HONDA INDIA POWER PRODUCTS LIMITED

RISK MANAGEMENT POLICY

Version	Effective from
Rev-03	February 13, 2026
Rev-02	January 05, 2024
Rev-01	August 01, 2017
Rev-00	July 20, 2016

Table of Contents

Chapter-1.	**Introduction**	4	
Article-1	Objective		4
Article-2	Importance of Risk Management		4
Article-3	Requirement as per Companies Act, 2013		5
Article-4	Requirement of Clause 49 of the Listing Agreement		5
Article-5	Key Definitions		5
Article-6	Access and changes to Risk Management policy		6
Chapter-2.	**Risk Management Framework**	7	
Article-7	Three line of defense		7
Article-8	COSO Guidelines (extract for reference)		8
	Article-8.1 : The Objective Dimension		8
	Article-8.2 : The Framework Component Dimension		9
Article-9	Critical factors for management of risk		10
Article-10	Minimum requirement of Risk management framework		10
Chapter-3.	**Risk Management**	12	
Article-11	Risk Management Process		12
Article-12	Key steps in Risk Management		12
Article-13	Key steps involved in the risk management process		13
	Article-13.1 : Risk identification		13
	Article-13.2 : Risk Assessment		13
	Article-13.3 : Risk analysis		13
	Article-13.4 : Risk Treatment – Mitigation (Response to risk)		14
	Article-13.5 : Control and Monitoring Mechanism		15
Chapter-4.	**Risk Organisation structure**	16	
Article-14	Risk Management Organisation:		17
	Article-14.1 : Risk Management Officer (RMO)		17
	Article-14.2 : Risk Response Committee		17
	Article-14.3 : Sub Risk Management Officer		17
	Article-14.4 : Overall Risk Management Coordinator		17
	Article-14.5 : Risk Owner		18
	Article-14.6 : Risk Champions		18

Table of Contents

Chapter-5. Risk Reporting 18

Article-15 Identification of new and emerging risks / review of existing risks 18

Article-15.1 : Risks to be reported to Audit Committee 18

Article-15.2 : Process of risk reporting 19

Article 16 Reporting of adverse event/crisis 19

Article-16.1 : Keeping records of Activities related to the crisis 19

Article 17 Response when crisis occurs 20

Article-17.1 : Reporting channels 20

Article-17.2 : Crisis level, Reporting Criteria 20

Article 18 Measures to be taken after the crisis Subsidises 21

Article 18.1 : Reports on Measures & others to prevent Reoccurrence 21

Article 18.1 : Implementation of Measures & others to prevent Reoccurrence 21

Chapter-6. Guidelines on Risk management 22

Chapter-7. Documentation 27

Chapter-8. Appendices 28

8.1 Impact Rating

8.2 Likelihood Rating

8.3 Risk Register Template

8.4 Key Risks

8.5 Risk Identification Form

8.6 Following details will be captured

8.7 Risk Alert Form

Chapter-1: Introduction

Honda India Power Products Limited (HIPP), is a subsidiary of Honda Motor Co. Japan and was incorporated on September 19, 1985. Ever since, it has been the undisputed leader in the power products industry, manufacturing and marketing a range of Portable Generators, Water Pumps and General Purpose Engine at its state-of-art manufacturing facilities at Greater Noida. It is also engaged in the marketing of Lawnmower, Brush Cutter, Long tailed outboard motors and Power Tiller.

HIPP has 15 Area Offices across India and over 600 dealers and have been continuously bringing joy and satisfaction through its range of power products that suit the requirements of a variety of customers segments in agriculture, domestic and commercial.

Every product manufactured is the result of persistence in quality, giving it the cutting edge for that extra reliability. It was in recognition of this that HIPP became the first power products manufacturing company in India to have been awarded the ISO 9001:2000 Certification for its Quality Assurance Systems & ISO 14001 for its Environment Management systems.

While maintaining its leadership in the domestic generator market and export to over 35 countries, HIPP, is making active efforts in developing new applications for its General-Purpose Engines (GPE). HIPP enjoys majority of market share of Generators and Water pumps. The business of GPE and Water Pump sets is expected to contribute significantly to the company's future growth plans.

Article-1: Objective

Risk management Policy 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.

Article-2: 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 fewersurprises 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
- Innovation
- 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, programme 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
- Managing project risk in the wider context of **programmes of change and the business**

The key risk of the Company are identified, assessed, measured, appropriately mitigated, minimized and managed i.e. to ensure adequate systems for risk management.

Article-3: Requirement as per Companies Act, 2013

Responsibility of the Board: As per Section 134 (n) of the Act, The board of directors' report must include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the Company.

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

Responsibility of the Independent Directors: As per Schedule IV [Part II-(4)] of the Act, Independent directors should satisfy themselves that financial controls and the systems of risk management are robust and defensible.

Article-4: Requirement of Listing Obligations

Responsibility of the Audit Committee: The role of the audit committee shall include the reviewing the company's financial and risk management system.

Article-5 : Key Definitions

Company: Means Honda India Power Products Limited

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

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. As per the Industry standards, 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.

1

- Crisis : A crisis refers to the situation where a risk manifests and has a serious impact on the management of the business.
- Ordinary Times : The period when a crisis has not yet occurred.
- When a crisis occurs : The period once a crisis has occurred and countermeasures are taken to prevent further damage and loss and to respond to the crisis.
- When a crisis subsides : The period after a crisis has subsided as a result of countermeasures to prevent the continued damage and loss and after the response to the crisis is mostly complete.

