Bharat Electronics Ltd

Risk Management Framework

1.0 Risk Management Policy Statement

1.1 Bharat Electronics Limited (BEL) will strive continuously to identify, evaluate, prioritize and mitigate existing as well as potential risks related to the business of the Company.

2.0 Scope and Objectives of Risk Management

2.1 BEL is continuously exposed to risks considering the globalization of business environment and fast changing technology.

2.2 Risk Management (RM) objective is to facilitate a common understanding of risks at an early stage for effective mitigation to meet the Company's business goals.

2.3 The mitigation measures identified shall be embedded suitably into the business processes of the Company.

3.0 Areas for Risk Management Initiatives

3.1 BEL has identified the following major areas of risks related to:

- (i) Technology
- (ii) Market/Product
- (iii) Human Resources
- (iv) Finance
- (v) Enterprise
- (vi) Operations
- (vii) Impact of Govt Policy/Legislation/Laws
- (viii) Security
- (ix) Others

4.0 Methodology for Risk Management

4.1 The Company has plans to cover risks in various areas of its operations. The existing risks in various areas have been identified. Some of them are given in **Annexure I.** Notwithstanding this, new potential areas of risks will emerge. These 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.

4.2 Further, the mitigation measures already incorporated in various business processes may not be effective enough and more effective measures will have to be identified and implemented. The methodology for RM in the Company recognizes this dynamic nature of RM 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.

5.0 Risk Management Process

5.1 A brief methodology for RM is given in **Annexure II**. Formats given in **Annexure III** and **Annexure IV** are to be used to capture various aspects of RM.

5.2 The RM process description and flow charts are given in **Annexure V**. The format at **Annexure VI** is to be used for approval of RM proposals.

6.0 Organization for Risk Management

6.1 BEL has 9 Units located across the country. These Units have their respective core business areas, infrastructure and neighbourhood. These Units can address the entire process of identification of risks, implementation of risk mitigation measures etc. However, in addition to the Unit-specific risks there will always be some risks which affect the Company as a whole, and these need to be addressed in a centralized manner at the Corporate level. In view of this, the methodology given below will be followed for the two categories of RM initiatives:

- Centralised RM initiatives
- Unit-specific RM initiatives

6.2 The organization structure for RM is given in **Annexure VII.**

7.0 Corporate Risk Management Committee

7.1 The role of RM Committee at Corporate Office will be to:

(i) Identify and update areas of risks covering the Company as a whole.
(ii) Assess the current status of RM in the Company.
(iii) Recommend mitigation measures for the identified risks.
(iv) Recommend the implementation of these measures.
(v) Evaluate the effectiveness of these measures.
(vi) Review RM status every quarter.
(vii) Report to MCM on the status of RM every 6 months.
(viii) Update the policy framework and RM structure.

7.2 Chairman of this Corporate Risk Management Committee (CRMC) shall be an executive not below the rank of General Manager. The Management will from time to time nominate the other members of the CRMC drawn from all major functional areas like Technology, Strategic Planning, R&D, HR, Marketing and Finance. The Committee may co-opt members either from the Units or external experts for specific initiatives to have domain expertise during the deliberations.

8.0 Risk Management Committees at Units

8.1 Each Unit/ CRL shall have a Unit Risk Management Committee (URMC). The role of this Committee is to:

(i) Identify and update Unit-specific areas of risks.
(ii) Assess the current status of RM in the Unit.

(iii) Recommend mitigation measures for the identified risks.
(iv) Recommend the implementation of these measures.
(v) Evaluate the effectiveness of these measures.
(vi) Review RM status every quarter.
(vii) Report to CRMC on the status of RM every quarter.

8.2 The respective Unit/CRL Head shall be the Chairman of the URMC and he shall nominate the members of the URMC drawn from all major function areas like Production, R&D, HR, Marketing and Finance.

8.3 The URMC shall oversee the implementation, monitoring and reporting of the progress of the proposals to the Functional director.

9.0 **Approval of Risk Management Proposal**

9.1 The risk mitigation measures recommended by the CRMC shall be approved by the respective Functional Directors, i.e., for technology related risks by D(R&D), for market related risks by D(Mktg), for HR related risks by D(HR) and for finance related risks by D(F) etc.

