assessment procedures conducted.  If RAF is disapproved, revise the RAF based on the discussion conducted and re-discuss with the senior management. | Senior Management | Duly approved RAF |
| 13 | Receives duly approved RAF and updates Risk Register. Files the RAF chronologically. | Compliance Department | Duly approved RAF |
| 14 | Facilitates the implementation of the planned controls and mitigating measures.  Department managers shall primarily facilitate the dissemination of information to his/her area of responsibility. | Compliance Department; Department Manager | Duly approved RAF |
| 15 | Implementation stage of the controls and mitigating measures. | Compliance Department; Department Manager | Duly approved RAF |
| 16 | Monitors and evaluates the effectivity of the controls and mitigating measures in place. | Compliance Department | Duly approved RAF |
| 17 | Update the RAF for the result of the risk assessment procedures, controls and mitigating measures effected. | Compliance Department | Duly approved RAF |
| 18 | Update the Risk Register of the results of the risk assessment and management procedures conducted. | Compliance Department | Updated Risk Register |

1. FLOWCHARTS
   1. Risk Management





1. BUSINESS FORMS
   1. Risk Assessment Form



No. of Copies/color - 1

Explanation - this form is used to document the risk assessment procedures conducted by the management and the corresponding controls taken. A Risk ID is to be indicated by the Compliance Department after approval by the Senior Management.

Prepared by - Department Manager

Approved by - Senior Management’s authorized representative

Distribution - Compliance Department (filed chronologically)

* 1. Risk Register



No. of Copies/color - 1

Explanation - this report is used to monitor the history of risks assessed and encountered by the Company. This is to be updated for every new RAF approved by the Senior Management.

Distribution - Compliance Department

1. EFFECTIVITY

This Policies and Procedures Manual shall take effect upon approval and shall supersede any memorandum/SOP inconsistent with this Policies and Procedures Manual. Any changes to the manual shall comply with the policies and procedures indicated in the process title *“Amendment of Manual”*.

**ANNEX**

ANNEX A

Key Question List

* + 1. What are the major opportunities facing the Company?
    2. How is the change affecting the risks faced and the risks that the Company has chosen to take?
    3. What are the ‘killer risks’ from which the Company would be unable to recover?
    4. What damaging press headlines need to be avoided?
    5. What problems have happened in the past in the Company or elsewhere?
    6. What are the types of fraud and business probity issues to which the Company could be particularly susceptible?
    7. What are the major regulatory and legal risks to which the Company is exposed?
    8. What risks arise from the business processes?

ANNEX B

Types of Risks

| Major Category | Minor Category | Description |
| --- | --- | --- |
| External | Infrastructure | Relating to infrastructures such as transport systems, power supply systems, suppliers, business  relationships with partners, dependency on internet and email |
| Economic | Relating to economic factors such as interest rates, exchange rates, inflation |
| Legal and Regulatory | Relating to the laws and regulations which, if complied with, should reduce hazards |
| Environmental | Relating to issues such as fuel consumption, pollution, etc. |
| Political | Relating to possible political constraints (i.e. change of government) |
| Market | Relating to issues in the market (i.e. competition and supply of goods) |
| “Act of God” | Relating to instances of uncontrollable natural forces (i.e. fire, flood, earthquake) |
| Financial | Budgetary | Relating to availability of resources or the allocation of resources |
| Fraud or Theft | Relating to the unproductive loss of resources |
| Insurable | Relating to potential areas of loss which can be insured against |
| Capital Investment | Relating to the making of appropriate investment decisions |
| Liability | Relating to the right to sue or to be sued in certain circumstances |
| Activity | Policy | Relating to the appropriateness and quality of policy decisions |
| Operational | Relating to the procedures employed to achieve particular objectives |
| Information | Relating to the adequacy of information which is used for decision making |
| Reputational | Relating to the public reputation of the Company and consequent effects |
| Transferable | Relating to risks which may be transferred or to transfer of risks at inappropriate costs |
| Technological | Relating to the use of technology to achieve objectives |
| Project | Relating to project planning and management procedures |
| Innovation | Relating to the exploitation of opportunities to make gains |
| Human Resource | Personnel | Relating to the availability and retention of suitable personnel |
| Health and Safety | Relating to the well-being of people |

ANNEX C

Tools and Techniques in Risk Identification

The following are some of the Tools and Techniques which may be used to determine risks:

**Documentation Reviews**

These are carried out for getting ideas on risks that may be existing or foreseen in the project. Documentation reviews involve reviewing the project documentation, including plans, assumptions, project files, and other information in order to identify areas of inconsistency or lack of clarity. The documentation is comprehensively reviewed for completeness, accuracy and consistency. Missing, inaccurate or incomplete information and inconsistencies can be indicators of risks in the project.