Article-6: Access and changes to Risk Management policy

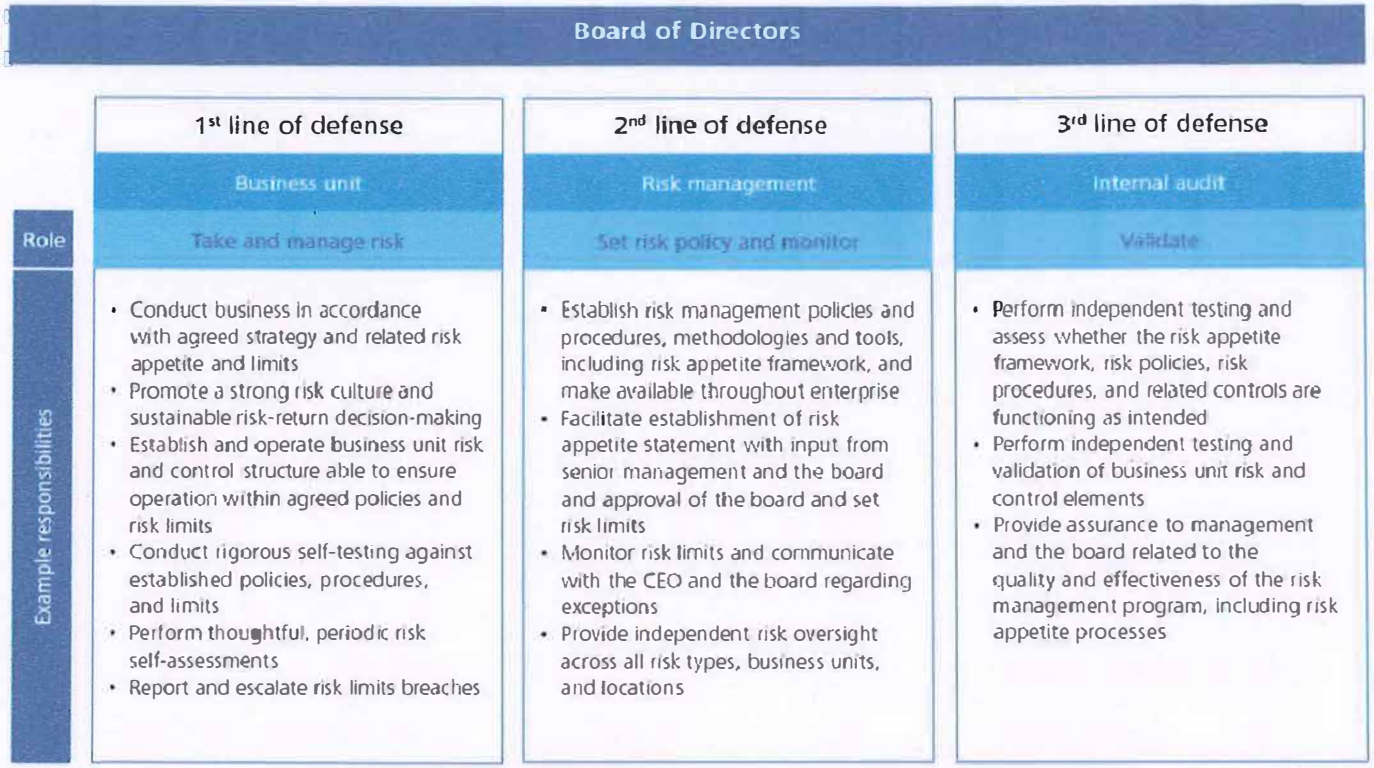
Risk management policy shall accessible to all personnel in risk organization structure of the Company.

Periodic review of Risk Management Policy will be performed and any changes in the policy will be initiated by overall risk coordinators. Any changes to this policy shall be assessed by Risk Management organisation with an intimation to the Audit Committee, which shall finally be approved by the Board of Directors.

Chapter-2. Risk Management Framework

Article 7: Three line of defense

The three lines of defense framework and example risk appetite framework activities



Source: Deloitte Analysis. Copyright © 2014 Deloitte Development LLC.

Article 8: COSO Guidelines (extract for reference)

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, operations, reporting and compliance. 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. As outlined by COSO, the framework provides eight components for use when evaluating ERM:

Article 8.1 The Objective Dimension

This enterprise risk management framework is still geared to achieving an entity's objectives; however, the framework now includes four categories:

- Strategic: high-level goals, aligned with and supporting its mission
- Operations: effective and efficient use of its resources
- Reporting: reliability of reporting
- Compliance: compliance with applicable laws and regulations

Article 8.2: The Framework Component Dimension

- **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**: 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.
- **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.
- **Education and Training : HIPP to** provide education and training to improve the ability of associates to recognize risks and respond to crisis.
- **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

Article-9 : Critical factors for management of risk

The key elements that need to be in place include:

- 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
- **Release of Information to Stakeholders:-The reports on the risk management activities of HIPP are prepared so that information can be disclosed to stakeholders at all times, to ensure transparency, and that the appropriate responses are provided by stakeholders.**
- 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.

Appropriate use of business continuity plans and contingency plans is an important element of the management of risk. So there are likely to be success criteria identified with regard to:

- Building in 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
- Existence of continuity plans which consider how the business will survive should the outcome not be achieved (this would include looking at if a service should fail to come on stream at the required time, or if the users refuse to make use of the service).

Joint working and partnerships often involve more complex types of risk that can adversely affect the delivery of business services. For example, if part of the service provided by one organisation is delayed or of poor quality, the success of the whole collaboration can be put at risk. You must make sure that your organisation knows about the risk management approaches of your partners. Sharing information about risk management means that risks in collaborative programmes can be identified and managed in a proactive way.

