RISK MANAGEMENT POLICY - 2019

भारत डायनामिक्स लिमिटेड

BHARAT DYNAMICS LIMITED

CONTENTS

Risk Management Policy as approved in 253rd Board Meeting held on 18.03.2019.

1. Risk Management Policy Statement

WE WILL STRIVE CONTINUOUSLY TO IDENTIFY, EVALUATE, MITIGATE AND MONITOR THE RISKS RELATED TO THE BUSINESS OF THE COMPANY. WE SHALL CONTINUALLY STRIVE TOWARDS STRENGTHENING THE RISK MANAGEMENT SYSTEM THROUGH CONTINUOUS LEARNING AND IMPROVEMENTS.

2. Scope

Risk Management Policy is applicable for all levels and units of the organisation.

3. Objectives of Risk Management

3.1 To ensure that all the current and future risk exposures of the company are identified, assessed, quantified, appropriately mitigated and managed.

3.2 To establish a framework for the Company's Risk Management process and to ensure companywide implementation.

3.3 To ensure systematic, transparent and uniform assessment of risks related with Projects and Operations.

3.4 To ensure that the risks faced are understood and managed.

3.5 To promote unified approach to risk management, including a common risk Language.

3.6 To instil an awareness of risk in employees and ensure that risk is considered in decision making.

3.7 To create an environment where all employees assume responsibility for managing the risk.

3.8 To ensure that risks are appropriately monitored through documentation and review and key treatment actions are reported on regular basis.

3.9 To exploit opportunities.

4. Risk Management Process

4.1 Risk Management as a process shall enable the organization to identify, assess and treat risks. Treatment of risks in the organisation depends on its risk attitude, risk appetite & risk aversion. Risk Management is the responsibility of everyone in the organization, and applies to all functions, product verticals and operations within the organization. Risk management is iterative. The primary objective(s) of establishing a Risk Management Process is to ensure that risks, faced by and opportunities for the organization shall be identified and recorded in the risk register enabling the top management to take a comprehensive view of the same. Risks identified shall be assessed, mitigated, monitored and reviewed on an ongoing basis

4.2 Organisation structure, flow charts, necessary explanations, guidelines and formats for identification & review are provided as annexure detailed below.

a) Risk management Organisational structure is given in **Annexure 1**.
b) Risk management process flow chart at corporate level is at **Annexure 2**
c) Risk management process flow chart at unit level is at **Annexure 3.**
d) Major areas of Risks for classification given in **Annexure 4.**
e) Risk Management Strategy & Process In General is in **Annexure 5.**
f) Basic definitions & abbreviations are given in **Annexure 6.**
g) Risk Identification pro forma is given in **Format 1.**
h) Risks register (Dynamic) pro forma given in **Format 2.**

5. Risk Identification

Risk assessment allows BDL to consider the extent to which potential events have an impact on achievement of objectives. Management should assess events from two perspectives − likelihood and impact.

Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an in-depth knowledge of the organisation, the market in which it operates, the economic, legal, regulatory, social, political, technological, operational and cultural environment in which it exists, as well as a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification shall be approached in a methodical way to ensure that all significant activities within the organization have been identified and all the risks flowing from these activities defined.

Risks are identified at various levels from line mangers to top management of the company. Other methods of identifying risks are

a) Brain storming
b) SWOT Analysis
c) Expert's inputs
d) Scenario thinking

6. Risk Categorisation

All the risks that have been identified shall be categorised under the following risk categories - Strategic, Operational, Reporting and Compliance risk.

Strategic Risk - Risk of loss or opportunities resulting from business factors. These risks affect the achievement of strategic objectives and may affect overall enterprise value.

Operational Risk - Risk of loss or opportunities resulting from inadequate or failed processes or new processes, people and information systems.

Reporting Risk - Risk of inadequate internal or external reporting due to wrong financial as well as non-financial information in the reports.

Compliance Risk - Risk of loss resulting from legal and regulatory factors.

6.1 Risk Classification

For better understanding of categorisation of risks, they are further classified as below:

a) Quality risk – The risk arising out for not fulfilling intrinsic & extrinsic customer requirements in terms of product quality, deliver, service and other contractual obligations.

b) Asset Risk- Risk of loss resulting from depreciation, under-utilisation or loss of control over physical assets of company

c) Competition Risk – Risks pertaining to the external competitors of the company such as entry of new competitors, FDI etc.

d) Compliance Risk - Risk of loss resulting from legal and regulatory factors, such as strict privacy legislation, compliance laws, and intellectual property enforcement

e) Contract Risk – Risks pertaining to the contracts signed with client and sub-contractors

f) Contractor/Vendor Risk – Risks originating from company's relationship and dependence on third party vendors, contractors or outsourcing partners

g) Corruption Risks: Risks of possible corruption due to improper process, review and monitoring.

