



Risk Management Manual

TABLE OF CONTENTS

1. PURPOSE	3
1.1 OBJECTIVES.....	3
1.2 BACKGROUND.....	3
2. SCOPE	3
3. POLICY	4
3.1 COMMITMENT TO RISK MANAGEMENT	4
3.2 RISK MANAGEMENT FRAMEWORK	4
3.3 RISK GOVERNANCE	5
3.4 LINKING RISK MANAGEMENT AND STRATEGY	9
3.5 RISK REGISTERS	11
3.6 INTERNAL AUDIT PROCESS	11
3.7 RISK REPORTING.....	12
3.8 RISK MANAGEMENT CONTINUOUS IMPROVEMENT.....	13
3.9 CRISIS MANAGEMENT.....	13
4. DEFINITIONS	13
5. RESPONSIBILITIES	13
5.1 POLICY MANAGEMENT	13
5.2 POLICY IMPLEMENTATION	13
6. PROCEDURE	14
7. REFERENCES	14
8. APPENDICES	15
8.1 RISK MANAGEMENT METHODOLOGY.....	16
8.2 PRINCIPLE 7 – RECOGNISE AND MANAGE RISK.....	33
8.3 MAJOR POLICIES	33
8.4 RISK REGISTER TEMPLATE (USING AN EXAMPLE OF THE BOARD RISK APPETITE REGISTER).....	36

1. PURPOSE

Risk is defined in ISO 31000:2018 as the 'effect of uncertainty on objectives'. Risk is inherent in all business activities, and every employee of Timken India Limited (hereinafter referred to as Timken or Company) continuously manages risk.

Risk management is defined in the ISO 31000:2018 as 'coordinated activities to direct and control an organization with regard to risk'. This document sets out the overarching policy for managing risk at Timken.

Timken recognizes that the aim of risk management is not to eliminate risk totally, but rather to provide the structural means to identify, prioritize and manage the risks involved in all our activities. It requires a balance between the cost of managing and treating risks and the anticipated benefits that will be derived.

Timken acknowledges that risk management is an essential element in the framework of good corporate governance and is an integral part of good management practice. The intent is to embed risk management in a very practical way into business processes and functions via approval processes, review processes and controls to add significant value to the Company; it is not to impose risk management as an extra requirement, which adds no value to the Company.

1.1 OBJECTIVES

The Risk Management Policy (the Policy) aims to ensure that the activities of Timken and its controlled entities if any, are undertaken within Board approved risk appetite and tolerance levels to protect the profitability, balance sheet and reputation of the company.

Embedding risk management principles and practices into strategy development and day-to-day operational processes is critical to achieving robust and proactive business outcomes – a balance between mitigating threats and exploiting opportunities. This Policy establishes the top-level framework for risk management at Timken.

1.2 BACKGROUND

Timken has developed a Risk Management Policy (the Policy) designed to protect and enhance resources and enable the achievement of its objectives.

The Policy emphasizes that risk management is an integral part of Timken's business processes.

The Policy is based on the following principles. Risk management is:

- The responsibility of the Board, all executives, managers, employees, and contractors
- Integrated into all business activities and systems.
- Based on the ISO 31000:2018 and
- Compliant with regulating laws

A structured risk management framework provides several beneficial outcomes by:

- Enhancing strategic planning through the identification of threats to the Timken's Vision and strategic goals
- Encouraging a proactive approach to issues likely to impact on the strategic and operational objectives of the Company.
- Improving the quality of decision making by providing structured methods for the exploration of threats and opportunities and allocating resources.

2. SCOPE

The Policy applies to all Directors, officers, employees and contractors of Timken and its controlled entities if any.

Where more detailed risk management policies or procedures are developed to cover specific areas of the Company's operations (e.g. Quality, occupational health and safety, environment, commercial activities) they should comply with the broad directions detailed in the Policy and should also comply to related Standards such as ISO 9001, IATF 16949, ISO 14001, ISO 45001 and sector specific needs such as IRIS and MI 1003.

