Updated on July 19, 2024

Escorts Kubota Limited

Risk Management Policy

Version	Effective From	Approved By
2024 - 1.0	01-08-2024	BOARD OF DIRECTORS

Table of Contents

1. Introduction

Escorts Limited operates in the sectors of agri-machinery, construction and material handling equipment and railway equipment. Headquartered in Faridabad, Haryana, the Company was launched in 1944 and has marketing operations in more than 62 countries.

Escorts Agri Machinery division was launched in 1960. The Company manufactures tractors under the brand names of Farmtrac, Powertrac and Steeltrac. It has four manufacturing plants in Faridabad, Haryana, One in Rudrapur, Uttranchal and one subsidiary unit in Poland in the name of Farmtrac Europe.

The Escorts Knowledge Management Centre (KMC) was set up in 1976 and spread over 100,000 sq.m. area in Faridabad, Haryana. This centre designs the entire tractor – engine, transmission plus hydraulic systems and vehicle design consisting of sheet metal (including styling), controls and accessories.

The KMC has facilities such as engine laboratory featuring computerized test beds with online control, data acquisition and analysis, advanced vehicle testing laboratory, noise vibration and harshness lab, metrology lab, and materials engineering lab. The KMC uses 3D-modeling, analysis and simulation software for engines, transmissions and vehicles. Physical prototypes are then tested for performance, durability and reliability.

1.1 Preamble

Pursuant to the Corporate Governance provisions, it is the responsibility of the Board of Directors of the Company to review the risk assessment and minimization processes currently existing in the Company. Based on such review the Board is to make a mandatory disclosure of the risk assessment and minimization processes/ initiatives to the shareholders in the annual report of the Company.

To facilitate this review process the top management group and every function/ department of the Company will document the risk assessment and minimization processes existing at various levels.

1.2 Objective

Risk Management Policy (RMP) helps organizations to put in place effective frameworks for taking informed decisions about risk. The guidance provides a route map for risk management, bringing together policy and guidance from Board of Directors, Company's, Insurers etc. It outlines the framework which will help to achieve more robust risk management.

1.3 Importance of Risk Management

A certain amount of risk taking is inevitable if the organization is to achieve its objectives. Effective management of risk helps to manage innovation and improve performance by contributing to:

- Increased certainty and fewer surprises
- Better service delivery

- More effective management of change
- More efficient use of resources
- Better management at all levels through improved decision making
- Reduced waste and fraud, and better value for money
- Management of contingent and maintenance activities

The key areas to be addressed are:

- The requirements of **Corporate Governance** — these include more focused and open ways of managing risk. The need for a 'risk owner' at senior level, role for an activity (strategy, program or project) and the need for risk owners at everyday working levels as appropriate for the activity and risk exposure
- Consideration of the **organizational capability** to successfully achieve the required outcome
- The need for **improved reporting** and upward referral of major problems
- The need for **shared understanding** of risk and its management at all levels in the organization with partners and key stakeholders, combined with consistent treatment of risk across the organization

1.4 Regulatory Provisions:

A) Companies Act 2013 (Act)

i) Section 134 of the Act requires the Boards' Report to include a statement indicating development and implementation of a risk management policy for the Company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company;

ii) Section 177 (4) of the Act, Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include evaluation of internal financial controls and risk management systems;

iii) As per the Code of Conduct for Independent Directors enumerated under Schedule IV, the Independent Directors shall satisfy themselves on the integrity of financial information and that financial controls and the systems of risk management are robust and defensible

B) Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (SEBI LODR)

All Listed Companies are bound by the SEBI LODR. The RMP is also intended to address the requirements of SEBI LODR.

i) Regulation 21 read with Part D of Schedule II, inter alia, define the role and responsibility of Risk Management Committee.

ii) As per Regulation 4(2)(f)(7), Board to ensure that appropriate systems of control are in place, in particular, systems for risk management.

iii) As per Regulation 17(9)(b), Board shall be responsible for framing, implementing and monitoring the risk management plan.

iv) As per Part C of Schedule II, Audit Committee is to evaluate the internal financial controls and risk management systems

1.5 Key Definitions

Company: means Escorts Limited

Audit Committee: Committee of Board of Directors of the Company constituted under the provisions of the Companies Act, 2013 and the SEBI LODR.

