Risk Management Policy

of

Advanced Weapons and Equipment India Limited
(A Government of India Enterprise)
Department of Defence Production,
Ministry of Defence

Originally framed	March 12, 2025
Current Revision Date	
Authority approving the Policy	Board of Directors

Table of Contents

1. Risk Management Policy Statement

We will continuously identify, assess, mitigate, and monitor the risks related to the company's operations. Our commitment is to strengthen the risk management system through continuous learning and improvement. We aim to minimize organizational risks to an acceptable level, while adopting risk management practices that align with the company's goals and objectives, ensuring effective risk reduction.

2. Scope of Policy

Risk management is an integral component of good corporate governance and it is inherent in any enterprise. Risk Management Policy helps organizations to put in place effective frameworks for taking informed decisions about risks. To minimize the adverse consequence of risks on business objectives, the Company has framed this Risk Management Policy. The guidance provides a route map for risk management, bringing together policy and guidance from Board of Directors.

Advanced Weapons and Equipment India Limited (AWEIL) desires to refine its organizational wide capabilities in risk management so as to ensure a consistent, efficient and effective assessment of risks in the achievement of the organization's objectives. It views risk management as integral to its objective of creating and maintaining business continuity, shareholder value and successful execution of its strategies.

The Company's risk management policy provides the framework to manage the risks associated with its activities. It is designed to identify, assess, monitor and manage risk.

3. Objective of the Risk Management Policy

The goal of this policy is to ensure sustainable business growth and stability while fostering a proactive approach to identifying, evaluating, reporting, and managing risks associated with the business. To achieve key business objectives, the policy outlines a structured and disciplined approach to Risk Management, addressing risk-related issues. The specific objectives of the Risk Management Policy are as follows:

3.1 To ensure the identification, assessment, quantification, proper mitigation, and management of all current and future risk exposures faced by the company.

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

3.3 To ensure that mitigation plans for key risk are agreed upon, assigned to risk owners and reviewed on a periodic basis.

3.4. To create an environment where all employees assume responsibility for managing the risk and risks are appropriately monitored through documentation and review and key treatment actions are reported on regular basis.

3.5 To avoid major surprises related to the overall risk and to protect & enhance stakeholders' value.

3.6 Ensuring sustainable business growth with stability and promoting a pro-active approach in reporting, evaluating and resolving risks associated with the business.

The Company strongly believes that Risk Management implementation should be in spirit and not only in form.