3. POLICY

The Policy covers the following areas:

- Commitment to Risk Management
- Risk Management Framework
- Risk Governance
- Linking Risk Management and Strategy
- Risk Registers
- Internal Audit Process
- Risk Reporting
- Risk Management Continuous Improvement
- Crisis Management

3.1 COMMITMENT TO RISK MANAGEMENT

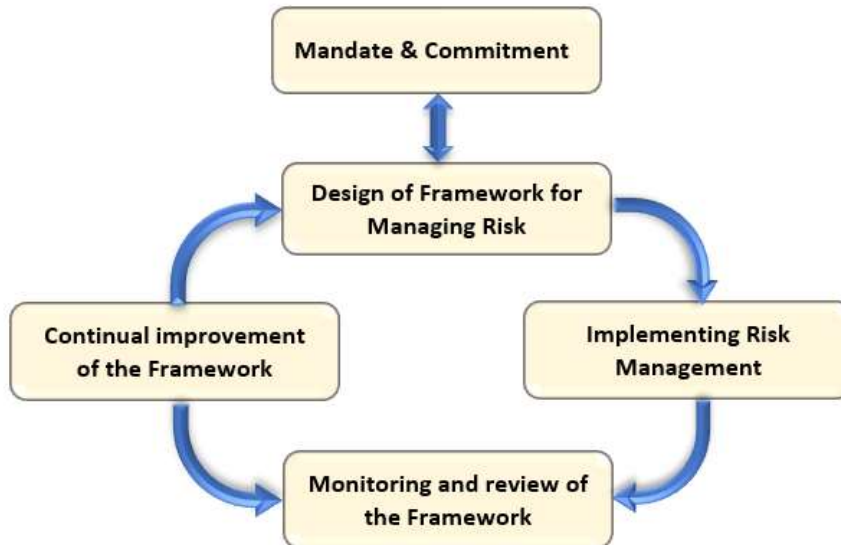
The Board and management of Timken are committed to the implementation and maintenance of a formal risk management system, including the integration of risk management throughout the organization, which is fundamental to the Company achieving its strategic and operational objectives.

3.2 RISK MANAGEMENT FRAMEWORK

The ISO 31000 forms the basis of the Policy. The Policy provides the foundations and organization arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout Timken. Figure 3.1 illustrates this framework diagrammatically.

The application of this standard is explained in the Risk Management Methodology set out in Appendix 9.1.

Figure 3.1: ISO 31000 Risk Management Framework



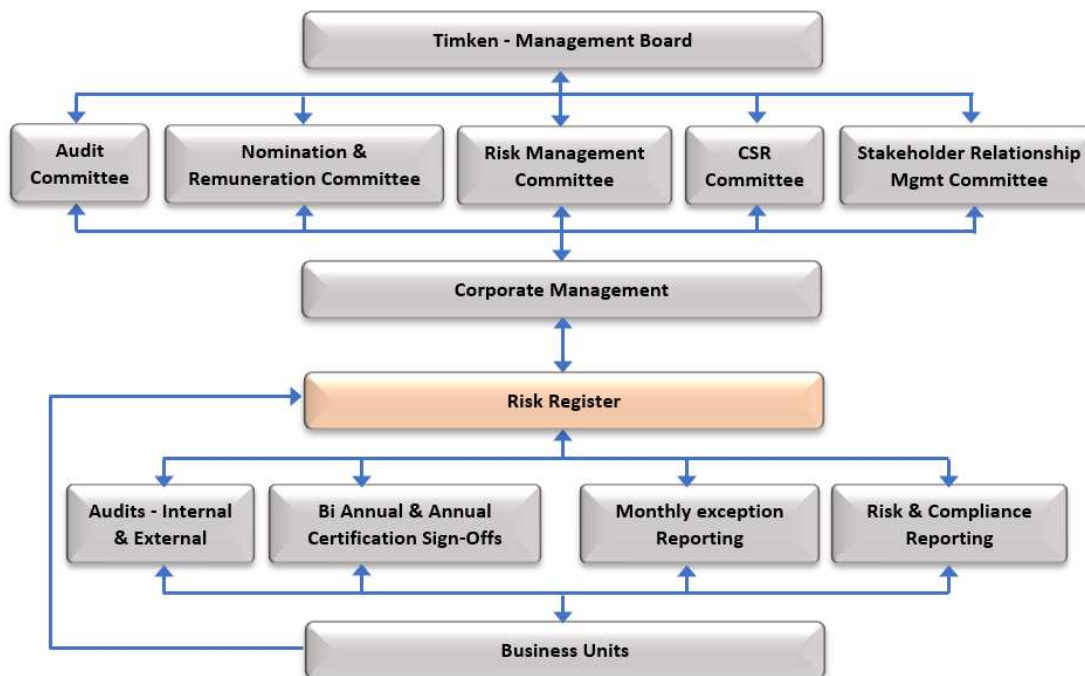
3.3 RISK GOVERNANCE

An effective risk management system is dependent on a governance structure that has:

- Roles and Responsibilities defined.
- Adequate separation of duties
- Proper systems of supervision and monitoring of activities and transactions
- Risk consciousness and a proactive approach to managing risks across the structure.

Figure 3.2 Provides an overview of Timken’s risk governance structure.

Figure 3.2: Risk Governance Structure



The Board

The Board retains the ultimate responsibility for risk management and for determining the appropriate level of risk that Timken is willing to accept. The role of the Board with respect to risk management encompasses both compliance and performance aspects:

- Compliance:
 - Allocate resources to implement and maintain the risk management process.
 - Delegate authorities and responsibilities
 - Monitor the organization’s performance having regard for its risk appetite and riskmanagement processes.
 - Review the ongoing effectiveness of the risk management process in achieving the organization’s objectives.
- Performance:
 - Agree the risk appetite of the organization having regard for the risk environment in which the organization operates.
 - Review the organization’s risk profile against its agreed strategy ensuring that they are aligned and within the agreed risk appetite.
 - Set the risk policies setting out the internal framework for ERM across the organization.
 - Set the ‘tone at the top’ for the organization including endorsing and adopting the Company’s Code of Conduct.

Board Committees

The Board has formally appointed the following board committees to monitor the relevant affairs of Timken on behalf of the Board:

- Audit committee
- Risk Management Committee
- Nomination and Remuneration Committee
- Stakeholder Relationship Management Committee
- CSR committee.

Provision is kept to form Special committees from time to time for specific events, for example growth projects, to enable the monitoring of processes etc .

Audit Committee

The Audit Committee has all the powers as mentioned in sub-regulation (2) (c) of Regulation 18 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (Listing Regulations). The role of the Audit Committee includes the entire role stated in Schedule II, Part C-A of Listing Regulations. The Audit Committee mandatorily reviews the information prescribed in Schedule II, Part C_B of Listing Regulations. The Audit Committee also acts in accordance with terms of reference prescribed under Section 177 of the Companies Act, 2013.

Nomination and Remuneration Committee

The committee shall identify persons who are qualified to become Directors and who may be appointed in senior Management in accordance with criteria laid down, recommend to the Board their appointment and removal and shall carry out evaluation of every Director's performance. The committee shall also formulate the criteria for determining the qualifications, positive attributes and independence of a Director and recommend to the Board a policy relating to the remuneration for the Directors, key managerial personnel and other employees and also devising a policy on Board diversity.

Stakeholders Relationship Committee

Terms of reference of this Committee include looking into grievances of security holders of the company, redressal of investor complaints, eg, transfer of shares, non-receipt of balance sheet, etc. and also to authorize registration of transfer of shares, issue of duplicate/new certificates, etc.

Corporate Social Responsibility Committee

The Committee shall formulate and recommend to the Board a corporate social responsibility (CSR) policy which shall indicate the activities to be undertaken by the Company as specified in Schedule VII, recommend the amount of expenditure to be incurred on the activities, monitor the CSR policy of the company from time to time.

Risk Management Committee

The committee shall monitor and review the risk management plan of the Company and discharge such other function as may be delegated to it by the Board of Directors of the Company. The committee will also Advise the board of the level of risk acceptable to Timken and Monitor and review the effectiveness of the risk and control environment.

On at least an annual basis the Risk Management Committee reviews the structure and processes in place within each relevant area to identify and assess the risks. This review includes a review of the status of all significant risks together with a review of risk events which have occurred since the last review and the resolution of those issues. . Role of this Committee shall be as per Schedule II, Part D of Listing Regulations

Special Projects Committee (on need base)

The Special Projects Committee can be framed on a case-to-case basis. The primary risk management role of this Committee relates to its role in reviewing, analyzing, and providing guidance to management on special projects that may arise from time to time. The Committee's is also tasked with providing guidance and recommendations during pre-feasibility and feasibility stages of various projects and



overseeing due diligence processes prior to recommendations being made to the Board

for approval of a special project.