Board of Directors / Board: As per Section 2 of the Companies Act, 2013. In relation to a Company, means the collective body of Directors of the Company.

RMP / Policy: Risk Management Policy

Risk*: Risk is an event which can prevent, hinder and fail to further or otherwise obstruct the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise's ability to maximize stakeholder value and to achieve its business objectives. Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the product of probability of occurrence of an event and the financial impact of such occurrence to an enterprise.

- Strategic Risk are associated with the primary long-term purpose, objectives and direction of the business.
- Operational Risks area associated with the on-going, day-to-day operations of the enterprise.
- Financial Risks are related specifically to the processes, techniques and instruments utilized to manage the finances of the enterprise, as well as those processes involved in sustaining effective financial relationships with customers and third parties.
- Knowledge Risks are associated with the management and protection of knowledge and information within the enterprise.

(* as defined in Standard of Internal Audit (SIA) 13 issued by the Institute of Internal Auditors)

Risk Components: Risks have three components:

- A **root cause**, which, if eliminated or corrected, would prevent a potential consequence from occurring,
- A **probability (or likelihood)** assessed at the present time of that root cause occurring, and
- The **consequence (or effect)** of that occurrence.

A root cause is the most basic reason for the presence of a risk. Accordingly, risks should be linked to root causes and their effects.

Risks can be classified into various types namely, internal and external, controllable and non-controllable, inherent and residual. Business risks are majorly classified in inherent and residual risks.

- **Inherent Risks:** The risk management process focuses on areas of high inherent risk, with these documented in the Risk Register. Recent performance in delivering a core service that is below expectations or does not meet agreed targets should be considered an indicator of high inherent risk.
- **Residual Risks:** Upon implementation of treatments there will still be a degree of residual (or remaining) risk, with the expectation that an unacceptable level of residual risk would remain only in exceptional circumstances.

Risk Appetite: Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value.

2. Risk Management Framework

2.1 COSO Framework (extract for reference)

COSO framework is the most widely accepted framework for risk management across the world.

COSO broadly defines enterprise risk management (ERM) as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

The COSO ERM framework is presented in the form of a three-dimensional matrix. The matrix includes four categories of objectives across the top – strategic/sectoral, operations/financial, reporting/ sustainability (particularly, ESG related risks) and compliance/information/Cyber Security Risk. There are eight components of enterprise risk management, which are further explained below. Finally, the entity, its divisions and business units are depicted as the third dimension of the matrix for applying the framework.

2.1.1 The Objective Dimension

The objective dimension of COSO framework divides the risks into four categories:

- **Strategic/Sectoral:** high-level goals, aligned with and supporting its mission
- **Operations/Financial**: effective and efficient use of its resources
- **Reporting/Sustainability (particularly, ESG related risks)**: reliability of reporting
- **Compliance/information/Cyber Security Risk**: compliance with applicable laws and regulations

2.1.2 The Framework Component Dimension

The Framework component dimension identify 8 elements of the risk management framework:

- **Internal Environment**: This component reflects an entity's enterprise risk management philosophy, risk appetite, board oversight, commitment to ethical values, competence and development of people, and assignment of authority and responsibility. It encompasses the "tone at the top" of the enterprise and influences the organization's governance process and the risk and control consciousness of its people.
- **Objective-Setting**: Management sets strategic objectives, which provide a context for operational, reporting and compliance objectives. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity, and are a precondition to event identification, risk assessment and risk response.
- **Event Identification**: Management identifies potential events that may positively or negatively affect an entity's ability to implement its strategy and achieve its objectives and performance goals. Potentially negative events represent risks that provide a context for assessing risk and alternative risk responses. Potentially positive events represent opportunities, which management channels back into the strategy and objective-setting processes.
- **Risk Assessment**: Management considers qualitative and quantitative methods to evaluate the likelihood and impact of potential events, individually or by category, which might affect the achievement of objectives over a given time horizon.
- **Risk Response (i.e. Risk Strategy)**: Management considers alternative risk response options and their effect on risk likelihood and impact as well as the resulting costs versus benefits, with the goal of reducing residual risk to desired risk tolerances. Risk response planning drives policy development. It is also known as the Risk Management Policy, management may adopt different risk management strategies based on risk assessment, namely,
  - Tolerate/Accept the Risk: This strategy is adopted when impact of risk is minor. In this case risk is accepted as cost of mitigating the risk can be high. However, these risks are reviewed periodically to check their impact remains low else appropriate controls are used.
  - Terminate: In this case the activity, technology or task which involves risks is not used/conducted to eliminate the associated risk.
  - Transfer: In this approach the associated risks are shared with the trading partners and vendors etc. e.g. outsourcing IT services to IT service Providers who have better capabilities to manage IT related risks. Insurance is another example of sharing risks.
  - Treat: In this case, organizations use appropriate controls to treat the risks e.g. using an antivirus software is a control for risks related to virus.
  - Turn Back: This strategy is adopted when impact of risk is expected to be very low or chances of occurring risk are minimum in such cases management decide to ignore the risk e.g. management may ignore risks due to flood in city like Gurgaon.
- **Control Activities**: Management implements policies and procedures throughout the organization, at all levels and in all functions, to help ensure that risk responses are properly executed.
- **Information and Communication:** The organization identifies, captures and communicates pertinent information from internal and external sources in a form and timeframe that enables personnel to carry out their responsibilities. Effective communication also flows down, across and up the organization. Reporting is vital to risk management and this component delivers it.

- **Monitoring:** Ongoing activities and/or separate evaluations assess both the presence and functioning of enterprise risk management components and the quality of their performance over time. The thought process underlying the above framework works in the following manner: For any given objective, such as operations, management must evaluate the eight components of ERM at the appropriate level, such as the entity or business unit level

2.2 Critical factors for management of risk

The key elements which will help the risk management process are:

- nominated senior management individuals' to support, own the risk management process and lead on risk management
- risk management policies, and the benefits of following them, clearly communicated to all concerned
- existence and adoption of a framework for management of risk that is transparent and repeatable
- existence of an organisational culture that supports well thought-through risk taking and innovation
- management of risk fully embedded in management processes and consistently applied
- management of risk closely linked to achievement of objectives
- risks associated with working with other organizations explicitly assessed and manage
- risks actively monitored and regularly reviewed on a constructive 'no-blame' basis
- allocating a risk allowance based on the risk assessment. These funds to be included in the financial provision. Unused funds for risk allowance to be redeployed when the activity completes or if the exposure to the related risk disappears

3. Escorts' Risk Management Policy

In order to fulfil the objectives of this policy and lay a strong foundation for the development of an integrated risk management framework, the policy outlines the following guiding principles of Risk Management:

3.1 Principles of Risk Management

a. All business decisions will be made with the prior information and acceptance of risk involved.

b. The Risk Management Policy shall provide for the enhancement and protection of business value from uncertainties and consequent losses

c. All employees of the Company shall be made aware of risks in their respective domains and their mitigation measures

d. The risk mitigation measures adopted by the Company shall be effective in the long- term and to the extent possible be embedded in the business processes of the Company

e. Risk tolerance levels will be regularly reviewed and decided upon depending on the change in Company's strategy

f. The occurrence, progress and status of all risks will be promptly reported and appropriate actions be taken thereof.