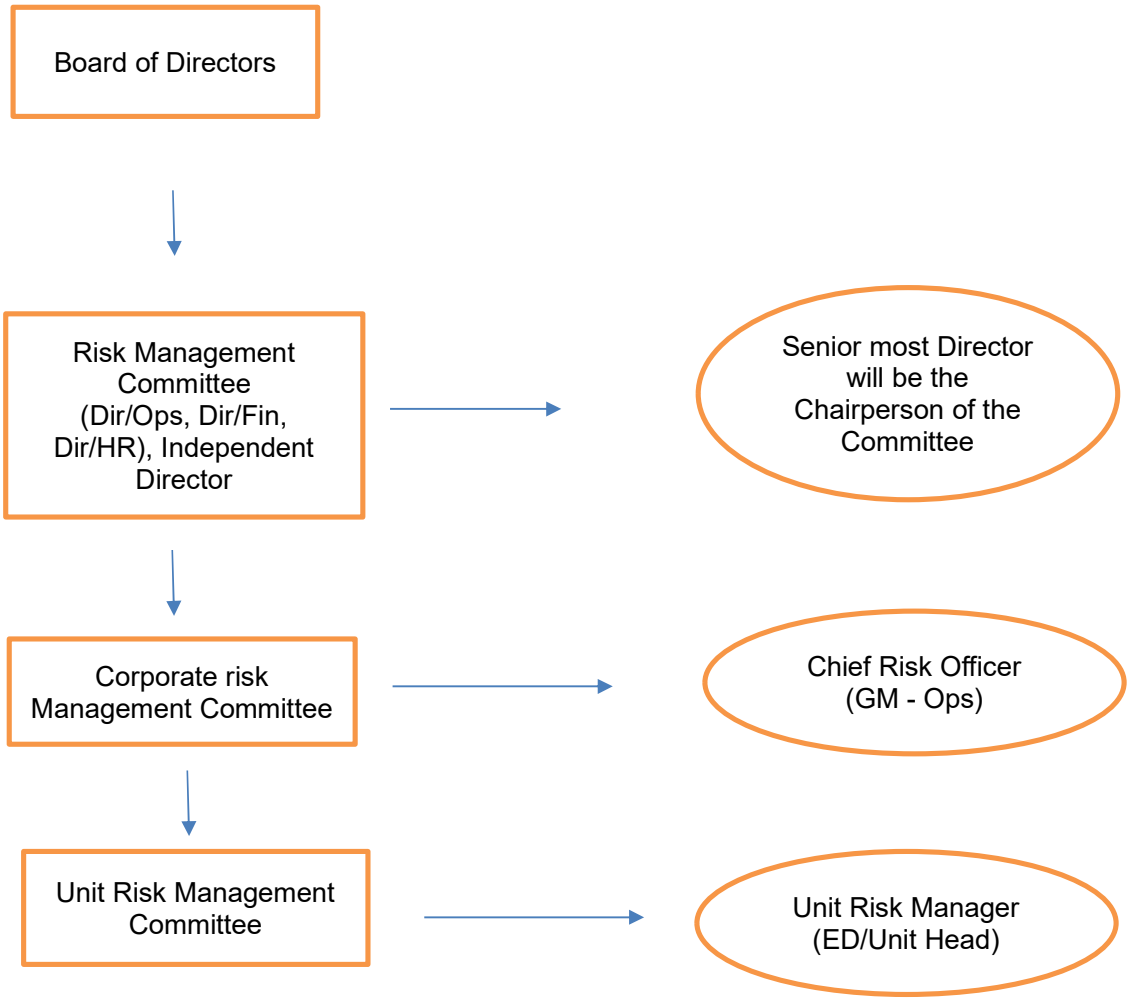
4. Risk Management Principles

Risk management is not a one-time event or exercise; rather, it is an ongoing process that involves a series of continuous actions integrated into the company's activities. It is not an end in itself but a crucial tool for building organizational resilience. The company's risk management principles are outlined as follows:

- All risk management activities will align with the company's corporate goals, objectives and priorities.
- Risk management will be proactive and well-reasoned, ensuring a dynamic, iterative and adaptable approach to change.
- It will be systematic and structured to address uncertainties and serve as an integral part of decision-making.
- Managers and staff at all levels will be responsible for identifying, evaluating, managing, and/or reporting risks, whether directly or indirectly.

5. Risk Management Governance Structure

The following diagram gives an overview of the risk management governance structure to be implemented in AWEIL;



The above is the implementation structure for Risk management across the Organization.

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.

6. Roles and Responsibility of Committees

6.1 Board of Directors:

- Approve and review the Risk Management Policy
- RMC would report to the Board about RM activities at least once in a year for its consideration and directives.

6.2 Risk Management Committee (RMC):

The RMC is the apex committee in the RM governance structure comprising of key decision makers within the organization. RMC is entrusted with the responsibility of implementing the risk management framework across the organization. RMC will apprise the Board of Directors about various risk management initiatives and ensure adequate reporting of the same to various stake holders on a regular basis.

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

  a. A framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, natural, sustainability, information, cyber security risks or any other risk as may be determined by the Committee.
  b. Measures for risk mitigation including systems and processes for internal control of identified risks.
  c. Business continuity plan.

- To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.

- To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.

- To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken.

- The committee to meet at least once in a year.