9.2 If the RM proposal involves policy matters, the CRMC will put it up to the Management during the MCM.

9.3 The risk mitigation measures recommended by the URMC shall be approved by the respective Functional Directors, i.e., D(BC) for BG-Cx related risks and D(OU) for other Units related risks.

9.4 The fund requirements, if any, for the approved risk mitigation measures shall be met as per the existing financial delegation of powers in the Company.

10.0 **Risk Champions**

10.1 **Corporate Risk Champion**

10.1.1 Corporate Risk Champion (CRC) shall be an executive not below the rank of AGM, to be nominated by the Management. The functions of CRC shall be to:

(i) Obtain approval for identified risk mitigation measures from the respective Functional Directors.
(ii) Co-ordinate with the Process Owner(s) for the effective implementation of the approved risk mitigation measures.
(iii) Seek clarification from CRMC/Management wherever deemed necessary.
(iv) Give periodical reports to CRMC/Management/Govt.

10.1.2 The CRC shall be the Member Secretary of the CRMC.

10.2 Risk Champions at Units

10.2.1 Depending on the size and operations of the Unit, the Unit Risk Champion (URC) shall be an executive at the level of AGM, to be nominated by the respective Unit Heads. The functions of URCs shall be to:

- (i) Obtain approval for identified risk mitigation measures from the respective Functional Directors.
- (ii) Co-ordinate with the Process Owner(s) for the effective implementation of the approved risk mitigation measures.
- (iii) Seek clarification from URMC/Unit Head wherever deemed necessary.
- (iv) Give periodical reports to CRC.

10.2.2 The URC shall be the Member Secretary of the URMC.

11.0 Review of Risk Management Initiatives/Programs

11.1 By the Unit Risk Management Committee

11.1.1 The URMC will review the progress of the RM initiatives/programs on a quarterly basis. The review would cover the time schedules, expenditure, extent of achievement of the objectives and sustainability status of the proposals. The URMC shall also review the feedback collected from the beneficiaries.

11.1.2 The committee shall submit a report (for quarters ending March, June, September and December) to the CRMC on these aspects. This report shall be sent by the URC to the CRC.

11.2 By the Corporate Risk Management Committee

11.2.1 The CRMC shall assess and review the progress of the RM initiatives/programs on a quarterly basis. Based on the reports received from the URCs/CRC, the CRMC shall report to the MCM on a half-yearly basis (in Dec for Apr-Sep period and June for Oct-Mar period).

11.2.2 The CRMC shall also review the continuation or otherwise of the ongoing centralized RM initiatives/programs, and identification and adoption of new centralized RM initiatives.

11.3 By the Board of Directors

11.3.1 The Board of Directors will review and monitor the status of Risk Management through the 'Risk Management Committee' constituted by the Board and entrusted with the following roles and responsibilities:

a) Examine the risks identified by CRMC
b) Assess the current status of Risk Management in the Company.
c) Monitor and Review the implementation and effectiveness of the risk mitigation measures in October every year.

d) Review the policy framework and Risk Management structure as and when required

12.0 Risk Management Reporting

12.1 The reporting of RM in the Company shall be as follows:

(i) Internal reporting on RM initiatives shall be done by the Units as per the format in **Annexure III** using parameters identified for measurement of effectiveness.
(ii) Only the CRC shall do the external reporting.
(iii) External reporting by the URMC, if required, shall be done in consultation with the CRC.
(iv) URC shall report to the CRC every quarter on the status of RM in the Unit.
(v) CRMC shall report to the Board level committee appointed by the Board of Directors, in October every year. CRMC's report will first be placed before the Functional Directors in the MCM and the report duly approved in the MCM will be placed before the Board of Directors for review in January every year.

13.0 Implementation of Risk Management

13.1 RM System shall be integrated and aligned with the corporate and operational objectives and will be implemented by suitable interaction with employees/staff at all levels in the organization. RM shall be undertaken as a part of normal business practice and not as a separate task at set times.

