BLUE DART EXPRESS LIMITED

RISK MANAGEMENT POLICY

1. Foreword

1.1. Context

Risk, as defined by ISO 31000:2009 (Risk Management - Principles and Guidelines), "is the effect of uncertainty on objectives". Risk Management is an integrated approach to proactively manage risks which affect the achievement of Blue Dart Express Ltd. (herein referred to as "Blue Dart" or the "Company") vision, mission and objectives. RISK MANAGEMENT is aimed at protecting and enhancing stakeholder value by establishing a suitable balance between harnessing opportunities and containing risks.

Blue Dart, South Asia's premier express air and integrated transportation & distribution company, offers secure and reliable delivery of consignments to over 56,400+ locations in India. As part of the DHL Group's (DHL Express, DHL Global Forwarding & DHL Supply Chain) E-commerce division, Blue Dart accesses the largest and most comprehensive express and logistics network worldwide, covering over 220 countries and territories and offers an entire spectrum of distribution services including air express, freight forwarding, supply chain solutions and customs clearance.

The product range of the Company comprises the following:

- Domestic Priority
- Dart Apex
- Dart Surface line
- Dart Plus
- Airport to Airport
- Charters
- Interline
- Time Definite Delivery (TDD) Service
- Smart Box
- Express Pallet
- International Services
- Temperature Control Logistics (TCL)
- Go Green Carbon Neutral Service
- Freight On Value (FOV)
- Freight On Delivery (FOD)
- Ground Point to Point
- Critical Express

In today's challenging and competitive environment, strategies for mitigating inherent risks in accomplishing the growth plans of the Company are imperative. The common risks inter-alia are regulations, competition, business risk, financial, operational, sectoral, information, environment, sustainability, governance (ESG), business continuity, cyber security and other risks.

1.2. Definition of Risk

Within Blue Dart, risk is regarded as the threat of some event, action or loss of opportunity such that, if it occurs, will adversely affect:

- Value to our stakeholders
- Our ability to achieve our objective.
- Our ability to implement our business strategies.
- The way we operate; and/ or.
- Our reputation

1.3. Definition of Risk Management

Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities

This involves:

- Identifying potential risks related to Financial, Operational, Sectoral, Information, Environment, Sustainability, Governance (ESG), Business Continuity, Cyber Security and other risks.
- Assessing the potential impact of each Risks
- Identification of measures for Risk Mitigation
- Taking action to minimize the potential impact by various mitigation plans.
- Monitoring and reporting on the status of key risks on a regular basis

Risk Management also provides Blue Dart with the opportunity to identify risk-reward scenarios and to realize significant business opportunities.

1.4. Purpose and Benefit of Risk Management

The purpose of risk management is to identify potential problems before they occur, so that risk-handling activities may be planned and invoked as needed to manage adverse impacts on achieving objectives.

The objective of risk management is not to eliminate risk, but to understand it so that the Company can minimize the downside and take advantage of the upside. This requires clarity on what risks the Company is prepared to take, how much, and ensure that the Company has the processes in place to manage these risks.

An integrated and clearly structured risk management policy can help support the maximization of shareholders' value in several ways, which include:

- Clarity of roles and responsibilities
- Minimize surprises & negative impact of risks on business objectives.
- Quicker, risk-oriented decisions by focusing on key risks.

- Achieve business objectives and strategic goals.
- Better informed and greater management agreement on key decisions taken.
- Enhanced communication to Board/Audit Committee
- Greater management responsibility and accountability.
- Integrated governance practices.
- Reduced earnings volatility and increased profitability.

2. Risk Management Policy

2.1. Purpose

This policy is intended to support and assist Blue Dart in achieving their business objectives by providing minimum standards for identifying, assessing and managing their business risks in an efficient and cost-effective manner at the same time ensuring the effective monitoring and accurate reporting of these risks to the key stakeholders.

The key objectives of this policy are to:

- Provide an overview of the principles of risk management
- Explain approach adopted by the Company for risk management.
- Define the organizational structure for effective risk management.
- Develop a “risk” culture that encourages all employees to identify risks and associated opportunities and to respond to them with effective actions.
- Identify, assess and manage existing and new risks in a planned and coordinated manner with minimum disruption and cost, to protect and preserve Company’s human, physical and financial assets.