3.2 Risk Management Policy Statement

The policy statement is as given below:

- To ensure protection of shareholder value through the establishment of an integrated Risk Management Framework for identifying, assessing, mitigating, monitoring, evaluating and reporting of all risks
- To provide clear and strong basis for informed decision making at all levels of the organisation
- To continually strive towards strengthening the Risk Management System through continuous learning and improvement

3.3 Scope and extent of application

The policy guidelines are devised in the context of the future growth objectives, business profile envisaged and new business endeavors including new products and services that may be necessary to achieve these goals and the emerging global standards and best practices amongst comparable organizations. This policy is meant to ensure continuity of business and protection of interests of the investors and thus covers all the activities within the Company and events outside the Company which have a bearing on the Company's business. The policy shall operate in conjunction with other business and operating/administrative policies.

The specific objectives of the Risk Management Policy are:

- Ensure that Organisation's strategic business objectives are clearly defined and communicated to all the function/ department heads.

- Establish a frame work for the company's risk management process and to ensure company wise implementation.
- Clearly define functional, sectional and process ownership, thus clearly defining risk management responsibility;
- Develop a process for risk documentation and communication;
- Clearly defining the risk escalation protocols and responsibilities of various review and oversight bodies;
- Instigate reviews to assess the effectiveness of the risk management strategy;
- Report the risk assessment and minimization procedures to the Board Members; and

To ensure business growth with financial stability.

3.4 Access and changes to Risk Management policy

Risk management policy shall be accessible to all personnel in risk organization structure of the Company.

Any changes to this policy shall be approved by the board upon recommendation of Risk Management Committee.

- The Policy shall automatically stand modified to cover revision(s)/amendment(s) in accordance with applicable laws and regulations in force from time to time.

4. Risk Management

4.1 Risk Management Process

Risk management is a continuous process that is accomplished throughout the life cycle of a system. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction. Effective risk management depends on risk management planning; early identification and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, and coordination.

4.2 Key steps in Risk Management

Risk management is a shared responsibility. The risk management process model includes the following key activities, performed on a continuous basis:

- Risk Identification,
- Risk Assessment or estimation,
- Risk Analysis,
- Risk Treatment,
- Risk Mitigation, and
- Risk – Control and Monitoring

Figure 2: Risk Management Model

4.3 Key steps involved in the risk management process

4.3.1 Risk identification:

This involves continuous identification of events that may have negative consequences on the Company's ability to achieve goals. Key departments have been identified by the Company and their key activities have been selected for the purpose of risk assessment. Identification of risks, risk events and their relationship are defined on the basis of discussion with the risk owners and secondary analysis.

- To look at what is at risk and why
- To consider the opportunities opened up by the current activity (e.g. programme or project) as that may also clarify where risk lies
- To aim to identify the 20% of risks that would have 80% of the potential Impact
- To ensure that everyone involved has a sound understanding of the mission, aims and objectives and plans for delivery
- To check that there are realistic plans for how providers could deliver the outcomes sought from the activity; check that there is shared understanding of the risks, whilst recognising that customers' and providers' perspectives on risk will not be the same.

4.3.2 Risk Assessment (i.e. Risk estimation)

Risk assessment is the process of risk prioritization or profiling. Likelihood and Impact of risk events have been assessed for the purpose of analyzing the criticality. The potential Impact may include:

- Financial loss
- Non-compliance to regulations and applicable laws leading to imprisonment, fines, penalties etc.
- Loss of talent;
- Health, Safety and Environment related incidences;
- Business interruptions / closure
- Loss of values, ethics and reputation;

The likelihood of occurrence of risk is rated based on number of past incidences in the industry, previous year audit observations, future trends or research available.

Risk may be evaluated based on whether they are internal and external, controllable and non-controllable, inherent and residual.

4.3.3 Risk analysis

Risk Analysis is conducted using a risk matrix for likelihood and Impact, taking the existing controls into consideration. Risk events assessed as "high" or "very high" criticality may go into risk mitigation planning and implementation; low and medium critical risk may be tracked monitored on a watch list.