h) Environmental Risk – Risks having implications on the environment, weather, pollution or risks arising due to changes in environment

i) Expense Risk – The risk of a change in value caused by the fact that the timing and/or the amount of expenses incurred differs from those expected, e.g. assumed for pricing basis.

j) Financial Risk - All risks which have a financial implication such as adverse movements in foreign exchange rates, capital expenditure etc.

k) Foreign environment risk - The risk arising due to exposure to foreign laws, regulation and socio-political environment

l) Litigation Risk - Risk of loss arising out of litigations against or litigation initiated by the company

m) Market Risk – Risks pertaining to external market factors such as demand uncertainty, price volatility etc

n) People Risk - Risks (like attrition) that are part of the personnel related processes of the company such as recruitment, skill sets and performance measurement

o) Process Risk/ Execution Risk – The risk arising due to lack of adequate process or inadequate execution of defined processes

p) Project Risk – Risks which impacts the execution of any project resulting in time and cost overrun

q) Regulatory/Political Risk - The risk arising due to change in regulatory policy of the country

r) Reporting Risk - Risk of inadequate internal or external reporting due to wrong financial as well as non-financial information in the reports

s) Reputation Risk – Risks having implications on the brand and reputation of the company.

t) Technology Risk – Risks originating from usage and deployment of technology in the organisation in its operations and management such as product obsolescence because of technology gap.

7. Methodology for Risk Management

7.1 The Company shall cover risks in various areas of its operation and new potential areas of risks could emerge over a period of time. The risks will have to be identified, evaluated, prioritized and managed. Mitigation measures will need to be finalized and incorporated in the business processes and practices followed by the Company.

7.2 Further, the mitigation measures already incorporated in various business processes may no longer be effective enough and more effective measures will have to be identified and implemented. The methodology for Risk Management process in the company recognizes this dynamic / iterative nature of Risk Management process and incorporates a procedure of continuous review for identification and management of existing and new risks and evaluating the effectiveness of risk mitigation measures.

8. Organisation structure & scope For Risk Management

The following is the implementation structure for Risk management across the Organisation. (Annexure – 1)

a) Board of Directors.

b) Risk Management committee (RMC).

c) Corporate Risk Management committee (CRMC) at Corporate level.

d) Unit Risk Management Committee (URMC) at Unit Level.

e) Divisional Risk management Committee (DRMC) at Divisional level based on requirement decided by unit head.

8.1 Board of Directors:

8.1.1 RMC would report to the Board about RM activities at least once in a year for its consideration and directives.

8.2 Risk Management Committee (RMC) :

8.2.1 This would be senior level committee with all Functional Directors and one independent Director, Chairman CRMC, Corporate Risk Manger (CRM) and Company Secretary. Chairman of RMC would be senior most Director. Company Secretary would act as member secretary of the committee.

8.2.2 Committee would review, twice in a year, the risks and opportunities, residual risks and mitigation measures identified by CRMC. They would recommend suitable mitigation measures or approve the measures proposed by CRMC. They would evaluate residual risk & the effectiveness of implementation of mitigation measures.

8.2.3 RMC would report to the Board the actions being taken for Risk Mitigation.

8.2.4 They would review the Risk Management Policy frame work and implementation across the company.

8.3 Corporate Risk Management Committee (CRMC)

8.3.1 CRMC would be corporate level committee with Unit Heads (URMs) &General Managers looking after- CC, CQC, Marketing, C.Plg, P&A, Finance and Heads of IA, R&D and Safety. The Committee may co-opt members either from the divisions or external expert for specific initiatives to have domain expertise during the deliberations. Chairman would be senior most member of the committee. Management shall nominate an executive not less than the rank of GM as Corporate Risk Manger (CRM). An executive of level DGM / AGM would be the convenor of the committee & he will also assist CRM in implementation of RM. Convenor shall be appointed by CRM.

8.3.2 CRMC will review the status half-yearly in the month of February & August, the risks, residual risks and mitigation measures identified by Unit Risk Management Committees (URMCs). They would recommend suitable mitigation measures or approve the measures proposed by URMC. They would evaluate the effectiveness of implementation of mitigation measures.

8.3.3 Potential areas of risks are identified by executives or by the committee. These risks cover various aspects of operation and other areas detailed at Annexure- 4. But not limited to them alone.

8.3.4 CRMC would review the Risk Management Policy frame work and implementation across the company. Identify and update areas of risks covering the Company as a whole.

8.3.5 Oversee the training needs and overall implementation of Risk Management policy across the organization. For all risks and opportunities CRMC / CRM shall identify a risk owner who shall report CRM periodically.