2.2. Applicability

This policy applies to every part of Blue Dart’s business and functions including its subsidiaries and associated companies. The policy complements the corporate governance initiatives of Blue Dart and does not replace other existing compliance programs, such as those relating to environmental, quality, and regulatory compliance matters.

2.3 Limitation and Amendment

The Board of Directors of the Company may in its discretion and on recommendation of the Risk Committee Audit Committee, make any changes/modifications and/or amendments to this Policy from time to time.

In the event of any conflict between the provisions of this Policy and of the Companies Act, 2013 (“**Act**”) or SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (“**LODR Regulations**”) or any other statutory enactments, rules, the provisions of the Act or LODR Regulations or statutory enactments, rules shall prevail over and automatically be applicable to this Policy and the relevant provisions of the Policy would be amended/modified in due course to make it consistent with the law.

2.4. Risk Management Guiding Principles

To fulfill this commitment, Blue Dart and its management abides by the following principles:

- Risk management is everyone's responsibility, from the Board of Directors/Audit Committee/Risk Committee to individual employees. Risks should be primarily managed by the business function transacting the business. All employees should actively engage in risk management within their own areas of responsibility.
- Blue Dart will manage its significant risks through a holistic approach that optimizes the balance between risks and return across all verticals and functions. Optimization ensures that the Company only accepts the appropriate level of risk to meet its business objectives.
- Each function is expected to undertake risk assessments on half yearly basis. However, in case a new risk suddenly appears on the horizon in between such risk assessments, such risk/incident to be reported immediately to the RMC. Risk Management will be integrated with major business processes such as strategic planning, business planning, operational management (including subsidiary and associated companies), and investment decisions to ensure consistent consideration of risks in all decision- making.
- Risk Management is a comprehensive, disciplined and continuous process in which risks are identified, analyzed and consciously accepted or mitigated within approved risk appetite.
- Risk Management in Blue Dart will continue to evolve to reflect international best and prudent practices that addresses the changes in our requirement, organizational structure, size and industries within which we operate.
- Risk management policies and processes of each function will be aligned and consistent with this Company-wide Risk Management policy.
- Blue Dart recognizes that the implementation and responsibility of the policy remains with the **RMC**, thus all risk strategies and risk appetite levels developed by the functions must be approved and endorsed by the RMC for approval of the **BOD**.

2.5. Change Management

This policy will be reviewed once in two years (or earlier if situation so warrants) by Blue Dart's Risk Management Committee (RMC) and would be placed before the Audit Committee and Board for their approval as and when any change takes place.

If the processes defined in this policy are changed, the following change management procedure shall be followed:

- All changes to the existing processes shall be authorized and circulated by RMC. Changed sections shall have a new version number (i.e. 1.1, 1.2, 1.3 and so on) and date.
- Risk Management Committee shall maintain a copy of the original manual and all revisions thereto.
- Users other than the Risk Management Committee shall destroy the replaced pages.

Subsequent issues of the entire manual shall have a new version number i.e. Version 2.0, Version 3.0 and so on.

