RISK MANAGEMENT POLICY

1 Purpose:

1.1 The purpose of the Risk Management Policy is to enable and support the Board in structured and effective management of Risks.

2 Approach:

2.1 Considering the status of various programs, projects and the emerging business scenario where a level playing market field is being created in the aerospace defense industry, a philosophy that must consistently guide the company's risk management approach is given below:

"Empowering business growth and competitiveness through strategic and structured Risk taking and sustained risk mitigation"

2.2 This philosophy implies Risk Management will be applied in a transparent environment, to sustain the business growth and profitability in a competitive market through structured risk taking and risk mitigation processes.

2.3 These processes will strengthen Technology Absorption and Development, product delivery, service and up-gradation, substantive self-reliance, Product Availability and affordability. This philosophy will be driven by a risk aware mindset where avoidance of necessary risks is discouraged.

2.4 The Risk Management Policy will initially keep the processes flexible to enable the users to adapt to their needs. The Board is provided with information on high risks identified and the plans for mitigation once **every six months.** Each complex MD/CEO will present the reports. The strategic planning group in CO will also present a feed forward map of the potential risks in the Political, economic, government policy, social and market/technology environment for the Board to consider changes in strategies and plans that may be required.

2.5 Risks shall be addressed effectively at each level through an appropriate organization and commensurate allocation of resources.

3 Scope:

3.1 Significant proposals that are approved by COPs / GMs / EDs / MDs / CEOs / FDs / Chairman / MC / Board will contain a summary of the Risk Assessment in the proposals and the Risk mitigation plans that are built into the proposals. Here significance implies short term and long term impact on financial and strategic parameters.

3.2 Contract drafting executives and Negotiating committees will address the Risks that are likely to emanate from the contracts.

3.3. Risk Management Policy steps in line with sub-policy on Corruption Risk Management (Annexure-9) and its scope is given therein.

3.4 Risks of legal /statutory non-compliances.

4. Responsibility:

4.1 The respective EDs / GMs / COPs / Project / Program managers will be responsible for embedding the processes required for the effective identification, assessment and mitigation and review of Risks arising out of Political, economic, government policy, social and market/technology environment as well as the internal risks projected by the various functions based on their perceptions and data.

4.2 The respective EDs / GMs / COPs / Project / Program managers will be responsible for ensuring that all personnel who are involved in planning / contracting / negotiating are appropriately trained in understanding the approach, framework and processes for identifying, assessing and mitigating risks.

4.3 The Mitigation plans should be focused and acted on within **six months** of the identification. The responsibility for acting on each Risk mitigating plan must be clearly defined. All monthly program, project and divisional performance reviews will highlight the progress or lack of progress on the mitigation plans till the closure of the risk mitigation plan is signed off by the respective ED / GM / COP / Project / Program Manager. Reports of the closure must be sent to the next higher authority for confirmation.

4.4 The respective ED / GM’s of Divisions / Complex will be responsible for ensuring compliance with the sub-policy on Corruption Risk Management.

5. Framework:

5.1 The Risk identification, assessment and analysis framework may be based on processes identified in the Annexure 1 to 9 as appropriate.

6. **Key Definitions and Explanations:**

6.1 **Risk:** Risk is an event that is likely to occur, which can potentially have an adverse impact (consequence) on the planned outcomes of a proposal, project or business decision. A Risk can be a result of unintended outcomes of well-reasoned decisions also.

6.2 Risks are normally assessed subjectively and initially dialogue would be required to arrive at the Risk level.

7 **Categories of Risks:**

Risks will be categorized as follows in order to clarify the approaches to be taken for risk mitigation and to allow risks to be taken where they are necessary for the survival and growth of the company.

7.1 **Category I: Preventable Risks**

7.1.1 These are internal risks, arising from within the organization, that are controllable and ought to be eliminated or avoided. Examples are the risks from (gaps in systems and decision making processes that need improvements), breakdowns in routine operational processes as well as and employees' and managers' unauthorized, illegal, unethical, incorrect, or inappropriate actions, which are covered by HR, Vigilance and System audit Policies.

7.1.2 This risk category is best managed through active prevention, i.e. monitoring operational processes, reviewing and improving systems and procedures and guiding and training people's behaviors and decisions toward desired systems and laid down norms.

7.2 **Category II: Strategy Risks**

7.2.1 These risks occur when the company or a division voluntarily accepts some risk in order to generate superior returns from its strategy. An example is when the company takes on risks through the research and development activities through its own funding, or accepts orders to penetrate markets with lesser than normal profits or as a Risk Sharing partner in an International program. Strategy risks are quite different from preventable risks because they are not inherently undesirable. A strategy with high expected returns generally requires the company to take on significant risks, and managing those risks is a key driver in capturing the potential gains.

7.3 **Category III: External Risks**

7.3.1 Some risks arise from events outside the company and are beyond its influence or control. Sources of these risks include major macroeconomic and geographical changes, policy changes by governments and changes in supply and competitive environments. External risks require another approach by managers to focus on identification and mitigation of their impact.

7.4 As the Risk Management Process matures, different processes can be adopted for each category depending on their applicability and the effect of the Risks on the growth of the company.

8. **Suggested Approaches to Mitigation Plan for High Level Risk**:

A few of the High impact risks that can affect the company's revenues and market share in the future and their mitigation plans are given below:

8.1 **Mitigation for Risks in Product Performance**

8.1.1 Contract related Risks and weaknesses should be addressed through a team of CO consisting of Planning, Contracts Cell and Legal cell. They may address review gaps in contracting in TOT leading to weaknesses in selecting the technology or inadequate depth in transfer of technology or in delays in receiving technology for product support. These gaps may be plugged to the extent feasible, in all new contracts yet to be signed – MMRCA, FGFA, MTA.