6.3 Corporate Risk Management Committee (CRMC)

The CRMC comprises of core management team of Corporate Department Heads Preferably General Managers looking after Operations, Finance, HR, BDU, Export, 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. The senior most member will be the Chairperson of the committee. They will:

- Implement and monitor the principles, actions and requirements of the risk management plan.
- Provide necessary tools and resources to identify, manage and mitigate risks.
- Review risks on half yearly basis- identification of new risks, changes to existing risks, updating risk register etc.
- Report the status of risk items to the Risk Management Committee.
- Appraise risk owners' actions taken to manage risk and correction of inappropriate performance.

- 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.
- Scope of work of corporate risk manager.

  a) He is the nodal officer for organization risk management activities.
  b) He is instrumental in integrating the activities of all the RM committees. i.e., RMC, CRMC and URMC.

- The committee to meet at least twice in a year in such a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.

6.4 Unit Risk Management Committee (URMC)

- 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 Executive Director (ED/Unit head) and he would be Unit Risk Manger (URM). Members of the URMC shall preferably be GM/ Jt. GM. Unit level committee meeting will be held quarterly.
- For all risks and opportunities **(Refer Annexure I),** URMC shall identify risk owners / risk coordinators.

6.4.1 Risk owners / Coordinators:

Department head [e.g. Finance Head, HR (Admin) Head, Production (Ops) etc.] will be the Risk owners/ Coordinators for their respective areas. They will play a key role in supporting the team in developing, maintaining and embedding the ri sk management framework within the Company. They will

- Identify any perceived risk at ground level in various processes.
- Ensure that implementation of recommendation and action plan approved by the Board, as per the policy, is done in spirit.
- Ongoing maintenance of risk framework and documentation including policies and procedures.
- Support and manage the risk workshop process.

7. Reporting of Risk Management

The reporting of Risk Management in the Company shall have three-line structure:

<u>First Line of Reporting</u>

The URMC shall prepare risk registers and share it with CRO on Quarterly Basis for discussion in CRC.

Second Line of Reporting

- The Chief Risk Officer along with the other members of the CRC shall review the risks on quarterly basis and decide upon the key risks which shall be reported to the Risk Management Committee.

- Based on CRC inputs for the mitigation plan, Risk Cell shall record it in the risk register and share the key risks with their mitigation plans to the CRO. CRO shall inform the concerned risk owner for the implementation of the mitigation plans.

- CRO shall consolidate the key risks based on the discussion of CRC which shall be reported to the Risk Management Committee on bi-annual basis.

Third Line of Reporting

- The Risk Management Committee along with Chief Risk Officer shall at least once a year review the key risks and respective mitigations decided by the CRC.

- Chairperson RMC shall annually apprise the Board on the key risks faced by the organization and the mitigation measures taken.

- Chief Risk Officer shall also apprise the RMC for decision on any new/ emerging risks faced by the organization in case of exigencies/ emergent conditions.

8. Risk Management Process

8.1 Risk Identification

Risk Identification is a process of identifying risks for assessment, evaluation and determination of appropriate mitigation plans. A systematic process of comprehensive risk identification is the foundation on which structure of risk management is built.

The company may use following tools & methodologies to identify new risks that may have emerged or risks that would have changed over a period of time:

• Structured workshops;

• Brainstorming sessions;

• Interviews by CRO and/ or the Risk coordinators;

• Review of loss event;

• Review of documents.

All identified risks shall be updated in a risk register **(refer Annexure II)**. Risk registers shall be quarterly reviewed and updated by the respective Risk Management Committees to ensure the relevance of the risks listed.

Risks that would have ceased shall also be closed appropriately. The CRO and Risk Coordinators shall ensure that the risk registers are reviewed and updated quarterly.

8.2 Risk Assessment

The risks shall be assessed on quantitative and qualitative two-fold criteria. The two components of risk assessment are:

a) The likelihood of occurrence of the risk event, and
b) The magnitude of impact if the risk event occurs

The risks shall be assessed according to the risk assessment criteria. The combination of likelihood of occurrence and the magnitude of impact provides the risk level. The magnitude of impact of an event (if it occurs), and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls.