Annexure I

Major Areas of Risks

Technology related risks

- In general, 'GSQR' based approach
- Wait for the customer's `preferences' before tying up source of technology
- Lag in technology w.r.t competitors
- DRDO `main stay' for technology
- Limited `long-term' tie ups with institutions for supply of technology
- Competitor's tying up with foreign suppliers for products traditionally held by BEL
- `Defence product' mind-set deeply ingrained – Resulting in non-competitive civilian product designs
- Technology obsolescence factor
- Gap in knowledge base (ToT, legacy systems and technological advancement)
- Hardware – Obsolescence management
- Software – Code decay, legacy systems, incremental change

Market/Product related risks

- Dependence on defence market and entry of private sector
- Civilian market/Export market – Product portfolio not comprehensive
- Limited use of market research approach – Especially for civilian products
- Existing marketing set up inadequate to handle the civilian product
- Shrinking global market for defence products leading to foreign party's direct marketing in India
- Defence Procurement Procedure of the Govt – Enabling increased participation by private and global players
- Business development' activity is limited
- Project Management tools not widely used

HR related risks

- Attrition of trained manpower
- Lack of strong competency mapping practices (available skills vs. needs)
- Quality of manpower input – Difficulty in attracting and retaining the bright candidates
- Limited `lateral' induction at middle/senior management levels
- Lack of `specialists' (Ph.D, ME, M.Tech etc) – Generally not welcome – Belief in `in-house/on-the-job training'

Finance related risks

- Surplus funds not put into business
- Foreign exchange rate variation

Enterprise related risks

- IPR related issues
- Claims against Directors/Officers
- Legal compliances
- Pressures on margins

Operations related risks

Impact of Govt policy/legislation/laws

Security related risks

Other risks

- Risk arising from unutilized lands
- Risk of carrying inventory

Annexure II

Methodology for Risk Management

1.0 Introduction

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

1.2 Following strategies will be used to manage a potential risk:

- Risk avoidance: Not performing an activity that carries risk.
- Risk reduction: Reduction of severity of loss.
- Risk retention: Acceptance of loss when it happens.
- Risk transfer: Causing other party to accept the risk.

1.3 The following steps will be followed for the RM process:

- Risk assessment: (i) Risk identification (ii) Risk description (iii) Risk estimation (iv) Risk evaluation
- Risk reporting: Threats and opportunities associated with risk identified.
- Decision: Whether to take up the risk treatment or not, keeping in view the impact and associated costs for risk mitigation measures.
- 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.
- Residual risk reporting: Mechanism of residual risk reporting after risk mitigation measures are implemented.
- Monitoring and review: Monitoring of the risk implementation measures and review with respect to parameters identified for effectiveness of these measures.

2.0 Risk Assessment

2.1 Risk Identification

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

Table 1 – Example of Key Drivers or Factors for Risks

Type of Risk	Due to Internal Drivers	Due to External Drivers	Due to both Internal & External Drivers
Operational Risks	- Accounting Controls - Information Systems	- Regulations - Culture	- Recruitment - Supply Chain

Strategic Risks	- R&D - Intellectual Capital	- Competition - Customer changes - Industry changes - Customer Demand - Technology changes	- M&A Integration
Financial Risks	- Liquidity - Cash Flow	- Interest Rates - Foreign Exchange - Credit	
Hazard Risks or Compliance Risks	- Employees - Properties - Products and Services	- Contracts - Natural Events - Suppliers - Environment	

2.1.2 The identification of the risk category, i.e., Operational, Strategic, Financial and Hazard helps in RM.

2.1.3 The following methods can be adopted for risk identification:

- Inputs from operating managers
- Brainstorming
- SWOT analysis
- Experts' inputs
- Scenario thinking

2.1.4 While identifying the risk, following may be considered:

- What is wrong or what are the shortcomings?
- What can go wrong?
- 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 given at **Annexure III** will be used for this purpose.

2.3 Risk Estimation

2.3.1 This can be quantitative, semi-quantitative or qualitative in terms of occurrence and possible consequences. This risk estimation can also be captured in format at **Annexure IV.**

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. With this, a 3 x 3 matrix as given in **Annexure IV** may be used to estimate the risk. This estimation can be used to prioritise the risks in conjunction with the cost and efforts associated with the risk treatment.

3.0 Potential for Improvements

3.1 Once risk evaluation is done and it is decided to go for improvements, then, Part C of **Annexure III** points are required to be addressed. The strategy and policy development is to be taken up by the function related to the risk area.

4.0 Strategy and Policy Deployment

4.1 Once strategy and policy for risk treatment is developed and accepted, the same is required to be deployed. Part D of **Annexure III** addresses actions and inputs to be generated.