8.1.2 Risks in technology processes and competencies including risks of quality failures due to improper / inadequate inspection or inadequate supervisions should be addressed by EDs / GMs / COPs through Mitigation plans and reported to the appropriate higher authorities or management. Where feasible the use of IT to strengthen these practices may be followed. Due diligence needs to be ensured to distinguish between systemic and personal causes of the risks to avoid individual blame.

8.2 **Mitigation for Risks in Product Delivery**

8.2.1 Any potential Risks of inadequacy of Project team formation (including planned strength and competencies) should be addressed by the respective ED / GM / COP or MD / CEO of the Complex and reported to the appropriate higher authorities or management. Similarly any other risks that may arise, which can have an impact on product or service delivery including liquidated damages, inventory holding should be addressed by the respective ED / GM / COP or MD / CEO of the Complex in consultation with FC / CFC and reported to the appropriate higher authorities or management. Risks due to development of critical must be assessed, including Vendor delivery related risks. Mitigation plans for ensuring that product delivery is not affected by the delays in the development and certification of the systems and sub-systems. They must be reviewed and redrawn to ensure effectiveness of the mitigation plans.

8.2.2 A policy on indigenization is required to be established to prevent destabilization of supplies due to recertification delays. (This has been addressed through recent changes in the DOP)

8.2.3 It is recommended that Risks relating to Purchase and outsourcing across multiple Divisions should be reviewed by the respective COPs or program managers every year and reported to the appropriate higher authorities or management.

8.2.4 Risks on account of Force Majeure clauses should also be indicated wherever applicable, by the respective Purchasing or Outsourcing department heads, in terms of their impact on product delivery and realization of payments. Their recommendations for plans for such risk mitigation should be reviewed.

8.3 Mitigation for Financial Risks

8.3.1 The respective finance heads should create an appropriate mechanism and financial information system for capturing the risks of cost overrun and bringing it to the attention of the Divisional / Project / Program management. Finance & IMM Head of the Division may also discuss in Divisional Committee of Management meeting on the aspects of budget monitoring, System Audit Reports, etc.

8.3.2 The Corporate Finance group will submit an assessment of the risks due to excessive Reserves and Surpluses, Cash and Bank Balances which are not in line with the business needs in gainfully deploying surpluses (to prevent a risk aversive mindset).

8.3.3 A Corporate annual SWOT (Strengths. Weaknesses, opportunities and Threats) analysis will be presented to the MC by Corporate Planning group for review of the strategies and for initiating and strengthening focused mitigation actions on risks arising out of Threats including threats arising out of current and potential competition for expected orders.

8.3.4 Financial risks arising out of Design and Development efforts with or without orders must be assessed and mitigation plans be prepared by the Corporate Planning group.

8.4 Mitigation for Risks transferred by partners/ stakeholders

8.4.1 The Complexes may evaluate Risks transferred by partners in current and future projects, prepare the risk mitigation plans and report the same to the Corporate Office. This will include risks arising out of changes in relevant Government Policies. The Corporate Office team mentioned in Para 8.1 above will assess the extent of risk mitigation and report as necessary to the MC.

8.5 **Mitigation of HR Risks**

8.5.1 Risks on talent acquisition, retention, engagement and Knowledge Management should be addressed by CO HR and reported to HR Sub-committee of the Board.

8.6 **Mitigation of Corruption Risks**

8.6.1 The Corporate Vigilance Office will consolidate the corruption risks identified by Corporate Vigilance and submit and suggest measures to mitigate minimize / eliminate and control corruption risks. The details of this sub-policy are placed in Annexure – 9.

8.6.2 The Corporate Vigilance Department will forward Annual Report on status of complaints received and cases of violations of CRM Policy to Risk Cell for submission to the Management Committee & Audit Committee.

8.7 **Mitigation of Legal Risks**

8.7.1 CO Legal Section and Company Secretariat will review the risks arising out of practical difficulties involved in legal and statutory compliances and the mitigation plans required will be prepared by the respective Divisional / Complex offices.

8.7 Mitigation of Legal Risks

8.7.1 CO Legal Section and Company Secretariat will review the risks arising out of practical difficulties involved in legal and statutory compliances and the mitigation plans required will be prepared by the respective Divisional / Complex offices.

8.8 Mitigation of ESG Risks

8.8.1 Business Responsibility and Sustainability Report (BRSR) has been introduced by Securities and Exchange Board of India (SEBI) as a compliance, which has elaborate provisions for Environment, Social & Corporate Governance (ESG) and hence the same will be dealt as part of BRSR.

8.9 **Mitigation of Cyber Security Risks**

8.9.1 As part of the IT Security Policy of the company, Cyber Security Risks will be presented to RMC along with existing risk reporting template (Annexure-7) of RMP.

8.10 **Mitigation of Business Continuity Plan (BCP) Risks**

8.10.1 A template for checklist for BCP of the company is prepared and placed at Annexure – 10, which covers up different parameters. The Divisions as part of ISO 9001:2015(E) will include BCP. Compliance will be submitted in the annual review by RMC.