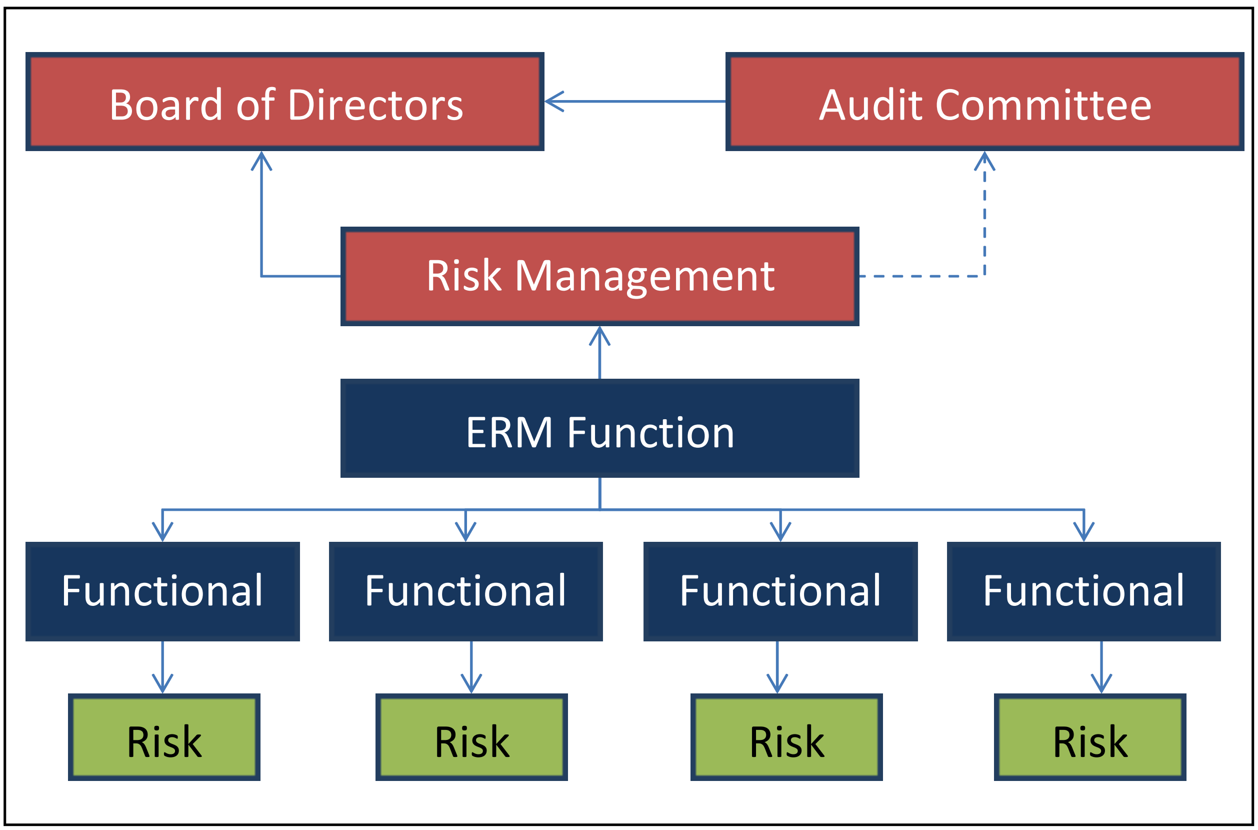
3. Risk Management Governance

3.1. Purpose

Risk Management Governance provides a consistent structure for risk management. Key components include the risk management organization structure, risk management roles and responsibilities and reporting relationships.

3.2. Risk Management Organization Structure

The below chart provides the risk management organization structure within Blue Dart



*ERM stands for Enterprise Risk Management

3.3. Risk Management Roles and Responsibilities

Roles and responsibilities for each member within the Risk Management Organization Structure are detailed below:

- Board of Directors (BOD)

  BOD has the ultimate responsibility for managing the risk profile of the organization. They will approve the organization's risk appetite. The Board will be responsible for ensuring that the risk management framework is contributing to achieving business objectives, safeguarding assets and enhancing shareholder value. The BOD is also responsible for the management of all key identified risks across the organization and ensuring that risks are being managed actively and effectively. However, it may delegate this responsibility to the Risk Management Committee for administrative reasons.

- Audit Committee

  Audit Committee shall overview the entire risk management process, review the risk profile of the organization on a periodic basis, review the organization's risk appetite and provide its inputs to the management and to RMC.

3.4 Risk Management Committee (RMC)

The role and responsibility of the Risk Management Committee may inter-alia include the following:

- To formulate a detailed risk management policy which shall include:

  (a) A framework for identification of internal and external risks specifically faced by the listed entity, including financial, operational, sectoral, sustainability (specifically, Environmental, Social and Governance related risks and impact), Business Continuity, Cyber Security risks and other risks.
  (b) Measures for risk mitigation
  (c) Systems for internal controls
  (d) Business contingency plan

- To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management and internal control systems.
- Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the listed entity.
- To keep the board informed about the nature and content of its discussions, recommendations and actions to be taken.
- Further, the Risk Management Committee shall coordinate its activities with the Audit Committee in instances where there is any overlap with audit activities.
- The Risk Management Committee would maintain a comprehensive oversight over all risks and their management. All policies which have implications on the organization's risks are to be endorsed by RMC for Board's approval. The RMC will provide guidance on the risk management activities, review the results of the risk assessment and mitigation plan development process, review and monitor the working of the risk management Process and report to the BoD on the status of the risk management initiatives and their effectiveness.