8.3.6 Scope of work of corporate risk manager

a) He is the nodal officer for organisation risk management activities

b) He is instrumental in integrating the activities of all the RM committees' i.e., RMC, CRMC and URMC

8.4 Unit Risk Management Committee (URMC)

8.4.1 Each Unit shall have a Unit Risk Management Committee (URMC) with Divisional Heads, Functional heads in the units as members. Chairman of the committee shall be Unit head and he would be Unit Risk Manger (URM). An executive of level DGM / AGM would be the convenor of the committee & he will also assist URM in implementation of RM. Convenor shall be appointed by CRM / URM. Unit level committee meeting will be held quarterly in the months of April, July, October & January.

8.4.2 URMC shall be formed for major units- KBC & Bhanur. However, whenever it is required URMC shall be formed at other units with approval of functional director.

8.4.3 URMC will review the status half-yearly in the month of January & July, The risks, residual risks and mitigation measures identified by Unit Risk Management Committees (URMCs). They would recommend suitable mitigation measures or approve the measures proposed by URMC. They would evaluate the effectiveness of implementation of mitigation measures.

8.4.4 URMC shall identify and update units-specific and divisional specific risks and opportunities. URMC shall assess current status of Risk (residual risks) and recommend mitigation measures in the Unit & divisions.

8.4.5 URM may form Divisional Risk Management committees (DRMC) based on needs to achieve objectives of QMS in specific divisions. DRMCs will meet periodically and submit report to URM. These risks & their status will be included in the agenda of URMC.

8.4.6 For all risks and opportunities URMC shall identify risk owners / risk coordinators.

8.5 Divisional Risk management Committee (DRMC)

Depending upon the requirement of a division, URM will define the scope, constitution and frequency of frequency of meetings and constitute DRMC in the division. Chairman of the DRMC will be the divisional head. DRMC will submit reports to URMC as and when the review. DRMC reports shall form input for MR meetings of the division.

9. Reporting of Risk Management

9.1 The reporting of Risk Management in the Company shall be as follows:

9.1.1 Perceived / Identified Risks to be registered through online Risk Register by any executive. The risks are approved by unit head / CRM to be taken up by the respective committees (URMC/ CRMC/DRMC). Divisional Head/ URM / CRM shall monitor the identified risks through online Risk Register along with previously identified risks with their residual risks. Risk is quantified for probability of occurrence between 1 to 5, with 1 being low and 5 being high. Consequence is rated between 1 to 5, with 1 being low and 5 being high. Risk score would be the product of probability or likelihood and consequence. Risk score less than or equal to 6 is Low and is not considered for Risk mitigation. Risk score above 6 and less than or equal to 15 is medium. Risk score above 15 is high.

9.1.2 Opportunities are to be captured and potential advantages will be recorded for exploiting the opportunities

9.1.3 Risks or Opportunities if require immediate attention the risk mitigation process is initiated on approval of divisional head / unit head based on severity and the same will be conveyed to convenor URMC / CRMC.

9.1.4 CRM shall assist CMD / Board regarding implementation of RM and communication to external agencies / Goo

10. Risk Treatment

10.1 All the consequences rated high or medium will be considered by DRMC / URMC / CRMC for Risk mitigation.

10.2 There could be certain cases where risk is not low but committee decides to accept the risk based on the prevailing conditions or risk appetite.

10.3 Where risk estimate is low but there could be strategic or potential impact due to the risk in such cases committee may take up the risk for mitigation or kept under observation for subsequent reviews.

10.4 Organisational approach towards the risks / risk attitude is considered by committees while taking risk mitigation measures.

10.5 Risks are grouped at Divisional / Unit / Corporate levels. Accordingly the risks are handled at the respective levels of division / unit / corporate for risk treatment. However they, intimate to next level & CRM for necessary action.