8.11 **Annual Review**

8.11.1 Risks will be placed for review by the Risk Management Committee periodically covering inter-alia the following:

a) Operational Risk by DRMC
b) Strategic Risk by Corporate Planning
c) Cyber Security Risk by CO-IT (Cyber security cell)
d) Compliance of BCP

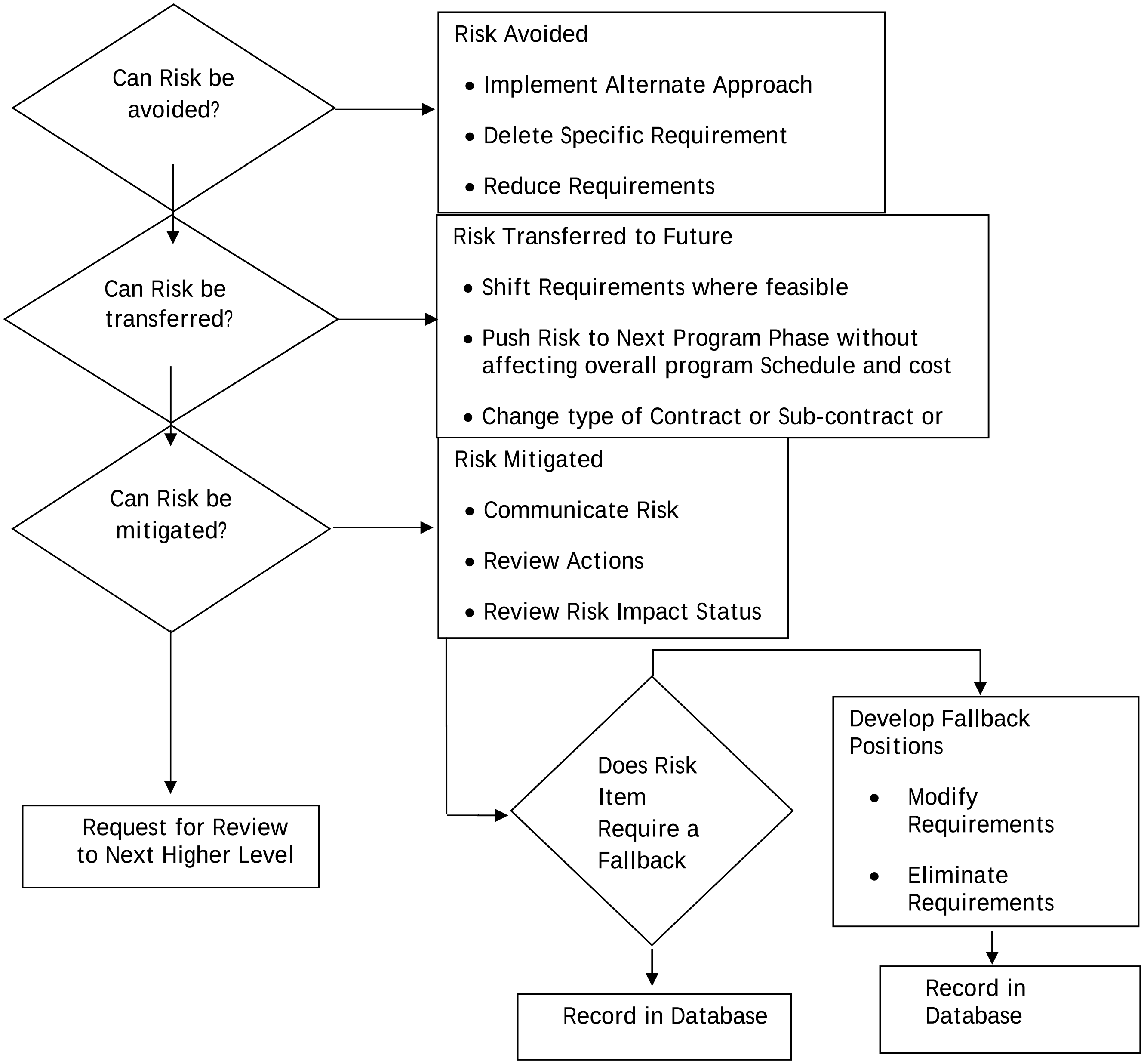
ANNEXURE - 1

RISK MANAGEMENT STEPS

Steps	**Procedure**	**Output**
Identify Risk events	1. Take an appropriate planning time horizon. Use brainstorming technique and the following inputs. 2. Consider plans for the period and data from internal information and understanding of technical and management Processes, finance, HR and IR reports and 3. Include analysis of external technology, economy, business and political events and developments 4. If possible obtain Expert judgment 5. Create a What-if scenario of uncertain events that can impact the planned results positively or negatively.	1. A list of risk events and alternative likely scenarios 2. SWOT Analysis
Qualitative Risk Analysis	1. Construct impact statements using the "If--- Then ------" for each scenario. 2. Evaluate the likelihood of the events happening as low, medium and high 3. Evaluate the impact of the event in terms of cost or delivery or quality or business in terms of low, medium and high.* 4. Prioritize the risks for actions	1. Risk Register 2. Risk Cube 3. Risk Impact classification
Plan Risk responses	1. Communicate the risks identified to the appropriate levels. Include in the proposal where necessary. 2. Analyze and prepare the actions that will mitigate the likelihood of events or the impact of the risks 3. Identify or obtain resources for taking the actions in a focused manner including the officer assigned for mitigating and reporting the same. The 4. Communicate a review plan. Include the same in the proposal.	1. Risk Mitigation plan with responsibilities 2. Risk mitigation plan Report 3. Risk Review schedule and reporting structure
Monitor and Control	1. Review reports and assess degree of risk mitigation 2. Assess impact of reduced risk on costs, schedules, business, products , cash flow etc 3. Close risk plans or scale up risk management 4. Feedback lessons learnt for training	1. Risk mitigation status 2. Closed risks register 3. Lessons learnt