- Risk Management Function

  Risk Management function will drive the risk management process with other Functions. The Risk Management Function is being performed by Internal Audit & Risk Management Team headed by Mr. Savio Mendonca – Head Internal Audit & Risk Management. The Internal Audit & Risk Management Team coordinates with all the Risk owners for each of the Risk and obtain quarterly update on the movement of the Risk and with assistance of the Risk owner will do the impact assessment for each risk which has moved upwards. The Function will also be responsible for providing Half yearly update on risks to the Audit Committee and Board on the top organization risks. The function will also perform a Risk Workshop with all stakeholders on a Yearly basis to effectively drive Risk Management and its mitigation within the Group.

- Risk Owner

  Risk Owners drive the risk management process within the functions and ensure risk management procedures are complied with in accordance with the Risk Management policy. They would be the point of coordinating and managing all the risk management activities approved by the RMC and BoD. Risk Owners should ensure risk consideration is part of the decision-making process and ensure close alignment and reporting of the functional risk management activity with the Corporate Risk Management. It is recommended that functional/Regional Heads are nominated as risk Owners, to effectively drive risk management operations within their respective verticals / functions.

3.4. Risk Management Committee

The purpose of the Risk Management Committee (RMC) is to develop and oversee the Company's risk management programs in order to prevent the occurrence of loss or harm, and to ensure appropriate action is taken to minimize the impact of losses or damages when they do occur.

The objectives of the RMC are:

- To develop and oversee implementation of the Risk Management program in order to foresee and respond to actual and expected risks.
- To ensure that an appropriate, optimal and profitable balance is maintained between risk and reward across the business.
- To minimize risk of unforeseen, unacceptable and/or unnecessary loss or harm
- Formal authority, responsibility and accountability for designing, implementing and sustaining effective risk management processes rests with the Board of Directors. Risk Management Committee will implement the Risk Management Program under directions of the Audit committee and Board of Directors.

- For operational purposes, the Risk Management Committee will form part of the agenda of all Management Committee meetings. Risk Management Committee meetings should be held at least twice a year and minutes to be documented and submitted to the Board for review. The quorum shall be either two members or one third of the committee members, whichever is higher, including at least one member of the board of directors in attendance. The meetings of the RMC shall be conducted in such a manner that on a continuous basis, not more than 180 (one hundred and eighty) days shall elapse between any two consecutive meetings.

Risk Management Committee Composition

The permanent members of the RMC include the following (or their equivalents following any future organizational or job title changes):

- Ms. Kavita Nair - Chairperson
- Mr Prakash Apte – Director
- Mr. R.S. Subramanian- Director
- Mr. Balfour Manuel- Managing Director
- Mr. Tushar Gunderia- Head (Legal & Compliance) & Company Secretary
- Mr. Savio Mendonca- Head Internal Audit & Risk Management

The RMC should have minimum of three members with most of them being members of the Board of Directors. If any permanent member position is vacant, the executive acting in that position may be invited as a member of the committee. The composition of RMC shall include at least one independent director.