10.6 The risks/opportunities are reviewed as per the Format-2 by the respective committees.

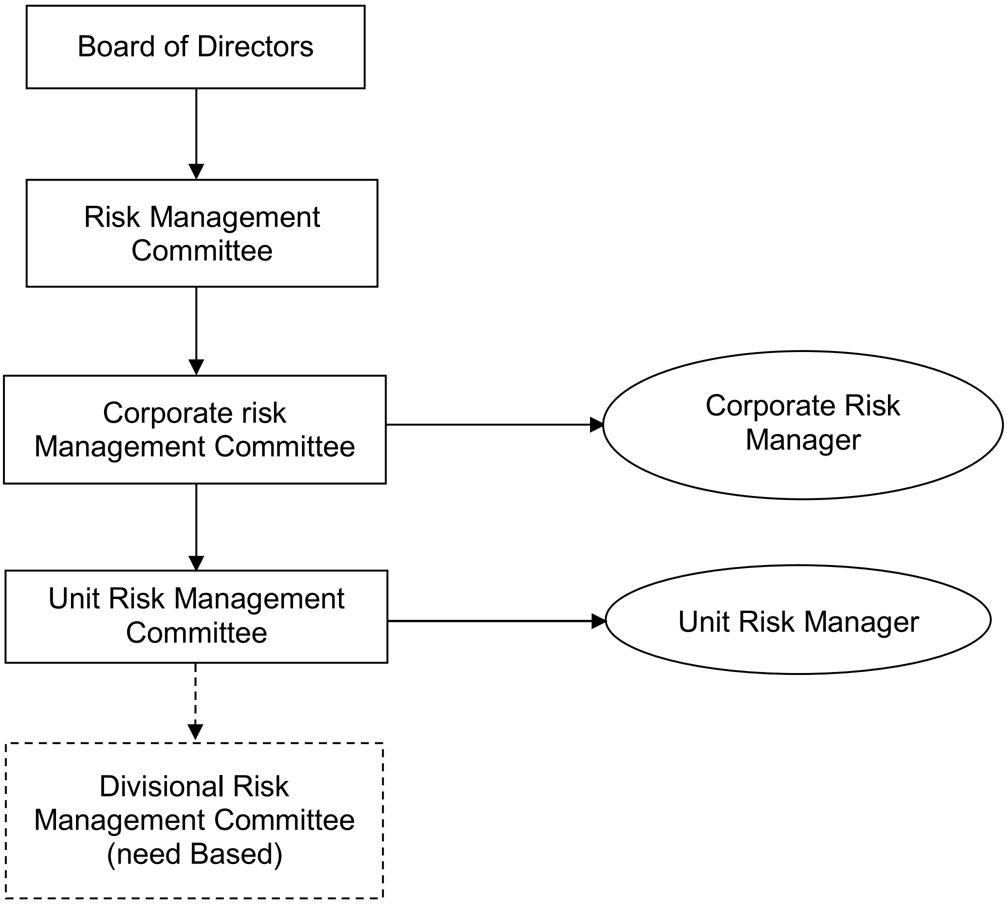
10.7 The risk will be reviewed until it is archived or risk is negligible or opportunity is no longer potential.

10.8 Committee would focus on pending risks and study appropriateness of the mitigation planned.

10.9 The mitigation plan for the Risks by the Risk Owner / Risk Coordinator will be taken into consideration by the respective committees.