Chairman Managing Director

The Chairman Managing director is responsible for the development and implementation of business strategies, budgets, setting performance benchmarks and creating a corporate culture compatible with the business objectives and risk appetite of Timken. Specifically, the CMD's key accountabilities include:

- Ensuring that a robust strategy is developed, regularly reviewed by management, discussed, and approved by the Board and communicated, as appropriate, within the company and with external stakeholders.
- Taking overall responsibility for implementing the agreed strategy to achieve the corporate-wide goals and KPIs set in the strategy.
- Reviewing on a regular basis and holding accountable the MD's direct reports for the performance of all the major divisions and units of the company in accordance with the corporate, business, project, and other plans.

A strong, useable, and effective ERM system underlies each of these key accountabilities.

The CMD promotes discussion amongst the senior management team of Timken on risk issues, in particular the process of assessing and identifying risks and alternative options for the treatment of these risks in line with changing business conditions, market practices and prudential controls.

Chief Risk Officer

The Chief Financial Officer (CFO) reports directly to the MD on the implementation, operations, and effectiveness risk management system. The CFO is the Chief Risk Officer and is responsible for the development and implementation of all risk management processes and methodologies. As such the CFO will:

- Lead the development, implementation, and management of the Timken risk framework in accordance with the applicable Standards for risk.
- Ensure that risk evaluation, monitoring, review and documenting occur in accordance with the Risk Management Policy and Methodology
- Provide advice to the Board to ensure compliance with relevant legislation, regulations, policies and standards and to build Timken's capability to mitigate risk related to human, financial and physical resources.
- Produce a consolidated Risk Register approved by the MD for submission biannually to the Audit and Risk Management Committee for review of limits of acceptable risk.
- Update the Risk Profile Matrix, which provides an overview of risks and potential liability.
- Additionally, the CFO is required to ensure that a comprehensive control system is operating efficiently and effectively.
- The CFO has overall responsibility for the management and reporting of risks and the implementation of risk management strategies and policies within Timken as determined by the Board.
- The Board has delegated to the CFO various risk limits and responsibility for the adherence to these risk limits.
- Additionally, the CFO is required to ensure that a comprehensive financial control system is operating efficiently and effectively.

Management

Management concerns itself with issues relating to the general operation of Timken as a whole and specifically with the operation and performance of activities under their direct control.

Management has a mandate to ensure risks are contained within approved risk tolerance levels and managed in accordance with Timken's Risk Management Policy.

Management has responsibility for ensuring there are adequate operating procedures and practices in place to identify, assess and manage risk in their direct areas of responsibility and test control systems for effectiveness and relevance. Additionally, management has responsibility to be generally involved in the management and treatment of risk throughout Timken.

Functional heads and risk owners identified by the function heads are responsible for affirming the accuracy of the Risk Registers for their area of responsibility and the effectiveness and on-going existence of risk mitigations to the MD.

Management is to hold risk management meetings at least biannually to discuss risk developments and initiatives to mitigate risk.

Management's role with respect to risk management comprises:

- Allocating resources to implement the agreed risk mitigation strategies on an ongoing basis.
- Developing and implementing systems to detect and report all risk events.
- Providing ongoing education and training in skills required to manage risk.
- Providing leadership in implementing and maintaining a structured risk management process to identify, assess and manage risks.
- Developing the enterprise-wide and strategic risks and mitigation strategies
- Agreeing the level of individual residual risks having regard for the agreed organization risk profile
- Ensuring the risk profile is aligned with strategy.
- Monitoring the major risks and risk events to ensure that risks are being properly identified and managed in accordance with the approved risk profile.
- Monitoring the ongoing effectiveness of the risk management process
- Mapping the risk environment of the Company
- Drafting and recommending the appropriate risk management structure
- Supporting the Board/Risk Management Committee in setting the 'tone at the top', including endorsing and adopting the Company's Code of Conduct.