ANNEXURE - 2

RISK HANDLING DECISION FLOW


Can Risk be avoided?
Risk Avoided
• Implement Alternate Approach
• Delete Specific Requirement
• Reduce Requirements
Can Risk be transferred?
Risk Transferred to Future
• Shift Requirements where feasible
• Push Risk to Next Program Phase without affecting overall program Schedule and cost
• Change type of Contract or Sub-contract or
Can Risk be mitigated?
Risk Mitigated
• Communicate Risk
• Review Actions
• Review Risk Impact Status
Request for Review to Next Higher Level
Does Risk Item Require a Fallback
Develop Fallback Positions
• Modify Requirements
• Eliminate Requirements
Record in Database
Record in Database

ANNEXURE - 3

TOOLS AND TECHNIQUES

The Risk Cube will be used to evaluate risks and monitor the progress on the impact of the mitigation plans.

🟥 HIGH
🟨 MEDIUM
🟩 LOW

5	🟩	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥 X	🟥 O
3	🟩	🟩	🟨	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨
	1	2	3	4	5

CONSEQUENCE

ANNEXURE - 4

CHECKLIST OF RISKS FOR INDIGENOUS PROJECTS

- Selection of technologies Impact on cost, time and life cycle management due to level of maturity of technology and time for readiness for production

- Selection of partners and contracts thereof Impact of extent of choice and its impact on negotiating power, cost, time and long term ability for life cycle management
- Opportunities for acquiring new dimensions to organizational capabilities Impact on Strategic competitive edge and new markets / product lines and core competencies

- Opportunities for funding attracting funding opportunities Impact on financial strength

- Opportunities for Intellectual Property rights Impact on competitiveness
- Opportunities for reducing overall company cost structure better utilization of core assets - Impact on profits

- Delegation of powers - Impact on critical path decision making and time
- Expertise requirement - Capacity and capability assessment - Impact on quality / reliability / design rework levels and thereby cost and time

- Setting of Infrastructure and effective and timely capital expenditure management - Impact on costs and time

- Creation of Project Teams in time for all critical and non-critical path activities including domain experts - Impact on time.

- Adequacy of trained manpower and bench strength for peak and non-peak project periods Impact on time

- Preparation of Partner organizations and aerospace eco-system for project execution - Impact on cost and time

- Information Management - integration of design modifications / shortfalls through System architecture and hierarchy and use of unified PLM / CAD / CAM Impact on rework / cost / time

- Make or buy decisions - Impact on strategic. Core competencies and costs/time

- Volume and economies of scale - Impact on costs

- Indigenous Design and development challenges / limitations - fulfilling strategic need for technological up gradation - impact on cost and opportunities

- Restrictive Technology export practices - Impact on long term serviceability of imported LRUs, cost and time

ANNEXURE - 5

CHECKLIST OF RISKS FOR TOT PROJECTS

- Inter-government agreements and restrictions - Impact of extent of access to technology, level of technology transfer or sharing, mode of evaluation of technology transfer, speed of resolution of conflicts and disputes on program time, cost and strategic

- Convergence of Schedule of transfer documents, Tools, availability of appropriate people and Training – Impact on critical path length and costs

- Project supplies from licensor associates – Impact on costs and schedules
- Technology transfer scope (from Design approach to Maintenance, repair and overhaul)

- Impact on Time for Technology transfer and implementation of project for fleet serviceability

- Contractual terms for support in managing obsolescence management – Impact on Life cycle management

- Technology readiness level of product and technologies including software – Impact on contracted delivery

- Setting of Infrastructure and effective and timely capital expenditure management – Impact on costs and time

- Creation of Project Teams in time for all critical and non-critical path activities including domain experts - Impact on time.

- Adequacy of trained manpower and bench strength for peak and non-peak project periods - Impact on time

- Preparation of Partner organizations and aerospace eco-system for project execution - Impact on cost and time

- Offset opportunities - Impact on Capacity, Competitive strength, Strategic benefits / Disadvantage contractual Risks

- Export opportunities – Impact on profitability, capability, capacity.

ANNEXURE - 6

FORMAT FOR RISK ANALYSIS

I. Name of the program:
II. Contract Reference:
III. Funding Status:
IV. Value of contract:
V. Time frame work:

TO:

Milestone 1:

Milestone 2:

Milestone 3:

IOC :

FOC :

VI. Technologies selected:

VII. Key supply chain / Design and development partners:

ANNEXURE - 7

FORMAT OF RISK IDENTIFICATION AND ASSESSMENT

Risk Description	Likelihood	Likely Impact Statement	Quantified Time / Cost / Other Impact	Risk Impact Level: High / Medium / low

ANNEXURE - 8

LIKELIHOOD VS CONSEQUENCE RATING CHART

(Table for classification of Risk Occurrence and Risk Impact)

Classification of Consequences – Both Threats and Opportunities	
High	Financial impact on the organization is likely to exceed 25% on the value of the proposals under consideration. Significant impact on the organization's strategy or operational activities Significant stakeholder concern
Medium	Financial impact on the organization likely to be between 10 and 25%. Moderate impact on the organization's strategy or operational activities Moderate stakeholder concern
Low	Financial impact on the organization likely to be less than 10% or Rs 10 Crores, whichever is lower Low impact on the organization's strategy or operational activities Low stakeholder concern

Probability of Occurrence – Threats		
Estimation	**Description**	**Indicators**
High (Probable)	Likely to occur repeatedly each year or more than 25% chance of occurrence.	Potential of it occurring several times within the project time period (for example three years). Has occurred recently.
Medium (Possible)	Likely to occur in a three year time period or less than 25% chance of occurrence.	Could occur more than once within the time period (for example three years). Could be difficult to control due to some external influences. Is there a history of occurrence?
Low (remote)	Not likely to occur in a three year period or less than 2% chance of occurrence.	Has not occurred. Unlikely to occur.