The Risk Reporting Matrix below is typically used to determine the level of risks identified. A risk reporting matrix is matched with specific likelihood ratings and Impact ratings to a risk grade of low (green), medium (yellow), high (amber) or very high (red).

RATING SCALE						
Probability (P) / Likelyhood factor		Impact (I)				
		Insignificant	Minor	Moderate	Major	Critical
		1	2	3	4	5
Almost Certain	5	L	M	H	C	C
Likely	4	L	M	H	C	C
Possible	3	L	M	M	H	H
Unlikely	2	L	L	M	M	M
Rare	1	L	L	L	L	L

Level of Inherent Risk	Desscription	Inherent Risk I * P
Critical	Immediate action required	Over 15
High	Corporate senior management attention is needed to develop and initiate action steps in near future	11 to 15
Moderate	Functional head attention is needed	6 to 10
Low	Managed by routine procedures	Less than 6

Figure 3: Risk Rating Matrix

4.3.4 Risk Treatment – Mitigation (Response to risk or Risk Strategy)

Based on the Risk Appetite/ Risk Tolerance level determined and reviewed from time to time, the Company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. The risk mitigation can be planned using the following key strategies:

- To terminate the activity
- To treat it by addressing the probability or impact and so contain it to an acceptable level.
- To **transfer** it to the party best placed to manage it (note that business and reputational risk cannot be transferred)
- To tolerate / accept the risk:

Risk Avoidance (Terminate the activity): By not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.

Risk Reduction (Treat): Employing methods/solutions that reduce the severity of the loss e.g., shotcrete being done for preventing landslide from occurring.

Risk Transfer: Mitigation by having another party to accept the risk, either partial or total, typically by contract or by hedging.

Risk Retention (Accept the risk): Accepting the loss when it occurs. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible.