5.0 Monitoring and Review

5.1 As part of strategy and policy deployment, the process owner should periodically present parameters for risk effectiveness measurement, failures and success. Management should review this.

Annexure III

Risk Description Format

Control No.:
Date:

Part A: Risk Identification

1. Name of the risk:

2. Scope of the risk (Note 1):

   (a) Qualitative description of the events:
   (b) Key drivers (Note 2):
   (c) Size of events (Note 3):
   (d) Dependant process/events (Note 4):

3. Process owner (Note 5):

4. Type/Nature of the risk (Note 6):

5. Qualification of the risk (Note 7):

   (a) Impact on organization:
   (b) Probability:

Part B: Current Status of Risk Management

6. Risk treatment and control mechanism (Note 8):

   (a) Primary means by which risk is presently managed (Note 9):
   (b) Process owner:
   (c) Adequacy of process and implementation structure:
   (d) Parameters for measuring the effectiveness (Note 10):
   (e) Levels of confidence in existing controls:
   (f) Adequacy of controls and monitoring (Note 11):

Part C: Potential for Improvements

7. Brief description for improvements:

8. Potential threats and opportunities:

9. Actions for improvements:

10. Strategy and policy development:

Part D: Strategy and Policy Deployment

11. Primary means of risk management:

12. Process owner:

13. Parameters for measuring effectiveness:

14. Objectives for risk mitigation:

15. Description of risk mitigation measures embedded into relevant processes:

16. Implementation structure:

17. Funds requirements:

18. Monitoring and review mechanisms:

Prepared by:	Provided by:
Name:	Name:
Designation:	Designation:
Location Address:	Location Address:

Notes

Part A: Risk identification captures the risk details for new risks as well as already identified risks. Some of the details may change with time due to internal and external factors.

Part B: Current status of Risk Management (RM) is basically review of the risk treatment and controls earlier identified.

Part C: Potential for improvements is applicable for already identified risks or newly identified risks

Part D: Covers the strategy and policy deployment for newly identified risks or revised strategy and policy deployment for already identified risks for increased effectiveness.

Part A

1. Against "Scope of Risk" mention whether the risk is confined to the Unit or may have company-wide significance.

2. Key drivers – What are the factors that are driving the risk? Internal or external factors may be indicated.

3. Size of events – What is the magnitude of the risk? How frequently is it occurring or the number of times the risk has occurred? This criterion is to get a feel about how big is the problem/risk.

4. Dependant process/events – What are the various processes that could be affected by the risk? What is the primary risk and what are the resultant risks?

5. Process owner – There can be multiple process owners. Please mention the basic process owner and the co-process owners/sub-process owners.

6. Type of risk – Whether it is a strategic risk? Classify under one of the following category of risks: (a) Technology related (b) Market/Product related (c) HR related (d) Finance related (e) Enterprise related (including risk arising from unutilized lands) (f) Operations related (including risk of carrying inventory) (g) Impact of Govt policy/legislation/laws related (h) Security related (i) Others. Also mention the impact of the risk on the organization.

7. Qualification of risk – Is it a tangible or intangible risk? How likely is it to occur (probability)?

Part B

8. Risk treatment and control mechanism – How is the risk being treated currently?

9. Primary means by which risk is presently managed – What mitigation measures have been taken and what further measures are proposed to be taken?

10. Parameters of measuring effectiveness – See Chart below giving an example.

Risk	Strategy and actions	Parameters and objective
Liquidated Damages	- Adopt Project Management tool to monitor project progress/implementation. - Contract Review - Manage the customer	90% of all projects over 12 months to be on this basis.

11. Adequacy of controls and monitoring – See Table below continuing previous example.

Achievements	Effectiveness	Alarm/failure reports
Adopting Project Management tool helped in 20% of the contracts meeting LD parameters	In all high cost projects it was possible to avoid LD.	In 40% of other contracts LD was levied.

Annexure IV

Risk Estimation Format

Control No.:
Date:

1. Name of the risk:

2. Risk impact (Consequence):

3. Risk probability (Occurrence):

4. Overall risk factor (2x3):

5. Risk treatment:

Table 1 : Risk Estimation Matrix

Probability / Consequences	High (Probable)	Medium (Possible)	Low (Remote)
High	√	√	X
Medium	√	√	X
Low	X	X	X

Notes

1. All cases of `√' have to be fully evaluated and addressed.

2. Case of `X' can be acceptable risks. If the consequences of risks are very high, then these also have to be evaluated.