ANNEXURE - 9

CORRUPTION RISK MANAGEMENT (CRM) SUB - POLICY

I) PREAMBLE:

a) Hindustan Aeronautics Limited (HAL), a public sector undertaking under the Ministry of Defence is premier Aerospace Complex in Asia involved in Design & Manufacture of aircraft & helicopters, aero engines, accessories and avionics (www.hal-india.com), with vision to become a significant global player in the aerospace industry.

b) Our business is built on seven core values. Integrity is one of seven core values in the company and a key for ethical and good corporate governance.

c) HAL has in place procedures and policies for all core business processes to ensure ethical and good corporate governance and uphold integrity of all stakeholders including third parties involved directly and indirectly in business transactions with the company.

d) Our business processes are continuously updated to strive towards Transparency, Openness, Integrity and Accountability in all our business processes.

e) It is normal for an Organization to be exposed to various risks in the course of execution of business objectives. HAL has operationalized "Risk Management Policy" to address business risks broadly categorised under Preventive, Strategic and External Risks.

f) Corruption is one of the major operational risk in achieving the business objectives which may be classified under the Preventable Risk Category.

g) Corruption is an intentional act of deception committed by individuals or group of people including but not limited to fraud, graft, nepotism, and abuse of public position, financial misappropriation, bribery, financial misconduct and other irregularities involving public money. It is abuse of official position / entrusted power for personal / private gain.

h) It is recognised that the risk of corruption is present and may occur in the organization in view of complex, ever changing business scenarios and impact of internal and external factors. Corruption is a major deterrent for ethical & good corporate governance.

II) **FRAME WORK**

As mandated by the DPE (Department of Public Enterprises) & CVC (Central Vigilance Commission) guidelines / instructions, public sector enterprises need to implement Corruption Risk Management policy and identify areas vulnerable to corruption. The policy framework all needs to identify and implement the measures required to mitigate, minimize / eliminate and control corruption related risks.

III) **STATEMENT**

a) HAL is committed to promote and adhere to the highest standards of probity, transparency and accountability in business operations and management of the organization. Through this policy, we commit fully and unequivocally to adopt a zero-tolerance approach towards corruption and we further commit to ensure compliance to the anti-corruption policy of organization and laws of state.

b) We shall continue to make all efforts to eliminate corruption associated with company business activities and promote transparency, accountability and integrity at all levels and across stakeholders through effective prevention, identification and punishment of all corrupt practices by leveraging Information Technology enabled tools. The policy outlines the company's systematic approach to identification, reporting, response & mitigation of corruption risks.

IV) **OBJECTIVES**

The objective is to create and implement a Corruption Risk Management (CRM) policy with holistic framework that minimises the risks of corruption, which shall aim at:

a) Raising awareness among all stakeholders about CRM and commitment for zero tolerance towards corruption.

b) To identify corruption risks associated with risk prone specific business processes, evaluate & rate the risks and put in place mitigation measures to address each type of risks.

c) Defining responsibilities of management and stakeholders in implementing this policy, identification and prevention of corruption.

d) Deterrent action against corrupt conduct by strict, prompt and uniform enforcement of Anti-corruption regulations and laws.

e) Reviewing corruption prevention controls and strengthening legal and regulatory framework of accountability as well as enforcement agencies.

f) Monitoring and Review of Policy at regular intervals to cope up with operational demands.

g) Learning from experiences & continually improving compliance, ethical decision making and integrity quotient of the Organization.