In determining what constitutes a given level of risk the following scale is to be used for likelihood:

Levels	Descriptors
5	Very High Likelihood
4	High Likelihood
3	Moderate Likelihood
2	Low Likelihood
1	Very Low Likelihood

In determining what constitutes a given level of risk the following scale is to be used for impact:

Levels	Descriptors
5	Very High impact
4	High impact
3	Moderate impact
2	Low impact
1	Very low impact

8.3 Risk Evaluation

For each risk, the average score for likelihood and impact shall be multiplied to arrive at a combined score. In case the rating of risks is done by a group, average of the group's score shall be determined. The average is to be determined for each component of risk assessment viz., Likelihood and Impact. The simple average for each component of each risk shall be calculated. Example for Calculation of Group Score:

Rating of Risk X

	Likelihood (A)	**Impact (B)**
Participant 1	**2**	**5**
Participant 2	**3**	**5**
Participant 3	**4**	**5**
Total	**9**	**15**
Group Score	**3**	**5**
i.e. Simple Average (Total/ No. of Participants)		
Combined Score (Group Score A*Group Score B)	**15**	

9. Risk Assessment Criteria

The risk assessment criteria for Impact parameter inter-alia include the following:

Criteria	**Very Low (1)**	**Low (2)**	**Medium (3)**	**High (4)**	**Very High (5)**
Financial	Impact < 0.25% of Turnover	Impact within 0.25-1% of Turnover	Impact within 1-2% of Turnover	Impact within 2-3% of Turnover	Impact above 3% of Turnover
Reputation	Minimal local media attention • Short term recoverability of reputation • Minimal impact on ability to raise finance • No impact on AWEIL brand image	Regional media attention • Loss of reputation for a moderate period of time • Relatively small impact on ability to raise finance	Sustained negative regional media attention • Loss of reputation for a long period of time • Major impact on ability to raise finance • Major impact on	Negative national media attention • Loss of reputation for a moderate period of time • Significant impact on ability to raise finance • Significant	Sustained negative national media attention • Significant loss of reputation for a long period of time • Critical impact on ability to

		• Minor impact on AWEIL brand image	AWEIL brand image	impact And AWEIL brand image	raise finance • Severely impact The AWEIL brand image
Regulatory / Legal	Notice of violation/ warnings requiring administrative action and minimal penalties	Local level cases subject to fines or penalties • Subject to administrative action at within local jurisdiction	Routine state level cases subject to fines or penalties • Subject to regulatory proceedings and/or hearings at state level	Routine central or state cases subject to substantial fines or penalties • Subject to regulatory proceedings and/or hearings • Non compliance with MOU	Major central or state scrutiny, investigations subject to substantial fines and penalties including criminal charges and/or shut down of operations • Possible regulatory action • Non compliance with MOU

The risk assessment criteria for Likelihood parameter are defined as follows:

Criteria	**Very Low (1)**	**Low (2)**	**Medium (3)**	**High (4)**	**Very High (5)**
Occurrence	Event may occur in exceptional situations	Event may occur sometime	Event should occur sometime	Event will occur in most circumstances	Event is certain to occur in most circumstances
Likelihood/ Probability	Event could occur once in more than 5 years	Event likely to occur once in 3 to 5 years	Event expected to occur once in 3 years	Event may occur once in a year	Event certain to occur multiple times in a year

10. Risk Mitigation approaches:

Avoid: Avoid risks that involve a high probability impact for both financial loss and damage.

Transfer: Risks that may have a low probability for taking place but would have a large financial impact to be mitigated by being shared or transferred. e.g. by purchasing insurance or outsourcing. Insurance of assets, inventory etc. to cover the loss due to fire hazard, flood etc.