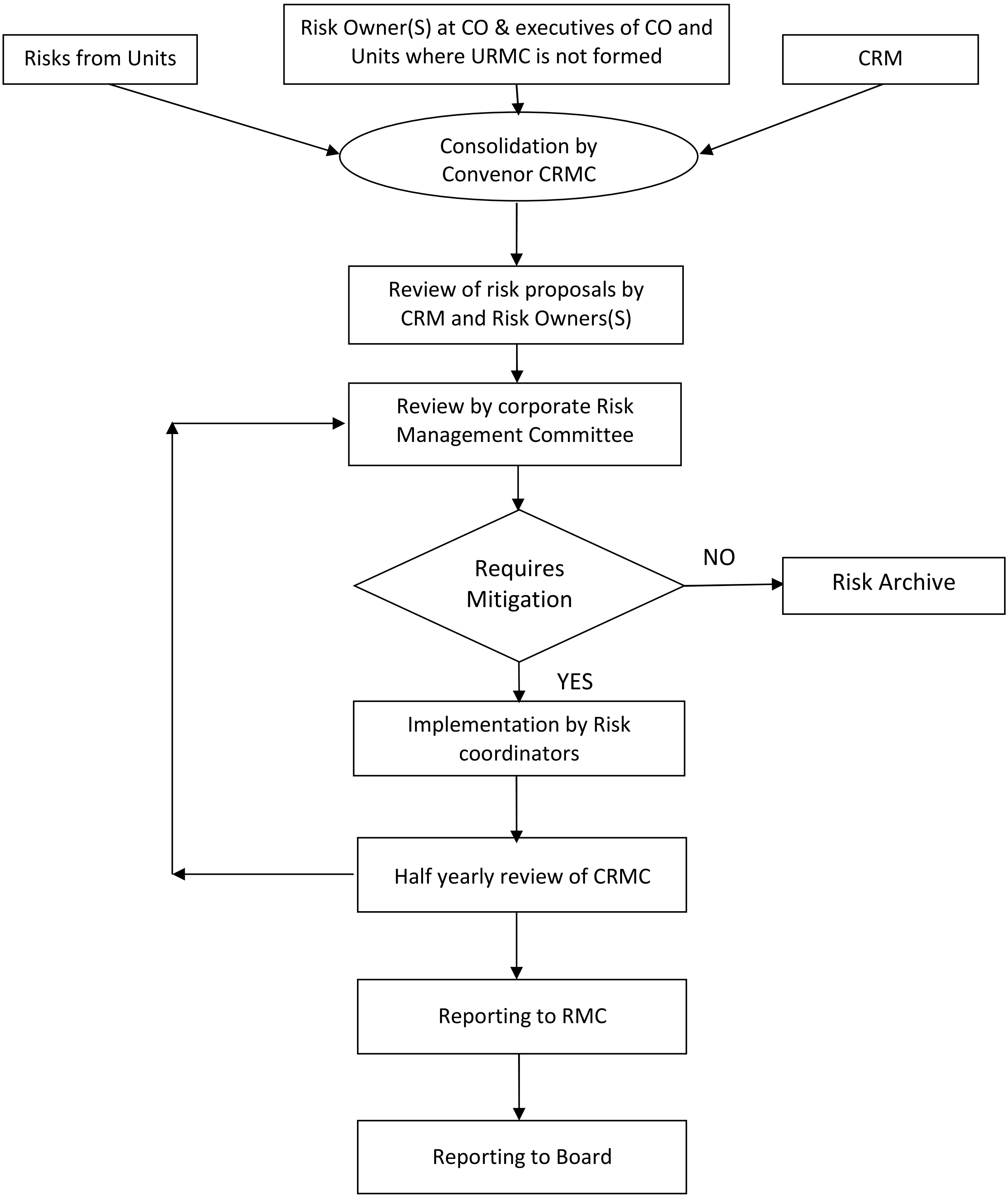
Annexure-1

ORGANISATION STRUCTURE FOR RISK MANAGEMENT



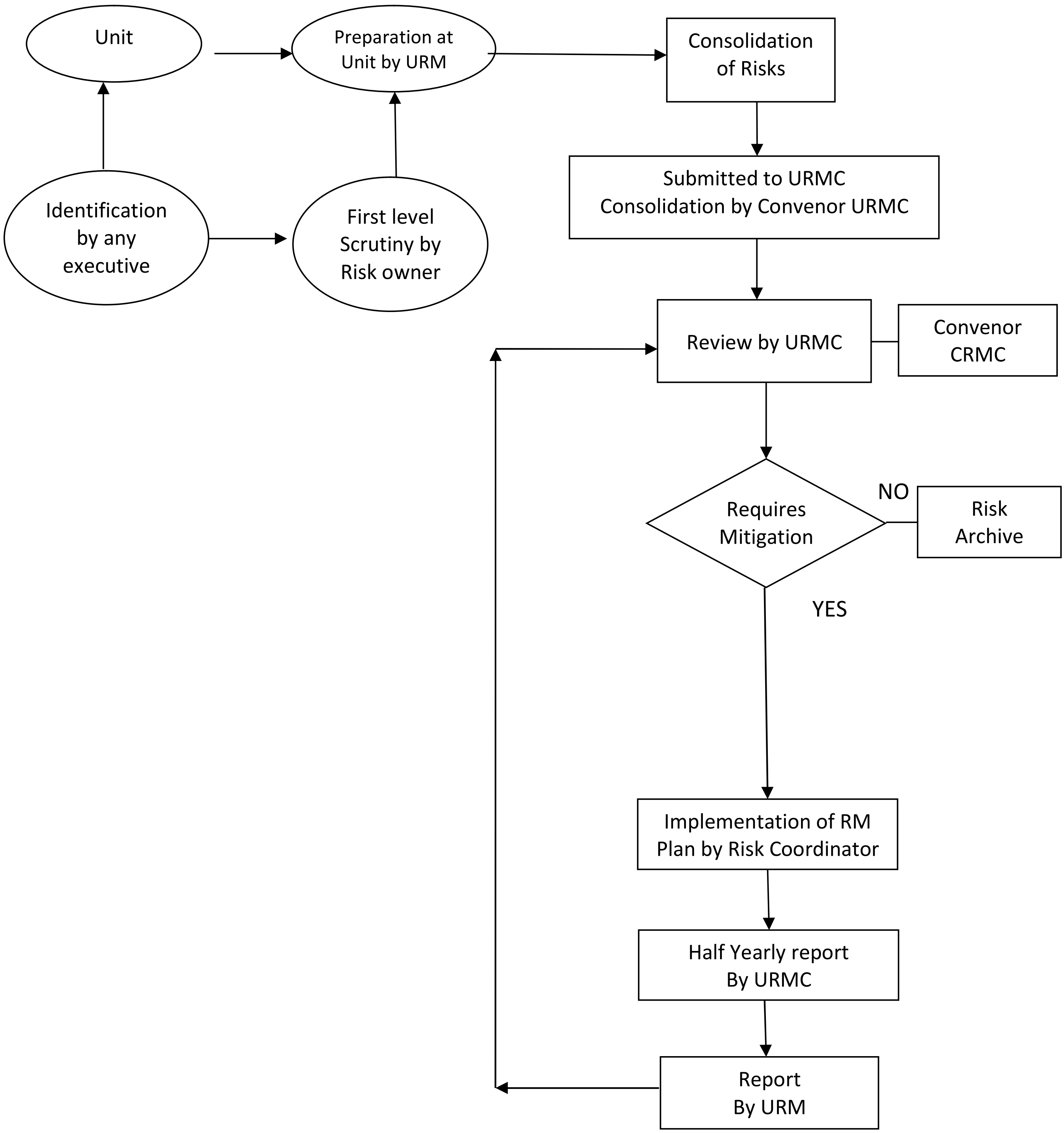
Annexure-2

RISK MANAGEMENT PROCESS FLOW CHART AT CORPORATE LEVEL



Annexure-3

RISK MANAGEMENT PROCESS FLOW CHART AT UNIT LEVEL



Annexure-4

MAJOR AREAS OF RISKS

1. Technology related risks.

1.1 Change in Quality Requirements by Customer / Designer / User.

1.2 Technology up gradation to suite global standards.

1.3 Lag in technology with respect to competitors.

1.4 Technology obsolescence.

1.5 Execution of user proposals.

1.6 Sanctions under Missile Technology Control Regime.

1.7 Long lead time of DRDO projects.

1.8 Lack of common platform with customer and collaborator.

1.9 Dependence on single source developed by designer.

1.10 DRDO ‘main stay’ for technology.

1.11 Limited ‘long-term’ tie ups with institutions for supply of technology.

1.12 Gap in knowledge base (ToT, legacy systems and technological advancement).

2. Market / Product related risks.

2.1 Dependence on Defence market and entry of private sector.

2.2 Shrinking global market for Defence products leading to foreign party’s direct marketing in India.

2.3 Defence procurement procedure of the Government – Enabling increased participation by private and global players.

2.4 Domain of Business Development & Marketing.

2.5 Effective usage of Project Management tools.

2.6 Government Policy on Export Sales.

2.7 Non placement of indents after user trials.

2.8 Reduced defence budget.

2.9 Bench mark Price is not appropriate.

2.10 Project Closure/ Export Order.

2.11 LD risk due to new vendors / technical problem at suppliers.

3. **HR related Risks.**

    3.1 Lack of Strong competency mapping practices and succession planning.

    3.2 Quality of manpower input–Difficulty in attracting and retaining the talented candidates.

    3.3 Overloading/Idling.

    3.4 Up gradation of skills through training.

4. **Finance related Risks.**

    4.1 Financial Frauds.

    4.2 Appropriate/ productive usage of Funds.

5. **Enterprise related Risks.**

    5.1 Issues related to Intellectual Property Rights.
    5.2 Legal compliances.
    5.3 Marginal profits.
    5.4 Inadequate utilization of resources, viz manpower, fixed assets and funds.
    5.5 Order book position.
    5.6 Land Acquisition.

6. **Operations related Risks.**