V) **SCOPE:**

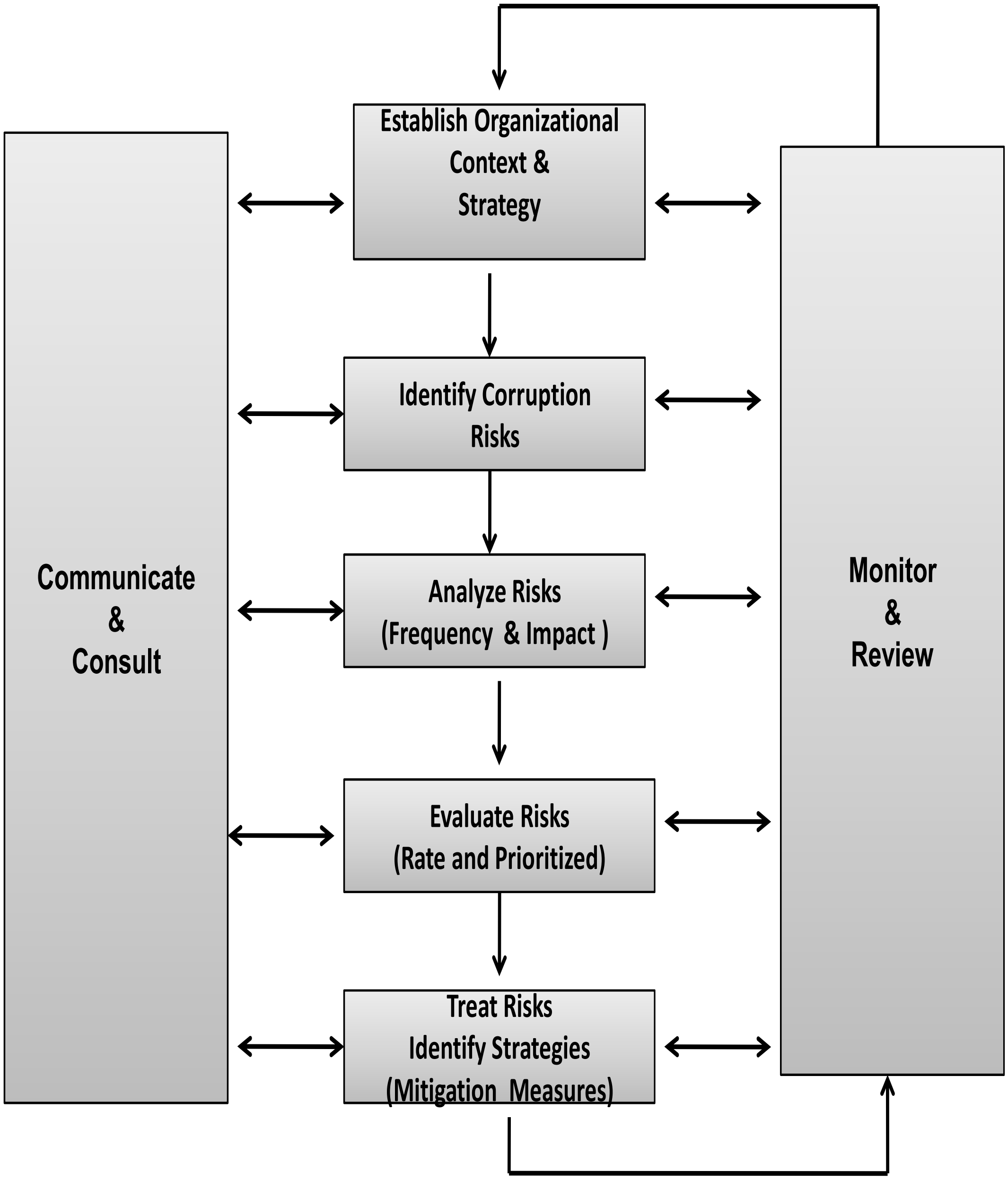
The scope of this policy covers the following:

a) This policy applies to all stakeholders including but not limited to all Whole time Board of Directors, and Independent Directors, Senior Management, Officers and other employee(s), ex-employee(s) working as advisors / consultants, persons engaged on contract / temporary basis, consultants etc.

b) This policy is applicable to external stakeholders through incorporation of appropriate clauses intenders / agreements / contracts etc.

c) External stakeholder shall include but not limited to suppliers / contractors / sub-contractors / Joint Ventures / Ancillaries / service providers / other outside agencies & representatives of suppliers / contractors / subcontractors / service providers / other outside agencies, who are doing business with the company and or any other parties having a business relationship with the company or any person acting in an official capacity for or on behalf of any of suppliers / contractors / subcontractors / service providers / Joint Ventures / Ancillaries / other outside agencies.

VI) CRM PROCESS - GRAPHICAL REPRESENTATION


Establish Organizational Context & Strategy
Identify Corruption Risks
Analyze Risks (Frequency & Impact)
Evaluate Risks (Rate and Prioritized)
Treat Risks Identify Strategies (Mitigation Measures)
Communicate & Consult
Monitor & Review

STAGES INVOLVED IN CORRUPTION RISK MANAGEMENT PROCESS

VII) **Publicity & Training**

Awareness will be created among all related stakeholders through wide publicity and training. Towards this adequate information and awareness about CRM policy & related regulations in case of violations, Complaint lodging in case of notice of any violations etc. will be created through:

a) Internal and external web enabled applications,

b) Appropriate display at entrance of divisions or offices at Reception, Security Gates, Head of Divisions office / Complex offices / Corporate Offices, Administrative department,

c) Regular awareness classes to all stakeholders to spell out the company's expectations for compliance with its corporate policies and procedures as well as anti corruptions laws and regulations. Training sessions shall be well documented & archived.

d) Handbooks to newly recruited employees, undertaking by employees / consultants / those engaged on contract basis etc to ensure compliance to CRM policy.

e) Incorporation of appropriate conditions in tender / contracts / orders / agreements etc.

VIII) **Responsibilities of Vigilance, Management and stakeholders in implementing policy**

The responsibilities are broadly categorised as under:-

a) **Vigilance Department:**

i. The divisional / corporate vigilance department shall identify the corruption related risks based on complaints, intelligent information sources and other means and rate the risks with suggested mitigation measures.

ii. The divisional vigilance department to submit annual report to CVO, HAL.

iii. It is responsibility of Corporate Vigilance Office (being Head office for Vigilance) to consolidate the corruption risks identified at division as well as corruption risks identified by Corporate Vigilance and submit comprehensive annual report to Management including corruption risks identified and suggested measures to mitigate, minimize / eliminate and control these risks

b) **Line / Staff Management:**

i. CRM policy implementation and compliance shall be driven by strong tone at the top management through strong administration and oversight of compliance.

ii. It is the responsibility of Head of division and Heads of every department to promote the anti-corruption policy within their areas of operation and to maintain an effective control system. They shall provide information to vigilance department on any noncompliance and potential corruption risks.

iii. It is responsibility of Corporate Management to take adequate mitigation and control measures based on annual report submitted by Vigilance and also ensure implementation of same by bringing in requisite changes in policy / procedures and administrative measures and other means as necessary.

c) **Other Stakeholders:**

All other stakeholder including third parties shall read, be familiar with and strictly comply with the policy. They shall actively report corruption to Vigilance department or Management and also prevent corruption practices.