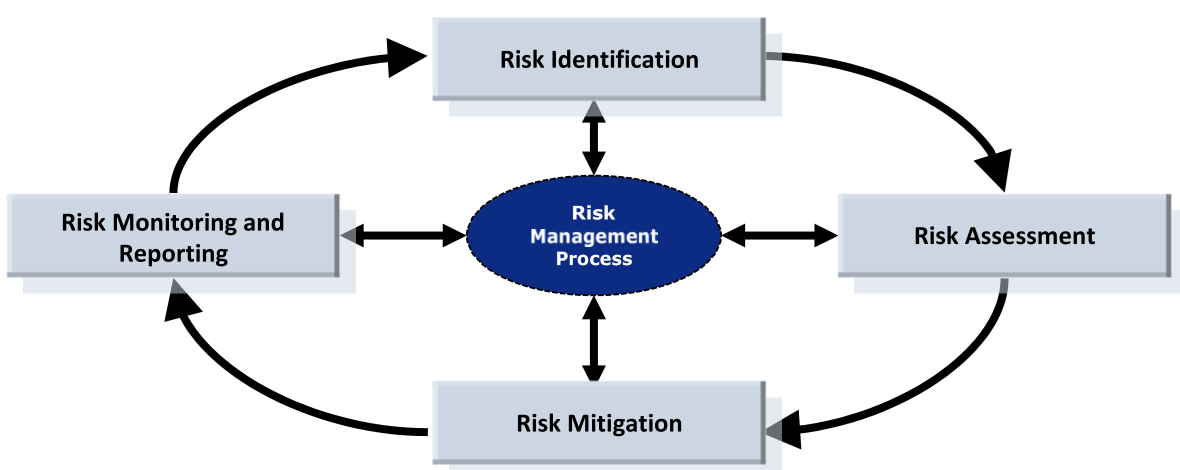
The RMC may invite other members from the managerial level, who possess a range of relevant expertise as well as adequate knowledge of the institution's risk exposure, as selected by the committee members from time to time.

The Board of Directors will approve the composition and membership of the RMC. The Chairman of the Committee may invite external advisors to participate in the RMC meetings as necessary.

4. Risk Management Procedures

4.1. General

The risk management process should be an integral part of management, be embedded in culture and practices and tailored to the business processes of the organization. The risk management process includes four activities: risk identification, risk assessment, risk mitigation and monitoring and reporting as shown in the figure below:



4.2. Risk Identification

The identification of risks is the first step in the risk management process. The purpose of risk identification is to identify the events that have an adverse impact on the achievement of the business objectives. Further, risk identification not only refers to the systematic identification of risks but also to the identification of their root causes.

All risks identified are documented in the form of a Risk Cards. The Risk Card incorporates the risk description, root cause, existing control/ mitigation measures and mitigation plan.

Techniques of Risk Identification:

The following risk identification techniques can be deployed to enable focused risk identification:

- Surveys / Questionnaires
- Structured interviews and brainstorming
- Root cause analysis
- Internal / external audit reports
- Risk management workshops

The process of risk management should be integrated within the strategy setting process. Risks should be identified at the time of strategy setting exercise. Risk identification should primarily be a top-down process with significant time commitment provided by the MD, CFO, Functional heads to the process. The process should also involve participation from select middle and junior management to provide a 360-degree view on risks.

Risk Categories

For better risk identification, it is important to know various risk categories. Some sample categories are provided below:

Risk Category	Definitions
Strategic	Potential risks affecting high-level goals, aligned with and supporting the entity's mission/ vision.
Operational	Potential risks affecting the effectiveness and efficiency of the entity's operations. They vary based on management's choices about structure and performance.
Financial	Potential risks affecting the performance and profitability goals of the Company including safeguarding resources against financial losses.
Compliance	Risk relating to adherence to relevant laws and regulations. They are dependent on external factors and tend to be similar across all entities in some cases and across an industry in others.
Cyber Security Information Technology	Potential risks affecting the integrity of networks, programs, technologies and data
Environment / Sustainability	Potential risk related to climate change impacts mitigation and adaptation, environmental management practice, working and safety condition, respect for human rights, anti-bribery and corruption practices, and compliance to relevant laws and regulation

4.3. Risk Assessment

Assessment involves quantification of the impact of risks to determine potential severity and probability of occurrence.

Risks may be assessed in workshops or using anonymous surveys, facilitated by the Internal Audit & Risk Management function. Each identified risk is assessed on two factors which determine the risk exposure:

A. Impact if the event occurs.

B. Likelihood of event occurrence

It is necessary that risks are assessed after considering the existing controls, so as to ascertain the current level of risk. Based on the above assessments, each of the Risks can be plotted on a Risk Assessment table and can be categorized as – Low, Medium and High.