3. This matrix can be used to prioritise the risks for mitigation.

4. The consequences and probability assignment guidelines given in Table 2 and 3 may be used.

Table 2 : Consequences of Risk – Threats and Opportunities

High	- Financial impact on the organization is likely to exceed Rs 10 crores. - Significant impact on the organisation's strategy or operational activities. - Significant concern of stakeholder.

Medium	- Financial impact on the organization likely between Rs 1-10 crores. - Moderate impact on the organisation's strategy or operational activities. - Moderate stakeholder concern.
Low	- Financial impact on the organization likely to be less than Rs 1 crore. - Low impact on the organisation's strategy or operational activities. - Low stakeholder concern.

Table 3 : Probability of Occurrence – Threats

Estimation	Description	Indicators
High (Probable)	Likely to occur every year or more than 25% chance of occurrence	- Potential of occurring several times within the time period of 5 years. - Has occurred recently.
Medium (Possible)	Likely to occur in 5 years time period or less than 25% chance of occurrence	- Could occur more than once within the time period of 5 years. - Could be difficult to control due to external factors. - There is a history of occurrence.
Low (Remote)	Not likely to occur in 5 years time period or less than 2% chance of occurrence.	- Has not occurred in 5 years time period. - Unlikely to occur.

Annexure V

Risk Management Process Flow Chart

1.0 Unit-specific Risk Management Initiatives

1.1 The flow chart at **Figure 1** gives the process flow for Unit level risks.

1.2 Line Manager(s) in a department and division identify the risks and capture in format given in **Annexure III.** All these risks are consolidated at Unit level and the Process Owner (s) of the function does first level scrutiny where the risk is reported.

1.3 Risks are further evaluated by the Unit Risk Champion (URC) along with Process Owner(s) as per the methodology given in **Annexure II.** Risks are identified as Unit-specific or corporate level.

1.4 URC and Process Owner(s) review the format given by the Line Manager(s) in **Annexure III** and the updated format is given for review by Unit Risk Management Committee (URMC) and the format is again updated.

1.5 These formats along with the Risk Management (RM) proposal as given in **Annexure VI** are put up to the concerned Functional Director for approval. Once approved by the Functional Director, these RM proposals will be taken up for implementation.

1.6 Risks identified as Unit-specific will be the responsibility of the Process Owner(s), and the URC will support the Process Owner(s) in discharging his responsibility. Similarly, risks identified as corporate level will also be responsibility of the Process Owner(s) and the URC will support the Process Owner(s) in discharging his responsibility.

1.7 In certain case, the URMC may decide to constitute a Committee as Process Owner and this Committee will work with the URC.

1.8 Process Owner(s) and URC will collect periodic data, as decided. This will be presented to the URMC for quarterly review as per format in **Annexure III.**

1.9 Completed format after quarterly review will be forwarded to the Corporate Risk Champion (CRC) for further processing.

2.0 Corporate Level Risk Management Initiatives

2.1 The flow chart at **Figure 2** gives the process flow for corporate level risks.

2.2 Corporate level RM proposals may be received from the Units or from Process Owner(s) at Corporate Office and the CRC. Other Managers at Corporate Office can also initiate proposals. These will be consolidated by the CRC and will be reviewed by the Process Owner(s) and the CRC.

2.3 After the review, these proposals will be put up to the CRMC who would further review before putting up to the concerned Functional Director for approval along with RM proposal format given in **Annexure III.**

2.4 After approval of the Functional Director, these RM proposals will be taken up for implementation by the Process Owner(s) and CRC or Unit depending on the type of the risk, i.e., Unit-specific or corporate level.