    6.1 Dependency on OEM & Single vendor.
    6.2 Risks identified through QMS / EMS.
    6.3 Safety and Compliance.

7. **Impact of Government policy / legislation / environmental regulations.**

8. **Security related risks.**

    8.1 Cyber Security and Monitoring Risk.

9. **Corruption Risk.**

    9.1 Potential risk areas due to ineffective / improper process.

10. **Other Risks.**

    10.1 Risk arising from unutilized lands.
    10.2 Risk of carrying excessive inventory.
    10.3 Risk associated with Force majeure clause

Annexure-5

RISK MANAGEMENT STRATAGY & PROCESS IN GENERAL

1. Introduction.

1.1 Risk Management (RM) process is identified as the vital part of Bharat Dynamics Limited strategic management process. It is a continuous and developing process, which encompasses the organization's strategy and implementation of that strategy. This will address systematically all the risks surrounding Bharat Dynamics Limited past, present and future activities. Also, it will address risks arising out of internal and external factors.

1.2 Depending on the nature and severity of identified risk, following strategies shall be followed to manage potential risk:

1.2.1 Risk Avoidance: Not performing an activity that carries risk.

1.2.2 Risk Reduction: Reduction of severity of loss.

1.2.3 Risk Retention: Acceptance of loss when it happens.

1.2.4 Risk Transfer: Causing other party to accept the risk.

1.3 The Risk Management process consists of following steps:

1.3.1 **Risk assessment**:

1.3.1.1 Risk identification.

1.3.1.2 Risk description.

1.3.1.3 Risk estimation.

1.3.1.4 Risk evaluation.

1.3.2 **Risk reporting:** Threats, Opportunities, Strength and Weakness associated with risk identified.

1.3.3 **Decision:** Whether to take up the risk treatment or not, keeping in view the impact and associated costs for risk mitigation measures.

1.3.4 **Risk Treatment:** Measures identified for risk mitigation, parameters identified for effectiveness of mitigation measures, identification of risk owners in the organization, acceptable limits of risk and process for failure reporting.

1.3.5 **Residual risk reporting:** Mechanism of residual risk reporting after risk mitigation measures are implemented.

1.3.6 **Monitoring and review:** Monitoring of the risk Implementation measures and review with respect to parameters identified for effectiveness of these measures.