Article-10: Minimum requirement of Risk management framework

The minimum requirements for a risk management framework are:

- Existence of the organisation's risk policy
- Clear identification of main stakeholders
- Clarification of the main approaches to be used to identify; assess and report on risks; as well as look at actions to deal with risks
- Clear assignment of responsibilities for managing risk and reporting to senior management, especially risks which cut across core business activities and organisational boundaries
- Clear audit trail of decisions to ensure that risk management reflects current good practice, with quality assurance of key decisions as input to audit.

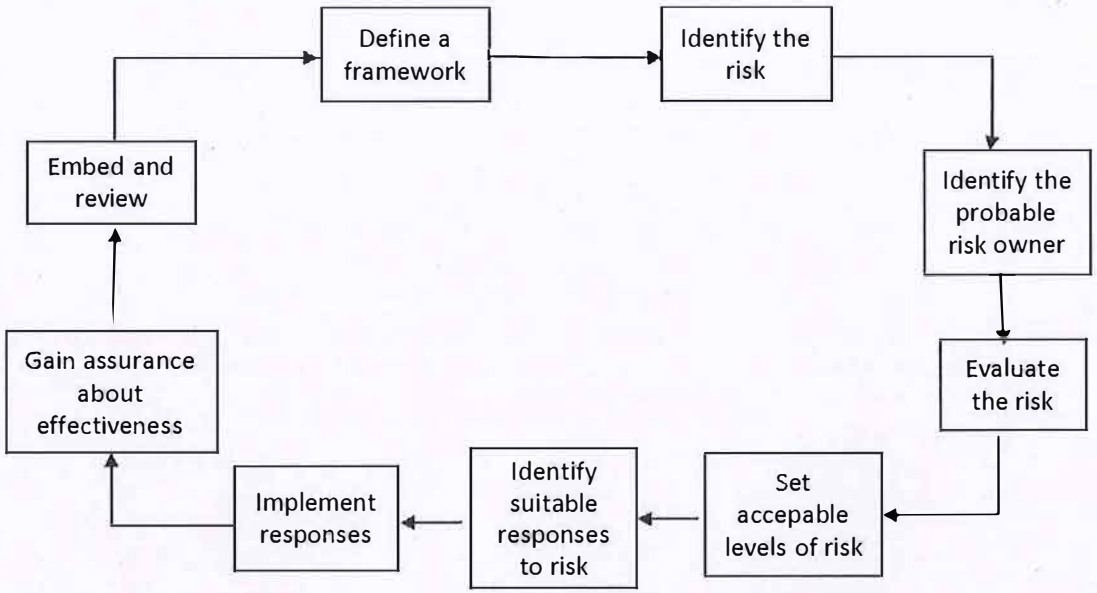


Figure 1: Strategic framework for the management of risk

A framework for management of risk sets the context, in which risks will be identified, analysed, controlled, monitored and reviewed. It will be consistent with processes that are embedded in everyday management and operational practices. It will address:

- Identification ofRisks
- Information about their probability and potential impact
- Quantification of risk
- Options to deal with them
- Decisions on risk management , such as further risk reduction
- implementation of Decision
- Subsequent tracking and managingrisks
- Evaluation of actions for their effectiveness
- Setting up and support of appropriate communication mechanisms
- To engage stakeholders throughout the process.

Chapter-3 Risk Management

Article-11: 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.

Article-12: 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,
- Risk Analysis,
- Risk Treatment,
- Risk Mitigation, and
- Risk – Control and Monitoring

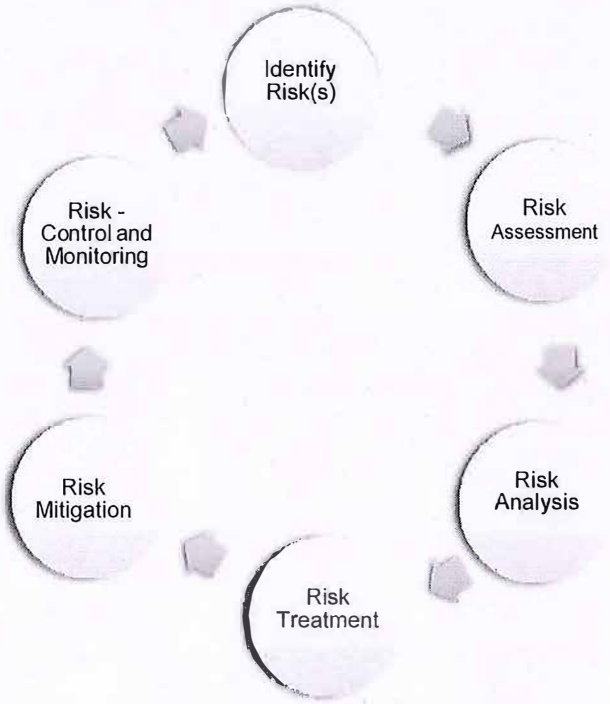


Figure 2: Risk Management Model

Article-13: Key steps involved in the risk management process

Article-13.1 : Risk identification:

This involves continuous identification of events that may have negative consequences on the Company's ability to achieve goals. Nine 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.

Article-13.2 : Risk Assessment

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;

For risk appetite card refer to Appendix 8.1.

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. For detailed likelihood ratings refer to Appendix 8.2.

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

Article-13.3 : 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).

Consequence	Likelihood				
	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost certain
5 Very High					
4 High					
3 Medium					
2 Low					
1 Insignificant					

Risk Score = Business Impact x Likelihood	
more than 15	Very High
9 to 15	High
4 to 8	Medium
3 or less	Low

Figure 3: Risk Rating Matrix

Article-13.4 : Risk Treatment – Mitigation (Response to risk)

Risk mitigation options are considered in determining the suitable risk treatment strategy. For the risk mitigation steps, the cost benefit analysis needs to be evaluated. Action plans supporting the strategy are recorded in a risk register along with the timelines for implementation. Risk mitigation options include:

- 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:

To put in place processes that will actively encourage cooperation and open dialogue between customers and providers. To ensure that providers share information about problems at the earliest opportunity so that small issues do not escalate.