The documents that could be reviewed include, but not limited to:

* Project charter
* Project scope statement
* Work breakdown structure
* Project schedule
* Cost estimates
* Procurement plan / budget
* Assumptions log

**Information Gathering Techniques**

This includes various techniques like brainstorming, Delphi technique, interviews and root cause analysis. The ultimate aim of all these techniques is to identify and prepare a comprehensive list of risks in the project or Company.

*Brainstorming*

It is one of the most widely used techniques to identify risks in a project. Project team usually performs brainstorming, often with subject matter experts, risk management experts and other important stakeholders who can contribute to the risk identification. It allows people to come up with risks. During brainstorming sessions there should be no criticism of ideas. The main focus is to open up possibilities of risk. Judgments and analysis at this stage inhibit idea generation. Ideas should only be evaluated at the end of the brainstorming session. Brainstorming sessions always have a facilitator to lead the team and help turn their ideas into a list of risks.

*Delphi technique*

This technique is used to build consensus of experts who participate anonymously. A facilitator uses a questionnaire to solicit ideas about important project risks. The questionnaire is often designed with forced choices that require the experts to select between various options. The responses are summarized and re-circulated to the experts for further review until consensus on the final list of risks is reached. Delphi technique helps reduce bias in the data and keeps any one person from having undue influence on the outcome.

*Interviewing*

Interviewing is generally a face-to-face meeting that includes question and answer sessions. The interviews are conducted with project manager, project team, stakeholders, subject-matter experts, and individuals who may have participated in similar, past projects. Interviews help to get first-hand information about others' experience and knowledge.

*Root cause analysis*

Root cause identification is a technique for identifying essential causes of risk. Reorganizing the identified risks by their root causes will help to identify more risks. This technique enables the Company to understand the risk more clearly so that responses can be planned to prevent recurrences.

**Checklist Analysis**

Checklist analysis can provide ideas for risks on a current project. Checklists can be developed based on historical information, knowledge from previous similar projects and from other sources of information.

Checklist analysis is quick and simple; can be used by team members who have relatively less experience in similar projects. But, the project manager has to understand that it is impossible to build an exhaustive checklist. So, care should be taken to also explore risks that do not appear on the checklist, because even highly similar projects will have their own, unique and different risks.

Checklists should be reviewed during project closure to incorporate any new lessons learned and also to improve the checklists for future projects.

**Assumptions Analysis**

This analysis explores the validity of all the assumptions that are identified and documented during the planning processes.

Assumptions analysis identifies risks to the project from inaccuracy, instability, inconsistency or incompleteness of assumptions. It is preferable to have the assumptions accurate, complete and consistent; but, in practice, it is not always possible. So, it is important for the project management team to review the justification or strength or support of the assumptions made. The risks are directly proportional to the consequences or the impacts to the project objectives if the assumption turns out to be wrong.

**SWOT Analysis**

It is a strategic planning tool used to evaluate the strengths, weaknesses, opportunities, and threats to a project.

This helps the Company in understanding the weaknesses of the business or projects so that proper management may be implemented to eliminate threats which otherwise would not have been foreseen or identified.

SWOT Analysis is a framework to identify strengths and weaknesses in a project. This is typically done in interactive groups, like brainstorming sessions, where people can discuss, assess, and elaborate on the identified SWOT elements and analyzing them in depth. It is also a method for maximizing the positive risks (opportunities) and minimizing the negative risks (threats). The analysis and deliberation are designed in such a way to identify avenues to take advantage of strengths and exploit opportunities, as well as minimize the impacts of weaknesses and protect the project against threats.

ANNEX D

Risk Assessment Model

**Risk Assessment Model**

The Risk Assessment Model is a method of risk assessment that will enable the Company to understand the threats to and vulnerabilities of its critical activities and supporting resources.