Flow Chart of Risk Management Process
Unit Level

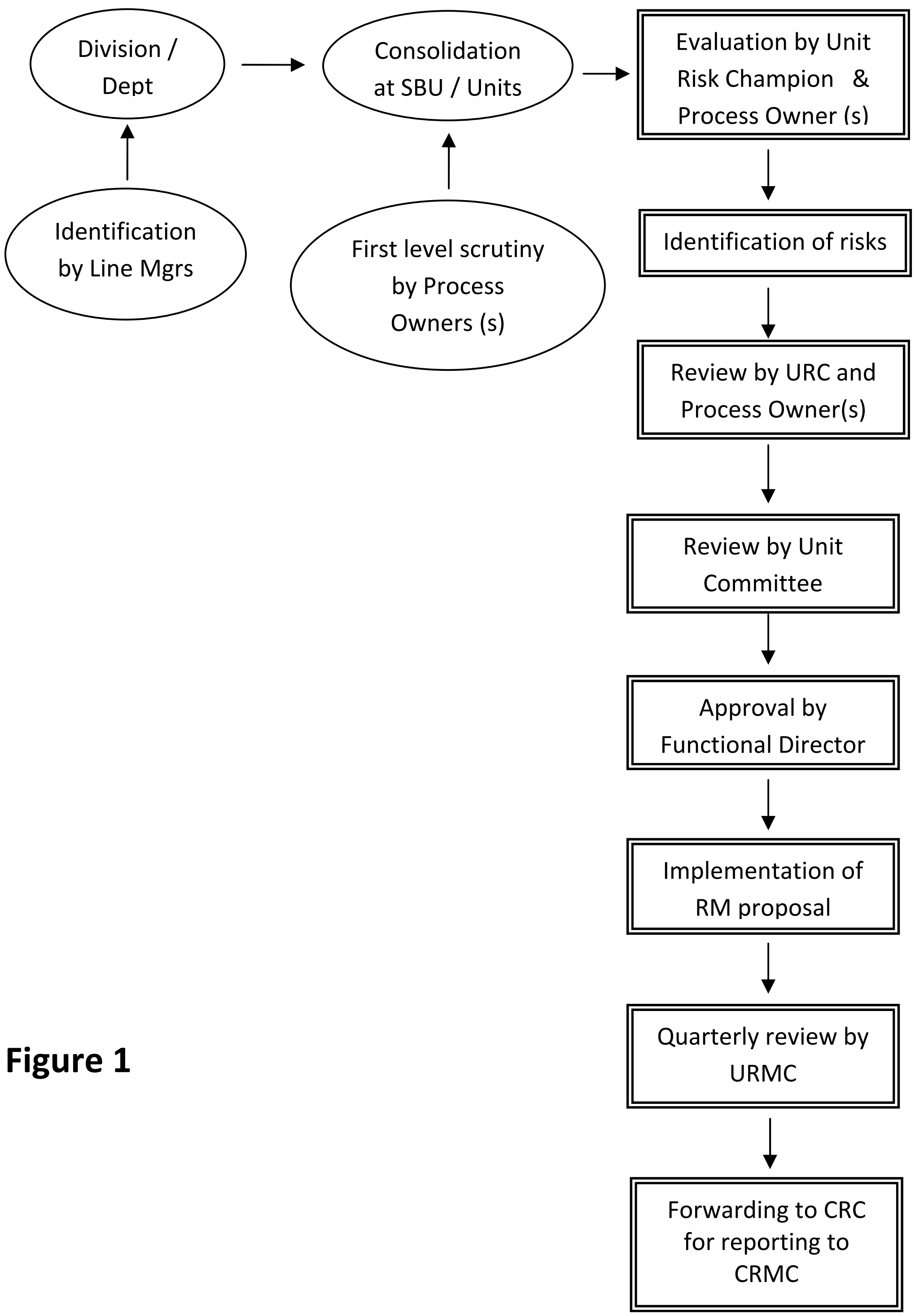

Figure 1

Flow Chart of Risk Management Process Corporate Level

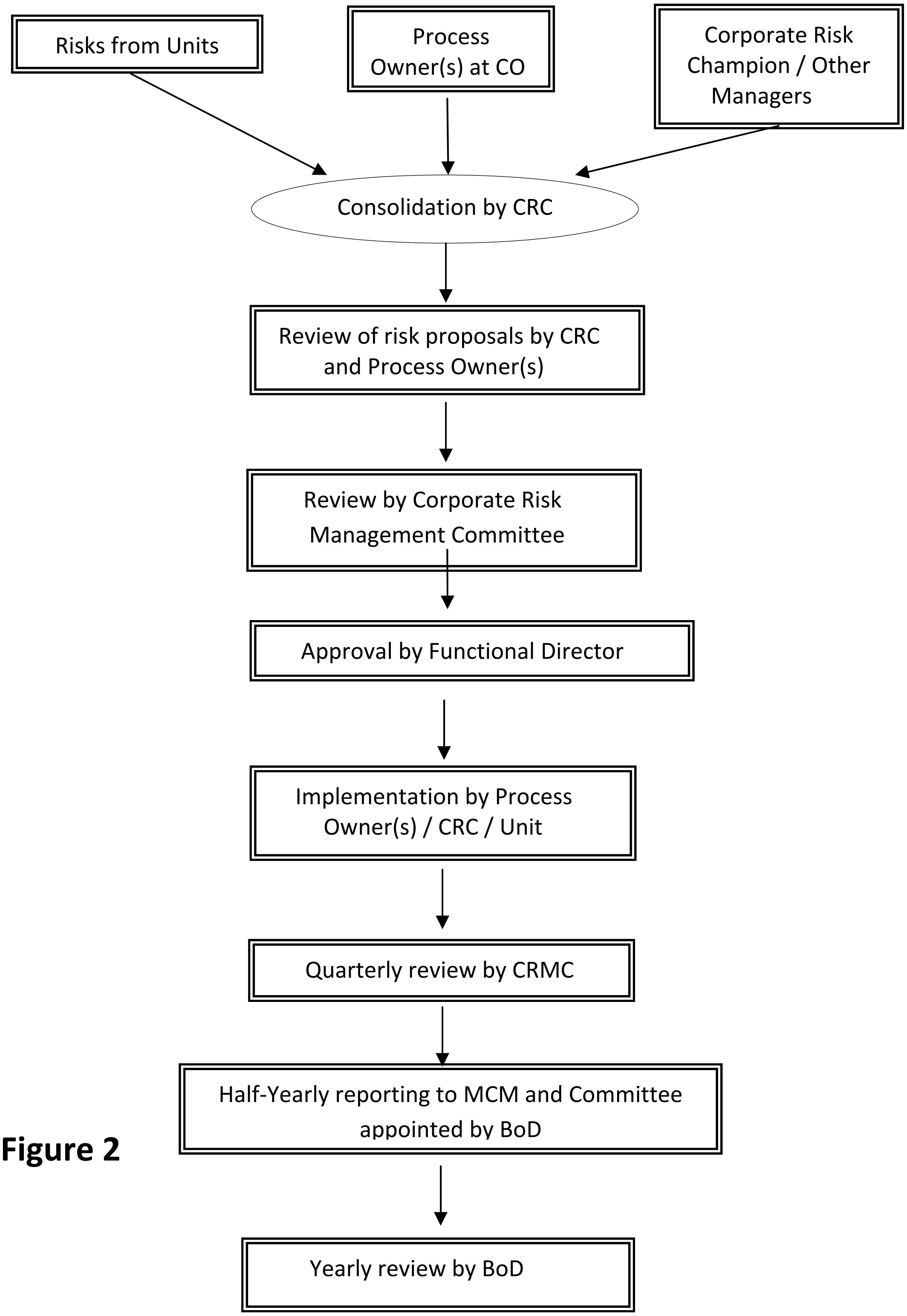

Figure 2

Annexure VI

Risk Management Proposal

1. Title of the proposed Risk Management proposal:

2. Name of Risk Champion:

3. Name of Process Owner:
   (Name, Designation, Location, Telephone No.)

4. Risk category: Unit-specific/Company level

5. Proposal objectives:

6. Type of risk: a) Newly identified/Already identified
   b) Strategic/Operational/Financial/Hazard/Compliance

7. Risk belongs to the functional area:

   (a) Technology related (b) Market/Product related, (c) HR related (d) Finance related
   (e) Enterprise related (including risk arising from unutilized lands)
   (f) Operations related (including risk of carrying inventory)
   (g) Impact of Govt policy/legislation/laws related
   (h)Security related, (i) Others

8. The following formats are to be enclosed mandatorily:

   (a) Risk Description Format as per Annexure II
   (b) Risk Estimation Format as per Annexure III

Risk Champion
Name:
Designation:
Location:

Date:

Unit Head/Functional Head
Name:
Location:

Date:

Annexure VII

Organisation Structure for Risk Management