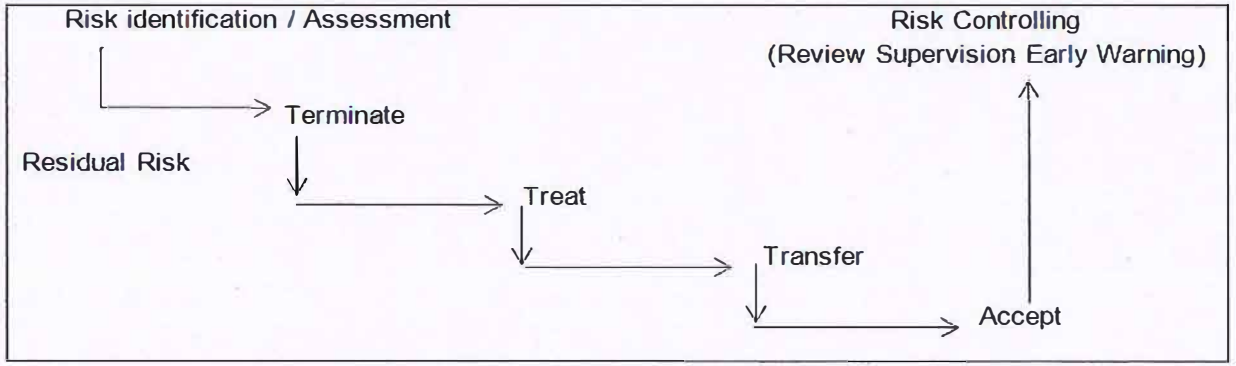


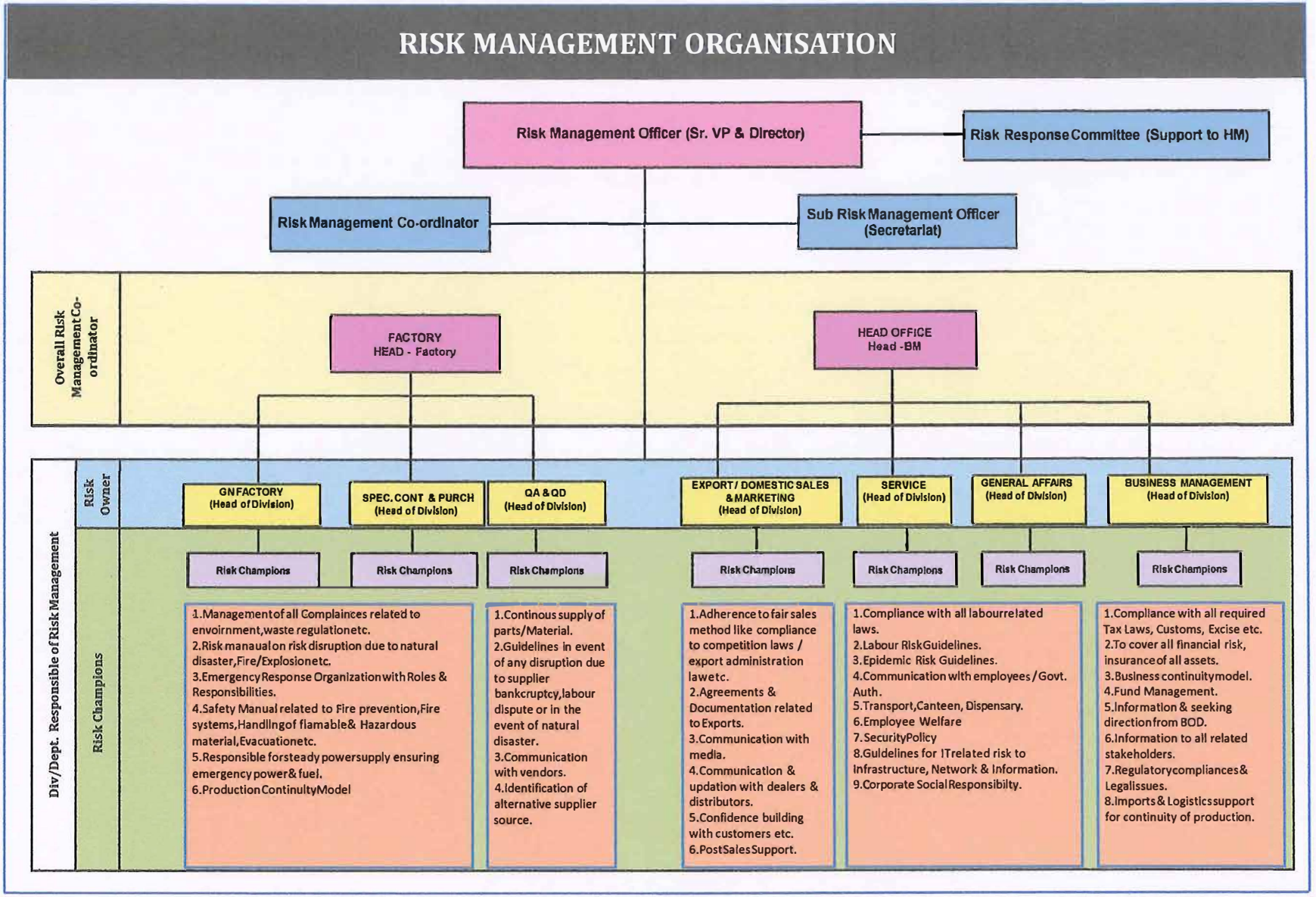
Figure 4: Mitigation of Risks – Typical Process Flow

Article-13.5 : 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.