IX) Corruption Risk Assessment (Actions Constituting Corruption):

a) The risk of corruption may occur in any sphere of business activities and may evolve in the light of changing circumstances and working environment or external influences or loophole in policies / procedures. In its endeavor to proactively address risks of corruption, it shall be ensured that a proper corruption risk management process is in place. Corruption Risk assessment shall focus on a thorough analysis of the functional activities in close collaboration with internal stakeholders involved in the processes with a view to identify potential corruption risk areas. The corruption risks shall also be identified based on complaints and other sources.

b) The corruption risks linked to business activity / processes and rating to identify the impact of corruption risks shall be done as per Enclosure - 01. The report on corruption risks shall be submitted based on the guidelines and as per format specified at Enclosure - 01.

X) **Corruption Prevention, Identification of Risks & its management (through Policy, Procedures, Audits, Surprise checks, Clarity in Reasonability and Accountability, Complaint handling)**

a) **Corruption Prevention:**

Company has laid down the following procedures / policies (which is illustrative and not exhaustive) towards ensuring compliance to high standards of ethics, transparency and fairness in all sensitive functional areas. The same shall be updated and circulated to all as and when required.

i. Senior Officers Code of Conduct
ii. Officers Code of Conduct (HAL CDA Rules, 1984)
iii. Standing Orders for Workmen
iv. Manuals / Procedure for recruitment, promotion, purchases, outsourcing, Works.
v. Delegation of Power to ensure proper responsibility and accountability for approvals.
vi. Preventive and punitive vigilance activities & other initiatives of Vigilance department.
vii. Signing of Integrity pact by bidders.
viii. Undertaking from employees engaged on contract basis etc.
ix. Job Rotation in sensitive functional areas.
x. Security system

b) **Identification of Corruption Risks:**

i. Company stakeholders who become aware of or suspect a violation of this Policy are under an obligation to report the same to the Company.

ii. Each of stakeholder will be encouraged to report wrongdoing and notify the company of suspected violations of the company's CRM policy and applicable regulations.

iii. Any non compliance will be also identified through routine auditing of files, Accounts, Project Reports etc by Auditors / Routine or Surprise verification by vigilance department.

iv. Promotion of Whistle blower policy.

c) **Complaint Management (by Vigilance Department)**

i. Any complaint related to corruption received by any stakeholder shall be referred to CVO, HAL for taking action as per laid down complaint handling policy of the company.

ii. Any stakeholder can lodge Complaint online by logging into HAL website. All complaints will be handled by Vigilance department as per Complaint handing procedure as detailed in Vigilance Manual within the time limits as defined.

d) **Action against corrupt conduct**

Based on investigation carried out by Vigilance department / Central Bureau of Investigation (CBI) / Police in case the complaint is referred to CBI / Local Police to investigate on account of limitation of jurisdiction of Vigilance, the report will be submitted to Disciplinary authority for appropriate action against those involved in corrupt conduct as per CDA rules / Standing Order of company apart from any legal provisions if applicable. However cases where company does not have jurisdiction to take action, legal action will be taken as per prevailing regulatory frame works (As per Contract Terms, Provisions of Integrity Pact, Prevention of Corruption Act, 1988 (as amended from time to time), The Lokpal and the Lokayuktas Act, 2013 (as amended from time to time) and other regulations effective at that point of time.

XI) Review of Policy & Corruption prevention controls

The Corruption Risk Management Policy will be reviewed as and when required by Risk Cell CO in coordination with CVO, HAL. The CRM policy will be reviewed annually during Risk Management Conference organized as per the mandate of the approved Risk Management policy. All such reviews will be based on:

i. inputs from Chief Vigilance Officer, HAL based on findings of various cases related to corruption;

ii. inputs from various stakeholders;

iii. Due to the changes in the regulations / Govt. guidelines or best practices etc.

iv. Need to strengthen effectiveness and adequacy of the Internal Control System to provide assurance that they are effective in countering corruption opportunities.

The outcome of such review will be put up to Management (Board of Directors) with suitable recommendations for additional / deletion / modification of policy and implementation of adequate controls / modification of procedures / manuals etc to mitigate risks of corruption. On approval the changes would be notified by the Management for information and compliance by all stakeholders.