Risk Appetite

Risk appetite refers to the amount of risk exposure or potential adverse impact from an event that the organization is willing to accept / retains in order to achieve its strategic objectives. It supports conscious decision-making based on risk-reward trade off and ensures management works within established limits to control exposure.
Blue Dart may express its risk appetite qualitatively, whereby any risks which have an >= 4 on a 5 pointer Scale are deemed beyond acceptable limits. These risks would require compulsory management attention for further mitigation. Blue Dart's Risk Management Committee should decide Blue Dart's risk appetite and propose to the Board for approval.

4.4. Risk Treatment

Risk treatment involves selecting one or more options for managing risks and implementing such action plans. This phase of the Risk Management process is intended to:

- Understand existing practice/ mitigation mechanisms in place for managing risks.
- Generate new action plans for treatment of risks.
- Assess the effectiveness of such treatment plans.

For the purpose of risk treatment, risk owners may consider various options (as indicated below) for risk treatment:

- Avoiding the risk by deciding not to start or continue with the activity giving rise to such risk.
- Taking or increasing the risk in order to pursue an opportunity.
- Removing the risk source
- Changing the likelihood or consequences of risk by instituting new monitoring activities
- Sharing the risk with another party or parties (e.g.: joint ventures, partnerships, insurance, back-to-back warranties etc.)
- Retaining the risk by informed decision

Risk treatment can be a choice from the above or a combination of multiple options.
For example, a combination of partially sharing the risk (through joint ventures) and partially accepting the risk can be the chosen treatment for a risk.

The choice of an appropriate treatment option must consider balancing the costs and efforts of its implementation against the benefits derived.
Below are some generic steps for risk treatment: -

- Evaluate the strategic mitigations in place for key risks.
- Evaluate monitoring requirements.
- Verify and evaluate the monitoring practices currently in place for key risks.
- Identify and evaluate the post event measures in place for risk.
- Review the financial risk protection measures in place to respond to the consequences of risk events, if quantifiable
- Take decisions on the acceptability of identified risks and controls.
- Document action plans for risk mitigation

4.5. Monitoring and reviewing risks

Risk monitoring, reviewing and reporting are critical components of the Risk Management process. Once risks are identified, it is necessary to prioritize them based on the impact, dependability on other functions, effectiveness of existing controls etc. The intent of monitoring and reviewing risks is to:

- Analyze and track events, changes in the business processes, operating and regulatory environment & future trends which affect identified risks. As part of this, the impact of such events on treatment plans is also assessed.

- Review risks which have materialized
- Review new emerging risks.
- Detect changes and assess the impact of changes to risk appetite, risk portfolio and risk treatment plans.
- Ensure that risk treatment mechanisms are effective in design and operation.
- Inter-dependence and cumulative impact of risks is discussed with all concerned to decide what is expected from whom.
- Provide cushion for non-measurable and unknown risks.

Risks do not normally exist in isolation. They usually have a potential effect on other functions, business processes and risk categories. These cause-and-effect relationships must be identified and understood. Many cross-functional effects of risk may not be immediately apparent without deliberate and systematic analysis, so a formal approach is required.

Respective functional heads shall review all risks affecting their functions on a half yearly basis. If any new risks have been identified, such risks will get discussed in the group meetings and once approved by the Functional head, will be added to the Risk Cards. The functional heads shall then implement an effective system of internal control to manage those risks, including designating responsibilities, and providing for upward communication of any significant issues that arise. Reports shall be provided on a half yearly basis to the RMC along with the status of action plans.

The RMC shall meet at least twice a year to review all risks escalated through the review meetings. The review shall include identifying / framing mitigating controls for the newly identified risks and discuss the status of mitigation in respect of already identified risks. In case the newly identified risks have been approved by RMC then the same will be added to the risk card. Further, the key risks along with the mitigating controls will be forwarded to the Audit Committee and Board of Directors on a half yearly basis.

Internal Audit function will audit all functions/ risk management processes during its coverage of respective functions as per the scope approved by the Audit Committee. The independent audit will provide management with assurance over the effectiveness of the risk management activity and its compliance with Blue Dart's Risk Management policy. Any audit observations will be communicated to the Functional Head and to Head – RMC. Functional heads should take specific actions to close the audit observations and communicate the same to Internal Audit.