1 Chapter-4 . Risk Organisation structure



*Roles and responsibilities at departmental level is an illustrative list.

Article-14 : Risk Management Organisation:

Risk Management organisation shall be constituted by the Company with the approval of Audit Committee in line with ASH guidelines/ HM guidelines and shall be responsible for ensuring that the Risk Management policy is being followed and is effectively contributing to early identification of risks and proper mitigation process.

Risk Management Officer shall be accountable to the Audit Committee for effective implementation of the policy.

Article-14.1 : Risk Management Officer (RMO)

- Executive Director (Other than President & CEO) shall act as Risk Management Officer of Risk Management Organiation.
- The Risk Management Officer shall be apex body to approve the risks, its mitigation plan and the future course of action in this regard.
- It will also direct Overall Risk Management Coordinators for any change in risk register and mitigating the risks identified.
- The Risk Management Officer would report its findings/observations/suggestions to the Board through Audit Committee for review and/or for approval.

Article-14.2 : Risk Response Committee

- Members of the Risk Response Committee will be defined and approved by Risk Management Officer (RMO).
- The Risk Response Committee will support to RMO.

Article-14.3 : Sub Risk Management Officer

- Head of the Factory of the Company will act as a Sub Risk ManagementOfficer.
- Sub Risk Management Officer will coordinate among members of Risk Management Organisation and ensures that members of Risk Management Organisations will meet at least twice in a year.
- Sub Risk Management Officer shall coordinate with Overall Risk Management Coordinator and Risk Owners to circulate agenda for the meeting.
- To devise and carryout independent self review to ensure compliance with the risk management policy.

Article-14.4 : Overall Risk Management Coordinator

- There will be Overall Risk Management Coordinators as approved by the RMO.
- Separate Overall Risk Management Coordinator will be appointed for Factory and Head Office respectively.
- Overall Risk Management Coordinator will review and approve the risk identified by Risk owners and present the same to Risk Management Officer for approval.
- Overall Risk Management Coordinator will monitor and evaluate the mitigation plan for the risks identified in the risk register and place it for review of Risk Management Officer in the meeting.
- Overall Risk Management Coordinator will chair the quarterly meetings of Risk Owners.

Article-14.5 : Risk Owner

- All divisional heads of the 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 Owners would define numbers of Risk Champions and coordinate with Overall Risk management officer.
- Overall Risk Management Coordinators 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 Overall Risk Management Coordinators for their approval on quarterly basis.
- In case of any serious risk identified, the same will be put up to Overall Risk Management Coordinators immediately, i.e. within 24 hours.
- Quarterly meeting will be conducted by the risk owners which will be chaired by the Overall Risk Management Coordinator.
- Minutes of the meetings will be prepared, signed by Overall Risk Management Coordinators and will be sent to Sub Risk Management Officer for records.

Article-14.6: Risk Champions

- The Risk Owners or Divisional Heads will appoint appropriate number of Risk Champions amongst officials working under him/her and head the Champions to evaluate the suggested risks based on their criticality.
- Risk Champions 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.
- Minutes of the meetings will be prepared, signed by risk owners and will be sent to Sub Risk Management Officer 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.

Chapter-5. Risk Reporting

Article-15 : Identification of new and emerging risks / review of existing risks

Article-15.1 : Risks to be reported to Audit Committee

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.

Significant risks include those risks that have a high likelihood or significant impact (i.e. having risk exposure 8 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.

Risk Management Officer will place Consolidated Risk Register to the Audit Committee and ASH.

Article-15.2 : 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 Sub Risk management Officer by completing the RIF and submitting it to designated mail id of Sub Risk Management Officer for discussion and inclusion in the Risk Registers.

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 Overall Risk Management Coordinators for evaluation. The risks identified shall also be discussed in the regular PDCA meetings.

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

Where risks are included in risk register, the RMO would have visibility of the new risk information in the half yearly meeting.

1 Article-16 : Reporting of adverse event/**Crisis**

All adverse event/**Crisis** or near miss must be recorded in Event Recording Register. Details will be captured as per format in Annexure 8.6.

The adverse event/**Crisis** 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/**Crisis** 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/**Crisis** reporting form to the Overall Risk Management Coordinator immediately.
For Risk Alert format refer Appendix 8.7

Following will be the reporting mechanism:

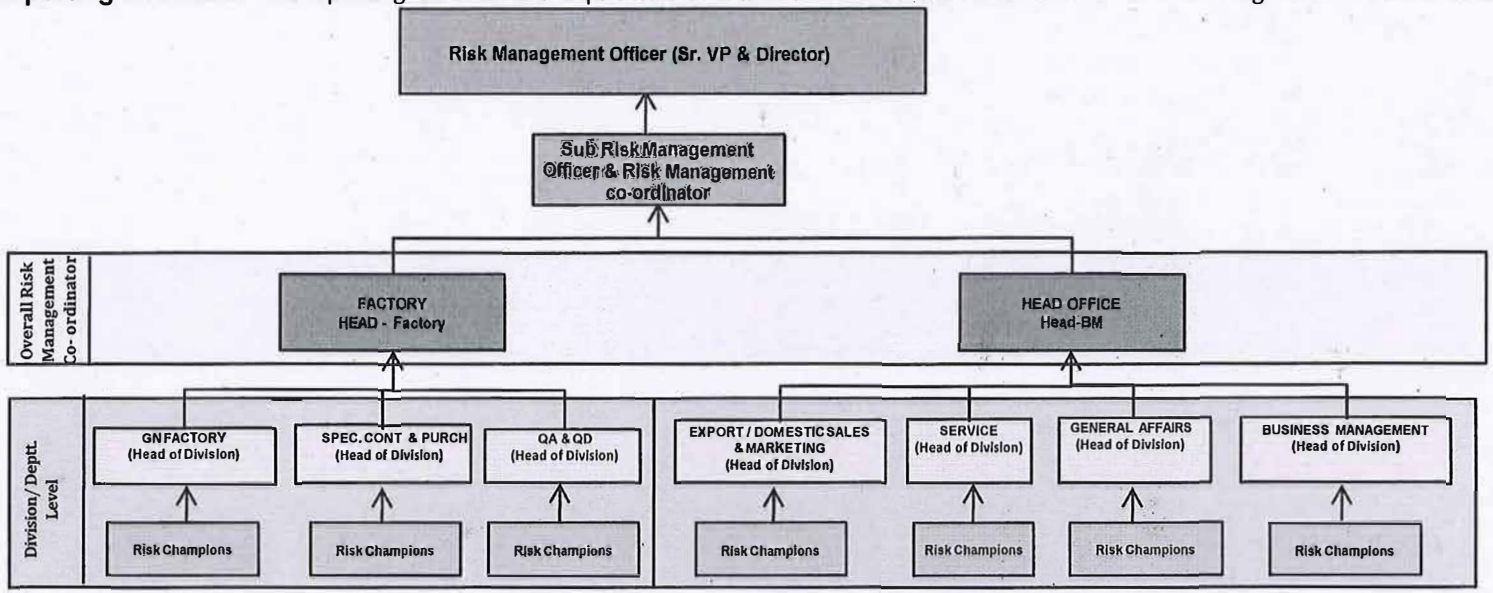
- **To Risk Management Officer:** The adverse events as may be jointly decided by two Risk owners (out of which one will be other department) as significant.
- **To Audit Committee / Board Level:** Adverse events with high risk impact rating 4-5.

1 Article-16.1 : Keeping Records of Activities Related to the Crisis

For the purpose of assessing the crisis response and examining reoccurrence prevention measures

1 Article-17 : Response When a Crisis Occurs

Article-17.1 : Reporting Channels- The reporting channels and implementation details when a crisis occurs or when there are signs of a crisis are as follows.



Article-17.2 : Crisis Level, Reporting Criteria- The reporting channels and implementation details when a crisis occurs or when there are signs of a crisis are as follows.

Crisis level		Need to report	Establish Emergency Headquarters		Response structure
			Global	HIPP	
Level A	The crisis affects other Genpos and the response provided in ordinary times cannot address the crisis.	Yes	◎	◎	• Global Emergency Headquarters takes the lead and responds while cooperating with the Emergency Headquarters established at HIPP. • HIPP which is effected by the crisis establish an Emergency Headquarters and respond according to a developed plan.
Level B	The crisis is limited to HIPP, but the response provided in ordinary times cannot address the crisis.	—	—	○	• HIPP shall take the initiative in implementing measures to deal with the crisis. • The Risk Management Officer of HIPP shall examine the establishment of an Emergency Headquarters.
Level C	The crisis can be addressed by the HIPP as in ordinary times.	—	—	—	• Responded to by HIPP in ordinary times.

Article-18 : Measures to be Taken After the Crisis Subsides

Article-18.1 : Reports on Measures and others to Prevent Reoccurrence

After the crisis subsides, the HIPP Risk Management Officer shall promptly analyze the cause of the crisis, and create a report on the crisis response, problem areas, and countermeasures to prevent reoccurrence, etc.
And shall be reported to the HM Risk Management Officer in coordination with the Risk Manager.

Article-18.2 : Implementation of Measures and others to Prevent Reoccurrence

HIPP Risk Management Officer shall immediately implement measures to prevent reoccurrence.

Chapter-6 : Guidelines on Risk management

Illustrative List of risk items

Risk Classification			No	Risk item
Internal /External Factor	Major Classification	Loss/ Corporate		
Internal Factor	Business Risk	Corporate	1	The effectiveness of philosophy and the vision is low
		Corporate	2	Risk by the company structure (organization, system, management efficiency)
		Loss	3	Injury / illness / death / scandal of the manager
		Loss	4	Disorder of the governance in the HONDA group
		Corporate	5	Brand power drop
		Loss	6	Legal action from stockholder, Activist/TOB etc
		Loss	7	Reputation Risk caused by Rumors.
		Corporate	8	Deficiency, lack of social activity and company mecenat
	Decision Making Risk	Corporate	9	Failure of M&A, Alliance, Joint venture
		Corporate	10	Failure of new business/Unable to create new business
		Corporate	11	Influence of the motor sports activity
		Corporate	12	Failure of Resource allocation, Business strategy
		Loss	13	Imperfect of the conference

	Strategy Risk	Corporate	14	Imperfect, lack of of the business strategy (sales network / price / advertising) /Correspondence delay to a competitor trend
		Corporate	15	Failure of the technological strategy (the product / product skill)
		Corporate	16	Failure of the production strategy (allocation, inside and outside product, facilities strategy)
		Corporate	17	Failure of the procurement strategy (local procurement, global procurement)
		Corporate	18	Failure of the IT strategy
		Corporate	19	Imperfect, lack of the public information strategy (information dispatch, media correspondence)
		Corporate	20	Lack of the quantity / quality of the talented person by the failure of the HR strategy (adoption, upbringing, assignment) of the HR strategy
		Corporate	21	Failure of the financing strategic (CF, insurance, financing)
		Corporate	22	Failure of the real estate strategy
	Study/Development Risk	Corporate	23	Delay / failure of the product / technology development
	Purchasing and Procurement Risk	Loss	24	Dependence on authorized business partner of the raw materials and parts
		Loss	25	Lack of the business partner's abillity (productive capacity, financing state)
	Production and Distribution Risk	Loss	26	The damage, trouble of facilities, the machine
		Loss	27	Fire / Explosion
		Loss	28	Supply chain troubles
		Loss	29	Shipment delay, Distributional trouble, The long-term stay stock
		Loss	30	Damage accident during transportation, safekeeping
		Loss	31	Imperfect of the import and export procedure