XII) **Information to Management Committee and Audit Committee**

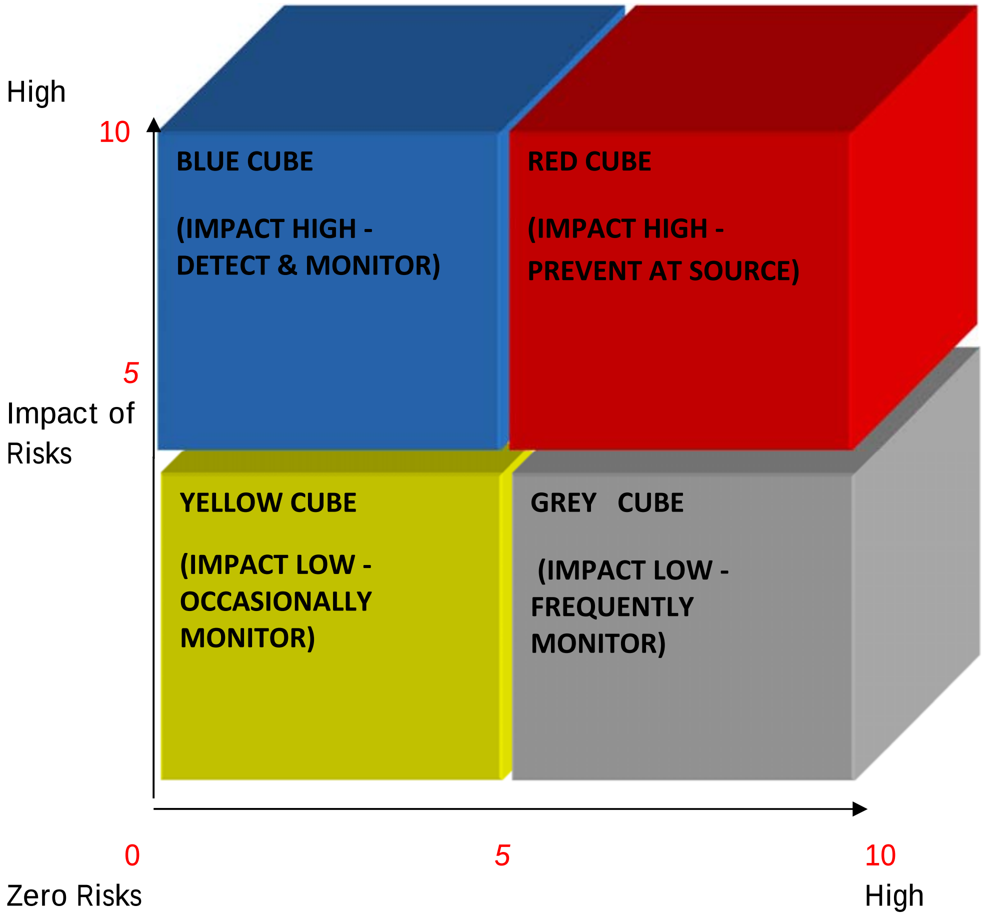
The Risk Cell of Corporate Office will report its collective findings to Management Committee (MC) & Audit Committee of the Board on annual basis (based on annual conference) about compliance to CRM policy and details of complaints, investigation status, action taken, review of controls / procedures, instances of non compliance of CRM policy and actions taken to strengthen policy on basis of previous lessons learnt based on investigations.

The Corporate Vigilance Department will forward annual report on status of complaints received and cases of violations of CRM policy to Risk cell for onwards submission to Audit Committee.

****

ENCLOSURE - 1

RISK ASSESSMENT CUBE


High
10
5
Impact of Risks
BLUE CUBE
(IMPACT HIGH - DETECT & MONITOR)
RED CUBE
(IMPACT HIGH - PREVENT AT SOURCE)
YELLOW CUBE
(IMPACT LOW - OCCASIONALLY MONITOR)
GREY CUBE
(IMPACT LOW - FREQUENTLY MONITOR)
0
Zero Risks
5
10
High

LIKELIHOOD OF RISKS

Sl. No.	Activity	How activities are prone to corruption (Corruption Risks)	Rating (Color Code of Risk Cube)	Suggested Mitigation Measures.

Rating: Classify / Rate the corruption risks into four Cubes based on parameters like frequency, if it happened what is impact in terms of cost to company, reputation damage, loss of customers and stakeholders confidence easy of corruption in particular activity etc. Accordingly risks will be classified into Cubes in which it falls, which will be the basis for arriving at Risk mitigation and Controls.

Risk Cube Rating	Types of Risks classified under the Cube
RED	IMPACT IS HIGH AND HENCE PREVENT AT SOURCE SINCE IT MAY AFFECT BUSINESS OBJECTIVES
BLUE	IMPACT IS HIGH IF IT OCCRUES, HENCE DETECT AND ADEQUATE MONITORING. FREQUENCY IS LOW. BUT WHENEVER IT OCCURS IMPACT IS HIGH.
GREY	REQUIRES FREQUENT MONITORING IMPACT IS LOW BUT FREQUENCY IS HIGH. IF NOT CONTROLLED / MONITORED IT MAY MOVE TO 'CUBE RED'.
YELLOW	LOW LEVEL OF MONITORING AND CONTROL.

Note: Use color code for Rating (example if type of risk falls under CUBE - RED, then put 'RED' under rating column against that corruption risk).

ANNEXURE - 10

Indicative Checklist for BCP		
Sl No	**BCP Elements**	**Monitorable Parameters**
1	Define Team	Create a business continuity team with members in every part of Organization
2	Detailed Plan	Create a detailed plan along with recovery process and responsibilities
3	Effective Testing	Mock drill to be part of the plan
4	Crisis Communications	The plan should include a crisis communication list with alternate communication channel like phone email, address, etc.
5	Training	Providing of emergency response training for employees.
6	Continuous IT Operation	Please check that back-up mechanism exist as part of BCP for IT.
7	Change Management	Change management process should allow for the expedient implementation of emergency changes during an event, such as changing an access control list to provide rapid access for troubleshooting and analysis.

****