Under this method, a Risk Magnitude Score (RMS) is established which is obtained by multiplying the scores – Severity (S), Likelihood (L) and Mitigation (M). That is: **RMS = S x L x M**

The RMS value can range from 1 to 125 and helps rank the identified risk events and the causes in order of priority. Higher scores will generally require priority in terms of action to be taken.

1. *Severity of Effects Score*

This is a score on a scale of 1-5 which reflects the assessment of the seriousness of the damages listed.

| Severity of Effects | Probability Score Criteria | Score |
| --- | --- | --- |
| Hazardous or Catastrophic | 1. May cause loss of lives, buildings or sites 2. The duration of recovery is very long | 5 |
| Very High | 1. May cause severe injuries 2. May lead to severe damage to buildings, equipment and goods 3. May cause severe hardships to customers, employees and suppliers and may lead to severe financial losses for all of them and the Company 4. The duration of recovery is long | 4 |
| High | 1. May cause major injuries 2. May lead to major damage to buildings, equipment and goods 3. May cause hardships to customers, employees and suppliers and may lead to financial losses for all of them and the Company 4. The duration of recovery is quite long | 3 |
| Moderate | 1. May cause minor injuries 2. May lead to moderate damage to buildings, equipment and goods 3. May cause moderate hardships to customers, employees and suppliers and may lead to some financial losses for all of them and the Company 4. The duration of recovery is moderate | 2 |
| Minor | 1. No injuries 2. None or minor damage to buildings, equipment and goods 3. Insignificant hardships caused to customers, employees and suppliers and may lead to minor financial losses for all of them and the Company 4. The duration of recovery is short | 1 |

1. *Likelihood of Occurrence Score*

This score measures on a scale of 1-5 the likelihood of occurrence of the identified risk event arising from the potential cause based on the guideline provided in the table below. The higher the likelihood, the higher the score.

| Likelihood of Occurrence | Probability Score Criteria | Score |
| --- | --- | --- |
| >90% chance of happening | Almost certain | 5 |
| 71% - 90% chance of happening | Likely | 4 |
| 51% - 70% chance of happening | Possible | 3 |
| 30% - 50% chance of happening | Unlikely | 2 |
| < 30% chance of happening | Rare | 1 |

1. *Mitigation Score*

This score measures the scale of 1-5 the assessment of availability measures for the identified risk event based on the evaluation criteria by the table below. The weaker the mitigation measures, the higher the score.

| Likelihood of Occurrence | Probability Score Criteria | Score |
| --- | --- | --- |
| Highly Ineffective | 1. Prevention is impossible or prevention measures are not in place 2. No known detection method is available or eve in available it has not been implemented 3. No response mechanism, in case of the event occurring, has been put in place | 5 |
| Ineffective | 1. Prevention is possible but preventive measures are not in place, or even if in place they are not effective 2. Known detection method(s) is/are available but it/they have not been implemented, or even if implemented they do not work effectively or work only occasionally 3. Response mechanism is in place but is not effective | 4 |
| Moderately Effective | 1. Preventive measures in place and are somewhat effective 2. Detection methods have been implemented and are somewhat effective 3. Response mechanism is in place and is somewhat effective | 3 |
| Effective | 1. Preventive measures in place and are quite effective 2. Detection methods have been implemented and are quite effective 3. Response mechanism is in place and is quite effective | 2 |
| Very Effective | 1. Preventive measures in place and are very effective 2. Detection methods have been implemented and are very effective 3. Response mechanism is in place and is very effective | 1 |

**Criteria for Risk Treatment/Response**

It may be noted that not all risks will require mitigating measures to be adopted. Based on the RMS score, a risk may be:

* Tolerated or accepted – in case of low risk
* Transferred (e.g. to insurance companies) – in case of medium to high risk, especially if it makes financial sense to transfer rather than mitigate from the return of investment point of view
* Treated or mitigated (using controls for prevention, detection and response) – in case of medium to high risk
* Terminated or take urgent corrective actions – in case of very high risks

The table below provides the guide evaluation criteria which may be used to decide if a risk will be tolerated/accepted, transferred or treated. The criteria table below is subject to the judgment of the Company’s management.

|  |  |
| --- | --- |
| RMS Score | Treatment |
| 91 – 125 | Take urgent actions |
| 27 – 90 | Mitigate or Transfer |
| 0 – 27 | Tolerable / Accept |