	Quality Risk	Loss	32	Product liability
		Loss	33	Product defect accident / Recall
		Loss	34	Inferior quality (specifications, production, others) / Voluntary recall
	Business/Sales/Service related Risk	Loss	35	Occurrence of the agglutination credit with the business partner
		Loss	36	Deficiency for customer
	Environmental Risk	Loss	37	Non-appropriate processing and disposal of the waste
		Loss	38	Release, leak of the pollutant (the atmosphere, the quality of the water, the soil)
		Loss	39	Energy saving, CO2 emission (aim in the company)
		Loss	40	Local damage by the noise, a bad smell, the vibration of the office
		Loss	41	Violation of Distribution E/M standard (NOx, PM, etc)
		Loss	42	Products in violation of environmental performance standards (fuel economy, emissions, noise)
		Loss	43	Products in violation of regulation standards for included chemical and toxic substances
	Intellectual Property Risk	Loss	44	Patent infringement
	Financial Risk	Loss	45	Deterioration of financing conditions and delayed payments
		Loss	46	Inadequate or wrongful actions in accounting, financial reporting, and tax matters
		Loss	47	Inadequate management or wrongful act regarding the projected benefit obligations and pension assets

	Information Risk	Loss	48	Information system and software program problems and breakdown
		Loss	49	Leakage of confidential information (model under development, business plan, technical information, customer data, financial information, etc.)
		Loss	50	Data erasure, falsification or theft by employee or due to other internal factors
	Legal Risk	Loss	51	Problems due to inadequate aspects of contract
		Loss	52	Violation of various laws and regulations related to business of Honda
		Loss	53	Risks of legal proceedings such as lawsuits
	Safety & Health Risk	Loss	54	Work accident, occupational disease, working environment
		Loss	55	Associate traffic accident (automobile, train, airplane, bicycle, etc.)
	HR Risk	Loss	56	Human rights issues, discrimination
		Loss	57	Labor dispute including strike, etc.
		Loss	58	Mental health issues, power harassment, sexual harassment
		Loss	59	Associate relations management, measures for dealing with labor unions
		Loss	60	Risk stemming from personnel treatment and performance appraisal
		Loss	61	Deterioration of in-house communication
		Loss	62	Decline in associate motivation and morale
	Internal Fraud	Loss	63	Misconduct by associates (driving under the influence, sexual offense, drug use, discrimination, slander, etc.)
		Loss	64	Accounts injustice by the employee individual (embezzlement, breach of trust, nonentry / dilution / imaginary ordering)
		Loss	65	Other injustice by the employee individual (bribery, insider trade, business with the anti-society power)
		Loss	66	Wrongdoing involving the whole organization

External Factor	Financial & Economic Risk	Loss	67	Exchange and interest rate fluctuations
		Corporate	68	Economic crisis and recession
	Disaster related Risk	Loss	69	Natural disaster (earthquake, tsunami, eruption, typhoon, tornado, flooding, lightning, hailstorm)
		Loss	70	Infectious diseases including new influenza strain, SARS, and tuberculosis, becoming prevalent
	Country Risk	Loss	71	Damage from radioactive leakage, environmental pollution, etc.
		Loss	72	Changes in local laws and regulations, institutions and business practices
		Loss	73	War, terrorism, political instability, security deterioration
		Loss	74	Change in political regime
	Industry Market Risk	Corporate	75	Rising material costs and decline in material supply volume
		Corporate	76	Rising fuel prices
		Corporate	77	Changes in consumer values and decline in demand
		Corporate	78	Intensifying competition with other companies
	Regulatory risk	Corporate	79	Changes in customs duties, import regulations or taxes
		Corporate	80	Tightening of environmental regulations
	Intellectual Property Risk	Corporate	81	Patent/Design right infringement
	Finance Business Specific Risk	Corporate	82	Residual value, capital cost, credit, and financing risks
	Business Partners Risk	Loss	83	Default, bad debt, and credit risks
		Loss	84	Wrongdoing at business partner
		Loss	85	Bankruptcy of correspondent financial institution
		Loss	86	Bankruptcy of supplier/dealer
	Infrastructure Risk	Loss	87	Roads cut off, suspension of public transportation services
		Loss	88	Supply of electricity, gas, or water stopped
	Crime Victims Risk	Loss	89	Theft
	IT System Risk	Loss	90	Communication line problems/ breakage
		Loss	91	Attack by hacker/computer virus

Chapter-7 : Documentation

- Each Risk Owner shall maintain the Risk Register of their department. Refer Appendix 8.3.
- All key risks identified shall be documented in the Consolidated Risk Register maintained by Risk Coordinator.
- Risk Identification Form (Appendix 8.4) should be prepared for any new risk identified to be placed to Risk Management Organisation for approval.
- Minutes of all Risk Management Committee should be documented and maintained with Risk Coordinator