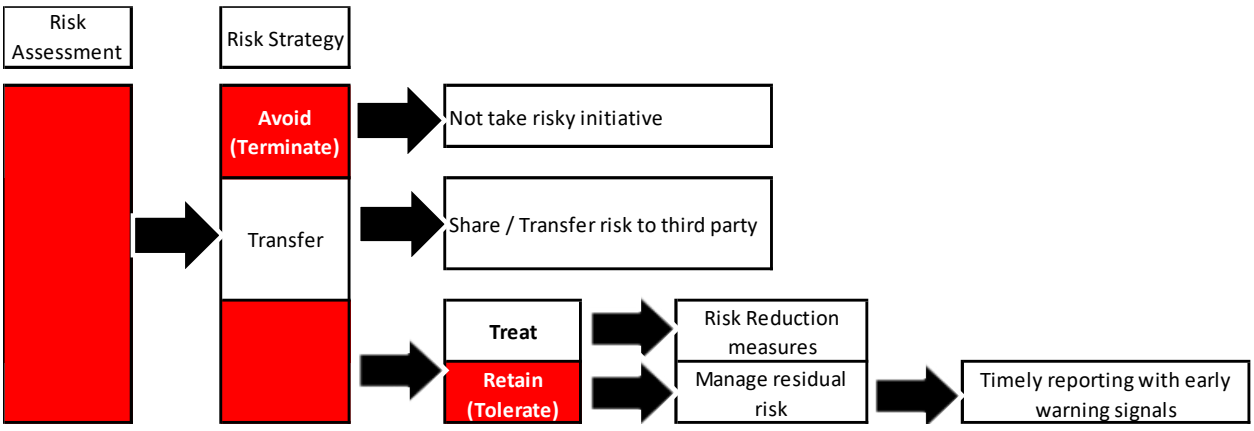


Figure 4: Mitigation of Risks – Typical Process Flow

4.3.5 Control and Monitoring Mechanism

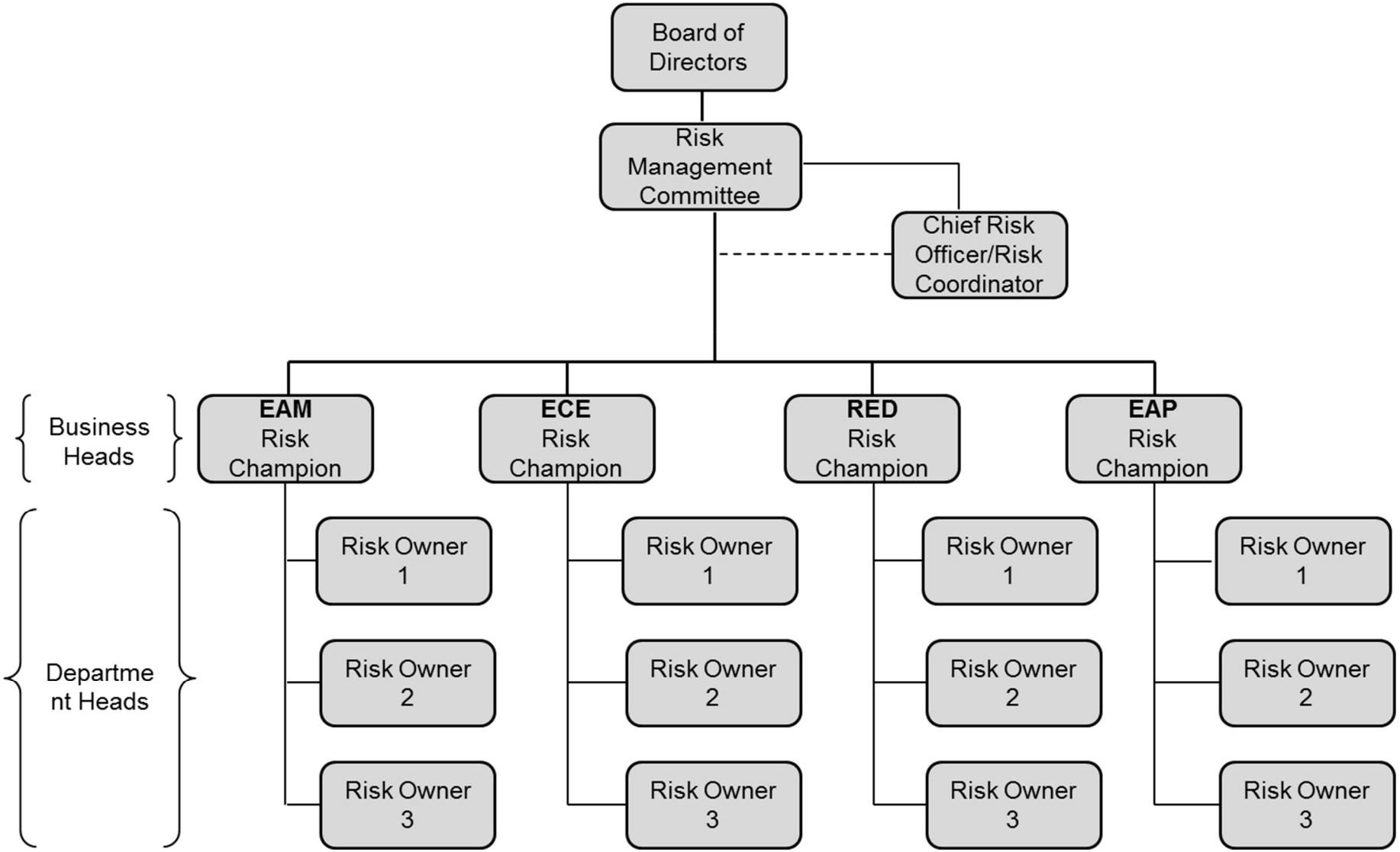
Risk management uses the output of a risk assessment and implements countermeasures to reduce the risks identified to an acceptable level. This policy provides a foundation for the development of an effective risk register, containing both the definitions and the guidance necessary for the process of assessing and mitigating risks identified within functions and associated processes.
In circumstances where the accepted risk of a particular course of action cannot be adequately mitigated, such risk shall form part of consolidated risk register along with the business justification and their status shall be continuously monitored and periodically presented to Risk Management Committee and Audit Committee.