2. Risk Assessment

2.1 Risk Identification

2.1.1 The first step in risk assessment is risk identification based on organizational processes and the key drivers of the risks. The key drivers can be categorized (as an example) as given below in table 1:

Table-1: Example of Key Drivers or Factors for Risks.

Sl. No.	Type of Risk	Due to Internal Drivers	Due to External Drivers
1	Strategic Risks	- D&E - Intellectual Capital	- Competition - QR Changes of Customer - Customer demand - Technology Changes
2	Operational Risks	- Accounting Controls - Information - Recruitment - Supply Chain	- Regulations - Culture - Recruitment - Supply Chain
3	Reporting Risks	- Liquidity - Cash Flow - Inventory	- Interest Rates - Foreign Exchange Credit
4	Compliance Risks	- Employees - Properties - Products and Services	- Contracts - Natural Events - Suppliers - Environment

2.1.2 Identification of the risk category, i.e., Strategic, Operational, Reporting and Compliance helps in Risk Management.

2.1.3 Following methods can be adopted for risk identification:

2.1.3.1 Inputs from operating managers.

2.1.3.2 Brainstorming.

2.1.3.3 SWOT analysis.

2.1.3.4 Expert's inputs.

2.1.3.5 Scenario thinking.

2.1.4 While identifying the risk, following may be considered:

2.1.4.1 What is wrong or what are the shortcomings?

2.1.4.2 What can go wrong?

2.1.4.3 What can be done?

2.1.5 The risk identification process should be applied to all significant activities and all associated risks defined.

2.2 Risk Description.

2.2.1 Identified risks are to be captured in structured manner to facilitate the risk Assessment. Format-1 will be used for this purpose.

2.3 Risk Estimation.

2.3.1 This can be qualitative, semi-quantitative or quantitative in terms of occurrence and possible consequence. This risk estimation can also be captured in Format-2.

2.4 Risk Evaluation.

2.4.1 Consequences of the risk both in terms of threats and opportunities may be categorized under high, medium and low. Similarly, the possibility of occurrence may be categorized under high, medium and low. The estimation can be used to priorities the risks in conjunction with the cost and efforts associated with the risk treatment.

3. Potential for Implements.

3.1 Once risk evaluation is done and it is decided to go for treatment, then, the strategy and policy deployment is provided by URMC / CRMC and risk coordinator will implement the decision with necessary approvals and sanctions, wherever required. He will work under Risk owner who is mostly divisional head / functional head.

4. Strategy and Policy Deployment.

4.1 Once strategy and policy for risk treatment is developed and accepted, the same is required to be deployed.

5. Monitoring and Review.

5.1 As part of strategy and policy deployment, the risk owner should periodically present parameters for risk effectiveness measurement, failure and Success. Management shall review periodically.

Annexure-6

BASICS, DEFINITIONS AND ABBREVIATIONS

1. Introduction

Enterprise Risk Management (ERM) is the identification; assessment and prioritization of risk (defined in ISO 31000:2009 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor and control the probability and / or impact of unfortunate event or to maximize the realization of opportunities. Risk can come from uncertainty in project failures (at any phase in development, production or sustainment life cycles), legal liabilities, credit risk, accidents, financial markets, quality related, natural causes and disasters as well as deliberate attack from adversary or events of uncertain root cause.

ERM is the overreaching policy statement about the role of risk management with in BDL and the associated responsibilities of the management and staff.

2. Definitions:

2.1 **ERMS** – Enterprise Risk Management System.

2.2 **Risk** - The effect of uncertainty on objectives of the enterprise, resulting in loss or sub-optimal performance.

2.3 **Risk Management** – Coordinated activities to direct and control an organization with regard to risk.

2.4 **Risk Management Framework** – Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

2.5 **Risk Management Policy** - Statement of overall intentions and direction of an organization related to risk management.

2.6 ***Risk Attitude*** *– Organization's approach to access and eventually pursue, retain, take or turn away from risk.*

2.7 ***Risk Appetite*** *– Amount and type of risk that an organization is prepared to pursue, retain or take.*

2.8 **Risk Aversion** – Attitude to turn away from risk.

2.9 **Risk Management Plan** – Scheme within the risk management frame work specifying the approach, the management component and resources to be applied to the management of risk.

2.10 Risk Owner – Person or entity with the accountability and authority to manage the risk.

2.11 Risk Coordinator: Person assigned with responsibility to execute the activities required for mitigation of risk. He reports to Risk owner. It is preferable that they belongs to same division.