Accept: Risks, where the expenses involved in mitigating the risk is more than the cost of tolerating the risk should be accepted and carefully monitored.

Mitigate/ reduce: Risk mitigation, to be considered to address a perceived risk and regulate their exposure. Risk mitigation usually employs some risk acceptance and some risk avoidance.

11. Risk Review

Effective risk management necessitates a reporting and review framework to ensure that risks are properly identified, assessed and that suitable controls are established. Regular audits of policy and standards compliance will be conducted, and the performance of standards will be reviewed to pinpoint areas for improvement. It is important to recognize that AWEIL operates in a dynamic environment. Changes within the organization and its external environment must be identified, with necessary adjustments made to risk management practices. The monitoring process will ensure that adequate controls are in place to address the organization's risks.

The vertical/ functional teams will review the progress of actions taken to mitigate risks and assess the current risk levels, including:

- Determining whether the actions have been completed or are on track for completion.
- Reporting the status of the mitigation plan implementation to the Corporate Risk Committee.

Any monitoring and review process will also assess whether:

- The adopted measures have achieved the intended outcomes.
- The procedures and information used for the assessment were appropriate.
- The acceptability of each identified risk and its mitigation plan is evaluated and risks are ranked to identify key risks for the organization.
- Proposed actions to eliminate, reduce or manage each significant risk are considered and agreed upon.
- Responsibilities for managing key risks and implementing mitigation measures are assigned to the relevant department or regional heads.

12. Review of the Policy

The Chief Risk Officer (CRO) shall review the risk management policy whenever necessary, considering changes in the business environment, regulations, standards or industry best practices and put up to RMC.

13. Interpretation and Amendment

Where any doubt arises as to the interpretation of the said policy, it shall be referred to the Company Secretary. Further, any changes required in the policy due to change in the provisions of the Company Act, 2013, DPE/Govt. Guidelines, Statutory provisions or based on review by CRO etc. shall be incorporated in the policy with the approval of CMD.

Annexure I: Template for Risk Register

Risk ID No.	Risk Category	SBU/ Segment	Risk Statement	Likelihood Score	Impact Score	Overall Score	Risk Owner

Annexure II: Indicative Key Drivers or Factors for Risks

S. No.	Risk Class	Definitions
1.	Operational Risks	Risks associated with production planning, production scheduling, environmental & operational safety, inventory management. Also includes risks associated with inadequate or failed internal processes, people and systems, or from failure of infrastructure largely having to do with the performance, protection and utilization of existing assets.
2.	Financial Risks	Financial risks include risks associated with capital structuring, capital allocation, financial management, debtor's management, forex, hedging and preparation of financial statements.
3.	Human Resources Risk	Risks associated with culture, organizational structure, Employee retention, Talent retention, communication, recruitment, performance management, remuneration.
4.	Technological Risks	Risk associated with Selection of Technology, Development/ Acquisition of Technology, Deployment of technology, Technology obsolescence, Regulatory framework/ compliance etc.
5.	Product Risks	Risk associated with Quality, Reliability, Product diversification, Price Risk, Demand Risk, Customer experience Reputation, Time to Market (TTM).
6.	Market/ Sales Risks	Risks associated with developing, implementing, and managing new and existing products, customer service, pricing, marketing and feasibility of new business opportunities.
7.	Cyber security Risks	Risk associated with failure of IT system, unauthorized access, data loss, fraud, system outages, breach of confidentiality, legal/ regulatory violations, as well as data integrity.
8.	Enterprise Risks	Risk associated with R&D Investments, Asset utilization, Controls/ Procedures, Litigation/ Arbitration, Industry changes, Competition, Govt. policies.
9.	Environment, Health and Safety	This category includes risks related to environment pollution, safety of resources and employees' health, etc.
10.	Man-made/ Natural risk	Risk of loss of property due to fire, accident, flood, inundation, storm, earthquake etc.

This list may be modified in future to add/ modify new risk categories that may emerge.