4.6. Managing Materialized Risks

In case a risk materializes, it is necessary to have in place a Crisis/ Incident Management Plan for timely and effective management of such events. The Incident Management Plan is a set of well-coordinated actions aimed at preparing and responding to unpredictable events with adverse consequences. The intention of this plan is to preserve the confidence of internal and external stakeholders in the Company's risk readiness for potentially adverse events. The relevant risk owner would be responsible to chalk out a detailed response plan in consultation with RMC to handle the risk which has materialized.

4.7. Managing Emerging Risks

The Company is subject to various risks and challenges emerging from the internal environment (e.g. operations, strategy, systems and processes etc.) and external environment (e.g. competition, changes in government policies, forex fluctuation and global economic environment etc.); which may have a significant impact on the organization. Hence, it is important to assess and take action steps in advance to mitigate such risks. Hence, emerging risks form an important part of Risk Management process.

All emerging risks should form an integral part of the risk management discussion. If any additions have to be made in the Risk Cards, it will be approved by the Functional Heads and will be forwarded to the RMC for reference. In case of High Risks, Risk Cards should be prepared and presented.

4.8. Risk Integration with Other Processes

RMC should ensure effective risk integration with key processes across their business. This section provides guidance on risk management integration with some key business processes. RMC should use these guidelines and establish formal working relationships with these processes.

Integration with New Opportunity Identification

Blue Dart would pursue several new business opportunities at any given point as part of its business development and expansion activities. In order to enable robust growth, Management shall take risk- informed decisions while choosing to pursue an opportunity or submit a bid. It is therefore essential to follow a rigorous process for evaluating options that maximize value and optimize risks at the inception stage of a project. The purpose of risk assessment of new business is to enable early cognizance of risk factors associated with the business being pursued.

Integration with Internal Audit

Each function should communicate and develop working relationships with the Internal Audit function to ensure clarity of roles and responsibilities and improve the risk-control environment.

Integration with Health Safety & Environment (HSE) and Business Continuity Planning (BCP)

Each function should ensure that major risks from HSE / BCP assessments are captured and appropriately reported within the Risk Management reporting process. Specific focus should be on the following areas:

- Use of consistent risk assessment methodology & rating scales
- Periodical exchange and validation of risk information
- Inclusion of major HSE & BCP risks in Risk Card

Integration with Insurance

Each function should co-ordinate with Finance Team and ensure that adequate insurance arrangements are made after a study of the risk profile of their business. Each function should ensure that they identify the risks driving their insurance requirements and manage those risks effectively to reduce their insurance costs / premiums.

Integration with Other Functions (Human Resources, Legal and Corporate Communications)

Each function should ensure that risks from the above functions are properly monitored and managed. Risks should be identified, assessed and their exposures evaluated using the Risk Management policy. Major risks should be identified, 0and mitigation strategies developed for those risks.

Integration with various committee viz; Capex Committee, Revenue Committee, CARO Committee

4.9. Risk Reporting

Risk reporting refers to the preparation and submission of periodic Risk Reports to facilitate pro-active monitoring of major risks by Senior Management.

Risk reporting shall be carried out in compliance with the risk management organization structure depicted in Section 3.2.

5. Reference

This section seeks to provide specific reference documents to the Risk Management personnel, including guidelines on Risk Management documentation, document retention and glossary of useful terms.

5.1. Documentation

The following documents are generated during the Risk Management exercise.

i. Risk Card – Presentation for Identified Risks along with movement of risks.
ii. Loss Event Database– Presentation for Materialized Risks
iii. Presentation for Emerging Risks
iv. Presentation on key risks & status on how they are managed.

5.2. Document Management

Any changes to this policy document need to be processed through RMC and require the consensus of the Board for ratification.

RMC shall ensure that updates to the policy are communicated across the organization and shall also be responsible for promoting risk awareness across the Company. Risk Management Committee may use tools, workshops, newsletters, formal training sessions, and undertake other initiatives as may be required for this purpose.

5.3. Record Retention

For the purpose of ensuring traceability of Risk Management activities, documentation shall be maintained in electronic form.

Electronic Records at an Enterprise level shall be maintained at the Corporate Office on behalf of the Board. However, those at the functional level shall be maintained by individual functions and the respective Functional Head shall be responsible for the same.