2.12 Risk Management Process – Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

2.13 Stake Holder *– Person or organization that can affect, be affected by, and perceive themselves to be affected by a decision or activity.*

2.14 Risk Assessment – Overall process of Risk identification, risk analysis and risk evaluation.

2.15 Risk Identification – Process of finding, recognizing and describing the risk.

2.16 Risk Source – Element which alone or in combination has the intrinsic potential to give rise to risk.

2.17 Risk Profile – Description of any set of risks.

2.18 Risk Analysis – Process to comprehend the nature of risk and to determine the level of risk.

2.19 Risk Criteria – terms of reference against which the significance of a risk misevaluated.

2.20 Level of Risk – magnitude of a risk expressed in terms of the combination of consequences and their likelihood.

2.21 Risk Evaluation – Process of comparing the results of risk analysis with risk criteria to determine whether the risk and / or its magnitude is acceptable or tolerable.

2.22 Risk treatment – process to modify the risk.

3. List of Abbreviations:

3.1	**BD**	Business Development
3.2	**BDL**	Bharat Dynamics Limited
3.3	**CC**	Corporate Commercial
3.4	**CO**	Corporate Office
3.5	**C.PLG**	Corporate Planning
3.6	**CQC**	Corporate Quality Control
3.7	**CRM**	Corporate Risk Manager
3.8	**CRMC**	Corporate Risk Management Committee
3.9	**DRMC**	Divisional Risk Management Committee
3.10	**DRDO**	Defence Research Development Organization
3.11	**URM**	Unit Risk Manager
3.12	**URMC**	Unit Risk Management Committee
3.13	**D&E**	Design & Engineering
3.14	**ERM**	Enterprise Risk Management
3.15	**FD**	Functional Director
3.16	**IA**	Internal Audit
3.17	**LD**	Liquidated Damage
3.18	**OEM**	Original Equipment Manufacturer
3.19	**P&A**	Personnel & Administration
3.20	**RM**	Risk Management
3.21	**RMC**	Risk Management Committee
3.22	**SWOT**	Strengths, Weaknesses, Opportunity & Threats
3.23	**TOT**	Transfer of Technology
3.24	**IRC**	Internal Review Committee

Format-1

RISK IDENTIFICATION FORMAT

Risk Control No: Date:

Department: Division: Unit:

Area of the risk (Ref Annexure 4) Category of Risk: Strategic/ Operational /Reporting / Compliance

1. Description of the risk:
2. Department primarily associated with Risk:
3. Impact/ consequence of Risk (Descriptive):
4. Risk Estimate

   a) Probability / Likelihood (1 to 5)

   b) Consequence (1 to 5)

   c) Risk Score (= a*b) (1 to 25)

Risk Score ≤ 6 is Low; > 6 ≤ 15 is Medium; > 15 is High

   High / Medium / Low

5. **Existing Controls of Risk:**

   a. Adequacy of process:
   (Refer Existing Control – Risk assessment table)

   b. Specify how it is being handled:

6. **Risk Mitigation**

   a) Suggested Risk Treatment / Mitigation Plan:

   b) Policy changes, specify if required:

   c) Funds requirements:

   d) Target Date.

Initiated by:

Signature:
Name:
Designation

Departmental Head

Risk Owner: (Name Designation) *

Risk coordinator: (Name Designation)*

Functional / Divisional Head:

URM / CRM

To

Convenor URMC / CRMC - For inclusion into Risk review format

Notes:

1) * - Risk owner & Risk Coordinators are to be nominated by Divisional Heads in case of Divisions or Functional Heads in case of common services or corporate.

RISK REGISTER

Format-2

Risk Register

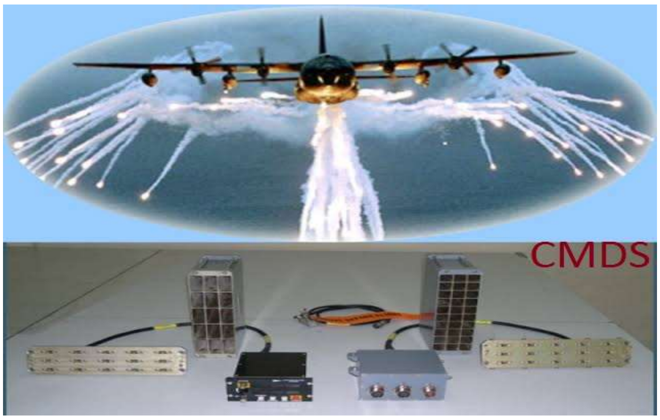
Department:

Division:

Unit:

Remarks					
Target Date					
Risk Coordinator					
Risk Mitigation / Treatment Plan (Preventive or Contingency)					
Existing Controls					
To be Considered (YES / No)					
Risk Score (L / M / H)					
Consequences (1 to 5)					
Likelihood /probability (1 to 5)					
Impact of Risk(Identify consequences)					
Risk Description(Including any identified triggers)					
Area of Risk & Risk Owner					
Department					
Review No & Date					
Date					
Risk No.					

Note:



BHARAT DYNAMICS LTD.
(A Govt. of India Enterprise)