Chapter-8. Appendices

8.1 Impact Rating

Impact Description	Impact Parameter	Impact Rating				
		5	4	3	2	1
		Very High	High	Medium	Low	Insignificant
Potential Financial Impact per event	Absolute impact on Revenue or	> INR 10 Crs	INR 5 - 10 Crs	INR 1 - 5 Crs	INR 20 lacs - 1 Cr	< INR 20 lacs
	%age of Average Profit of past 3 years	> 10%	5% - 10%	3% - 5%	1% - 3%	< 1%
Compliance & Regulatory	Penalty/Demand	Penalty of more than INR 5 lacs	Penalty of INR 50k – 5 lacs	Penalty of less than INR 50k	Caution / instructions from Ministry	Routine issues raised by regulatory authority
	Restrictions to operate	Loss of rights to operate in specific areas	Restrictions on activity	Intensive scrutiny		
	Prosecution	Imprisonment of key officials				
Loss of Talent	Separation of employee	Separation of key individuals at senior management level	Separation of skilled personnel effecting operations for long run	Separation of skilled personnel effecting operations for short term	Impacts operations but gaps can be filled with existing employees	Separation not impacting operations
Health, Safety and Environment	Accidents	Fatality	Multiple persons /injuries per project (i.e. hospitalization for more than 24 hours)	Single persons /injury per project (i.e. hospitalization for more than 24 hours)	Multiple persons / injuries per project (i.e. hospitalization for less than 24 hours)	Single persons / injury per project (i.e. hospitalizatio n for less than 24 hours)

	Environmental damage	Environmental damage requiring >iNR 5 lacs to correct	Environmental damage requiring INR 1 to 5 lacs to correct	Environmental damage requiring INR 50k to 1 lac to correct	Environmental damage requiring less than INR 50k to correct	Insignificant Environmental damage
Business Continuity	Loss or corruption of critical data/ designs / knowledge	Complete inability to deliver projects for more than 15 days	Inability to deliver key projects for 7 – 15 days.			
	Unavailability of critical infrastructure, staff, utilities and/or IT services/funds	Widespread inability to deliver projects.	Inability to deliver key projects for up to 4 weeks. Consequent major disruption to projects over multiple milestone periods.	Unavailability between 3 & 5 days	Unavailability between 1 & 3 days	Inability to deliver projects for 2 days or less at non-critical times of the year.
	Disruption of Business	Disruptions up to 15 days	Disruption between 7 to 15 days			
Reputation	Brand Image	Significant negative publicity resulting having a measurable consequent impact.				
		Sustained negative publicity (nation-wide)				
Ethics	Confidentiality	Breach of confidentiality				

8.2 Likelihood Rating

Rating	Criteria
5 - Almost Certain	80 - 100% probability of risk occurring or
	Ongoing risk
4 - Likely	50 - 80% probability of risk occurring or
	Risk likely to occur weekly basis
3 - Possible	30 - 50% probability of risk occurring or
	Risk likely to occur monthly basis
2 - Rare	10 - 30% probability of risk occurring or
	Risk likely to occur once a year
1 - Unlikely	0 - 10% probability of risk occurring or
	Risk likely to occur only in exceptional circumstances

8.3 Risk Register Template

The Management has established a template for each section to develop their Risk Register. The template could be viewed as a single sheet, which shows the following fields (or headings). Completion of the Risk Register in below format will allow review by senior management.

- Risk Identification Number
- Risk (a short description of the foreseeable risk)
- Likelihood rating (estimate of likelihood of occurrence)
- Impact rating (potential consequence to people, the environment and/or Company operations)

- Risk Mitigation Plan (existing and additional for residual risk)
- Indicative root cause (reasons due to which risk persists)

Risk No.	
Functional Area	
Risk Description	
Control Description	
Risk Owner	
Impact Score	
Likelihood Score	
Risk Score	

					RISK ASSESSMENT - RESIDUAL RISK							
Risk reference no.	Risk Name	Risk description	Indicative Root Cause	Current Mitigation Plan	Likelihood rating	Likelihood factor	Impact rating	Impact factor	Exposure ratings	Action Plan	Owner	Target Date

8.4 Key Risks

The Company has identified following key risks. The department and the risks are identified as under: *(To be updated)*

Department wise risk summary:

S. No.	Department Categorization	No. of Risks
1	Finance & Accounts	
2	Production, Quality and Maintenance	
3	Human Resource & Payroll and Administration	
4	Order to Cash	
5	After Sales Service	
6	Part Control Production Control	
7	Purchases	
8	Information Technology General Controls	
9	Logistic	

8.5 Risk Identification Form

Risk Identification Form
Assessment No.

HONDA
POWER PRODUCTS

Brief outline of activity or work		**Assessor**	
Location		**Reviewed by:**	

Risk Identified	Who might be a risk	Existing Controls	Likelihood	Severity	Residual Risk	Additional Control Measures Required	Date actioned	Estimated Residual Risk

REVIEW DATE

8.6 Following details will be captured:

Event Recording register

Sr. No.	Date of occurrence of event	Nature of event	Whether the event already identifed in Risk Register, if yes		Risk Treatment - Mitigation (Terminate, Treat, Transfer, Accept)	Action taken to mitigate or reduce the risk	Actual impact on the Company	Date of reporting of risk, if any
			Risk Reference no.	Mitigation plan				

8.7 Risk Alert Form

RISK ALERT Subject 1st Report

TO:
cc:

Company name (abbreviation)	Reporter (Risk Management Officer)

Date of Occurrence	
Event occurred / which may occur	
The sequence of Event (briefly)	
Content of Violating act	
Law supporting Violating act	
Influence / Penalty (including worst scenario)	
Possible Causes	
Urgent Countermeasures	
Expert Comments and Reasons (if already got)	

*If you have detailed information, please attach it separately.

RISK ALERT

Subject

Report

TO:

cc:

Company name (abbreviation)	Reporter (Risk Management Officer)

Date of Occurrence	
Event occurred / which may occur	
Content of Violating act	
Law supporting Violating act	
influence / Penalty (including worst scenario)	
Possible Causes	
Expert Comments and Reasons	
Essential and real Cause	
Countermeasures (interim) and Completion date	
Countermeasures (permanent) and Completion date	