4.3.6 Business Continuity Plan

Business entities are constantly vulnerable to a variety of threats that are caused by the various External and Internal factors which includes but not limited to financial, operational, sectoral, Strategic, Reporting, sustainability (particularly, ESG related risks), Compliance, information, cyber security risks or any other risk as may be determined by the Committee.
In order to protect the Continuity of the Company from all the potential risk, the Company should regularly have a track on the possible adverse outcomes, associated with such risks.

The Committee shall be apprised regularly under Enterprise Risk Management (ERM) with the Key risks and mitigation plans for such risk in order to track and monitor the risk related to Business Continuity Plan.

5. Risk Organisation structure



5.1 Risk Management Committee:

Risk Management committee shall be constituted by the Company as per the requirement of the Companies Act and the role and responsibility of Risk Management Committee shall be :

a) To formulate a detailed Risk Management Policy which shall include:
   I. A framework for identification of internal and external risks specifically faced by Escorts Limited, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.
   II. Measures for risk mitigation including systems and processes for internal control of identified risks.
   III. Business continuity plan.
b) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.
c) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
d) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity.
e) To keep the Board of Directors informed about the nature and content of its discussions, recommendations and actions to be taken;
f) Review the appointment, removal and terms of remuneration of the Chief Risk Officer (if any).
g) To ensure that the Risk Management policy is being followed and is effectively contributing to early identification of risks and proper mitigation process. Risk Champions shall be accountable to the Risk Management Committee for effective implementation of the policy;
h) To ensure the cyber security.
i) Coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board of Directors

The Risk Management Committee shall be apex body to approve the risks, its mitigation plan and the future course of action in this regard. While discharging the above mentioned roles and responsibilities, the Committee can seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

5.1.1 Risk Champions (RC)

- CEOs of respective business unit / division shall act as Risk Champions of Risk Management Committee.
- The Risk Champions will report its findings/observations/suggestions to the Risk Management Committee for review and/or for approval through Chief Risk Officer / Risk Coordinator.
- Risk Champions will review and approve the risk identified by Risk owners and present the same to Risk Management Committee for approval.

- RC will monitor and evaluate the mitigation plan for the risks identified in the risk register and place it for review of Risk Management Committee in the meeting.
- RC will chair the quarterly meetings of Risk Owners of the respective division.

5.1.2 Chief Risk Officer / Risk Coordinator (CRO)

- Head of the Legal and Secretarial Department of the Company will act as a Chief Risk Officer.
- Chief Risk Officer will coordinate among members of Risk Management Organisation and ensures that members of Risk Management Organisation will meet at least twice in a year.
- Chief Risk Officer / Risk Coordinator shall coordinate with Risk Champions and Risk Management Committee to circulate agenda for the meeting.
- To devise and carryout independent self-review to ensure compliance with the risk management policy.

5.1.3 Risk Owner

- All department heads of the respective divisions of Company will act as the Risk Owners of the risks related to his/her area.
- The Risk Owner will be responsible for mitigation of risk of their respective areas.
- Risk Owner shall present the new risks identified along with proposed mitigation plan to Risk Champions.
- Risk Owners would define such numbers of Risk facilitators as thinks appropriate to facilitate and support them in risk management exercise.
- Risk Champions will act as Risk Owners of different strategic risks which are not covered under the scope of various Departmental Heads.
- Risk Owner will have responsibility of identifying future risk, evaluate the criticality of the risk and formulate the steps of mitigation.
- Risk Owners will put up all the new risks identified and mitigation plan to Risk Champions for their approval on quarterly basis.
- In case of any serious risk identified, the same will be put up to Risk Champions immediately, i.e. within 24 hours.
- Quarterly meeting will be conducted by the risk owners which will be chaired by the Risk Champions.
- Minutes of the meetings will be prepared, signed by Risk Champions and will be sent to Chief Risk Officer / Risk Coordinator for records.

5.1.4 Risk Facilitators

- The Risk owners will appoint appropriate number of Risk Champions amongst officials working under him/her.
- Risk Facilitators will meet at least once in three months for deliberation to identify risks and Risk Owners will participate in the meetings of respective departments.
- The findings of these meetings shall be consolidated and reviewed in the quarterly meetings with Risk Champions.
- Minutes of the meetings will be prepared, signed by Risk Owners and will be sent to Chief Risk Officer / Risk Coordinator for records.

Periodic workshops will be conducted to ensure awareness of the policy and the benefits of following them. This will ensure that risk management is fully embedded in management processes and consistently applied. Senior management involvement will ensure active review and monitoring of risks on a constructive 'no-blame' basis.

6. Risk Reporting

6.1 Identification of new and emerging risks / review of existing risks

6.1.1 Risks to be reported to Audit Committee / Board of Directors

While the Company will be monitoring, evaluating and responding to risks. Only significant risks (or those that could become significant) need to be reported to the Audit Committee and Board of Directors.

Significant risks include those risks that have a high likelihood or significant impact (i.e. having risk exposure 11 or more) or where there is limited ability for mitigation by the Company. These risks are identified and assessed based on the Company's expertise, judgement and knowledge.

Risks with high risk score or exposure rating will be identified and summarized in Consolidated Risk Register.

Chief Risk Officer / Risk Coordinator will place Consolidated Risk Register to the Audit Committee and Board of Directors post discussion and approval by Risk Management Committee.

6.1.2 Process of risk reporting

The Risk Identification Form (RIF) will be used to highlight emerging risks or add new risks to the risk register throughout the year. On an ongoing basis, when a new or emerging risk is identified, Risk owners of respective department will notify to Risk Champions by completing the RIF and submitting it to designated mail id of Chief Risk Officer for discussion and inclusion in the Risk Registers and discussion in Risk Management Committee.

After submission of RIF, the form will be assigned a unique number which will be communicated back to the Risk Owners via acknowledgement of receipt. The same will be forwarded to Risk Champions for evaluation. The risks identified shall also be discussed in the monthly MANCOM meetings.

After review of the RIF and any further clarifications from Risk Owners, Risk Champions will determine whether the risk contained in this report warrants inclusion in the risk register.

Where risks are included in risk register, the Risk Management Committee would have visibility of the new risk information in the half yearly meetings provided that on a continuous basis not more two hundred and ten days shall elapse between any two consecutive meetings.

6.2 Risk reporting of adverse event

All adverse events and near misses must be recorded in Event Recording Register.

The adverse event reporting form (Risk alert Form) should be completed as soon as possible after the event, within one working day, unless there are exceptional reasons for delay, for example the event was identified retrospectively following a complaint or claim. All adverse events, as may be decided as significant by 2 risk owners, should be reported, even if some time has passed since the event occurred. The final decision of an adverse event to be reportable or not lies with the overall risk coordinator.

It is imperative that person(s) reporting the adverse event reports the fact. There is no place for any opinion or assumptions. It is important that details are accurate and factual for any future review.

Risk owners will present the adverse event reporting form to the Risk Champions and Chief Risk Officer immediately.

Following will be the reporting mechanism:

- **To Risk Management Committee:** The adverse events as may be jointly decided by Risk Champions in consultation with Chief Risk Officer as significant.
- **To Audit Committee / Board Level:** Adverse events with high risk impact rating 4-5.

7. Documentation

- Each Risk Owner shall maintain the Risk Register of their department.
- All key risks identified shall be documented in the Consolidated Risk Register maintained by Chief Risk Officer.
- Risk Identification Form should be prepared for any new risk identified to be placed to Risk Management Committee for approval.
- Minutes of all Risk Management Committee should be documented and maintained with Chief Risk Officer/Risk Coordination.