Employees and Contractors

It is the responsibility of all Timken employees and contractors to:

- Be aware of those aspects of the risk management system that are immediately relevant to their jobs. To be aware of and act in accordance with all policies, procedures, guidelines, and work practices related to risk within their area of responsibility.
- Comply with all legislative, regulatory and Company policies and communicate any breaches promptly and accurately to the appropriate supervisor or manager.
- Report to their immediate supervisor or manager any real or perceived risks to the health, safety and working environment of themselves, their peers, or the public.
- Report to their immediate supervisor or manager any real or perceived risks that may significantly affect the profitability, performance, or reputation of Timken or that may leave the Company exposed to legal or regulatory action.
- Look for opportunities to improve operational efficiencies, optimize outcomes and minimize risk.

All employees are responsible for the ownership of, and for undertaking their part in, the actions and requirements of Risk Action and Mitigation Plans.

3.4 LINKING RISK MANAGEMENT AND STRATEGY

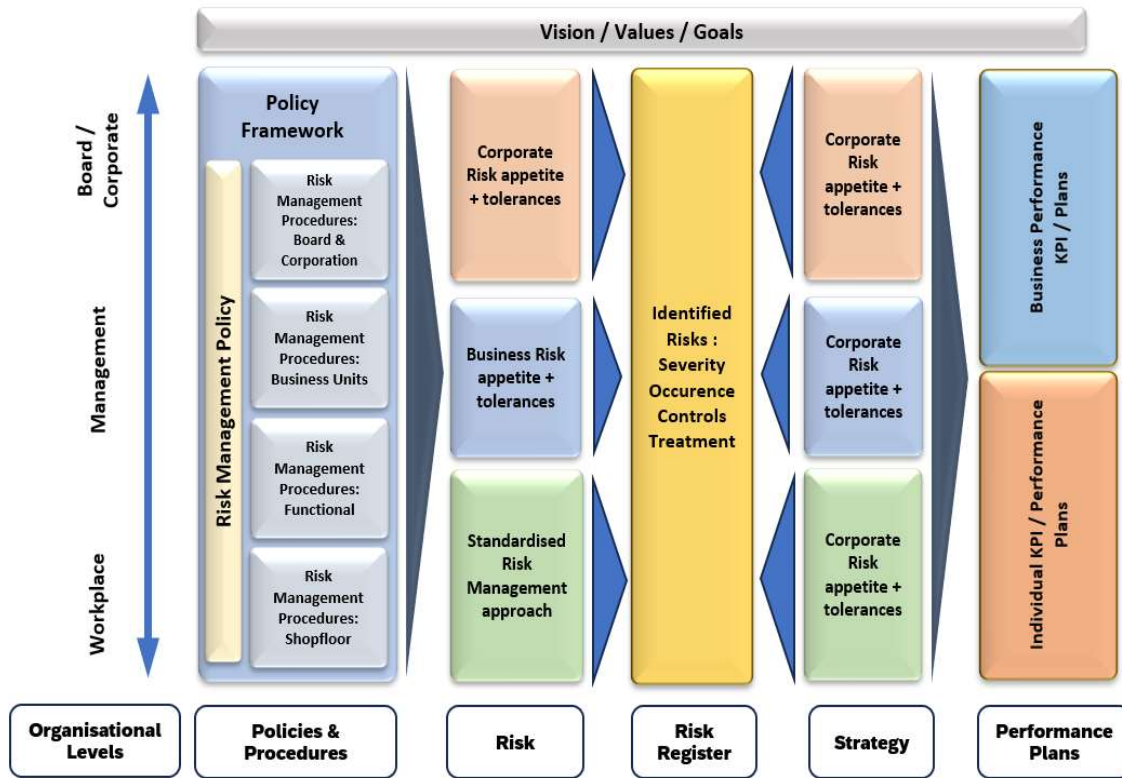
Embedding risk management principles and practices into strategy development as well as day-to-day operational processes is critical to achieving robust and proactive business outcomes – a balance between mitigating threats and exploiting opportunity.

As a general principle, the risk management process is to be undertaken in conjunction with strategic planning. The risks identified and evaluated as part of the strategic planning process will be the risks that will affect the entire Company and its ability to achieve its Vision.

Risk Registers are the primary mechanisms to bring corporate, business, and operational/functional strategies, as articulated in the hierarchy of strategic plans, together to ensure appropriate risk minimization plans are built into strategic implementation plans. The figure below illustrates how this occurs.

Figure 3.5: Linking Risk, Strategy and Performance and Process interaction

W



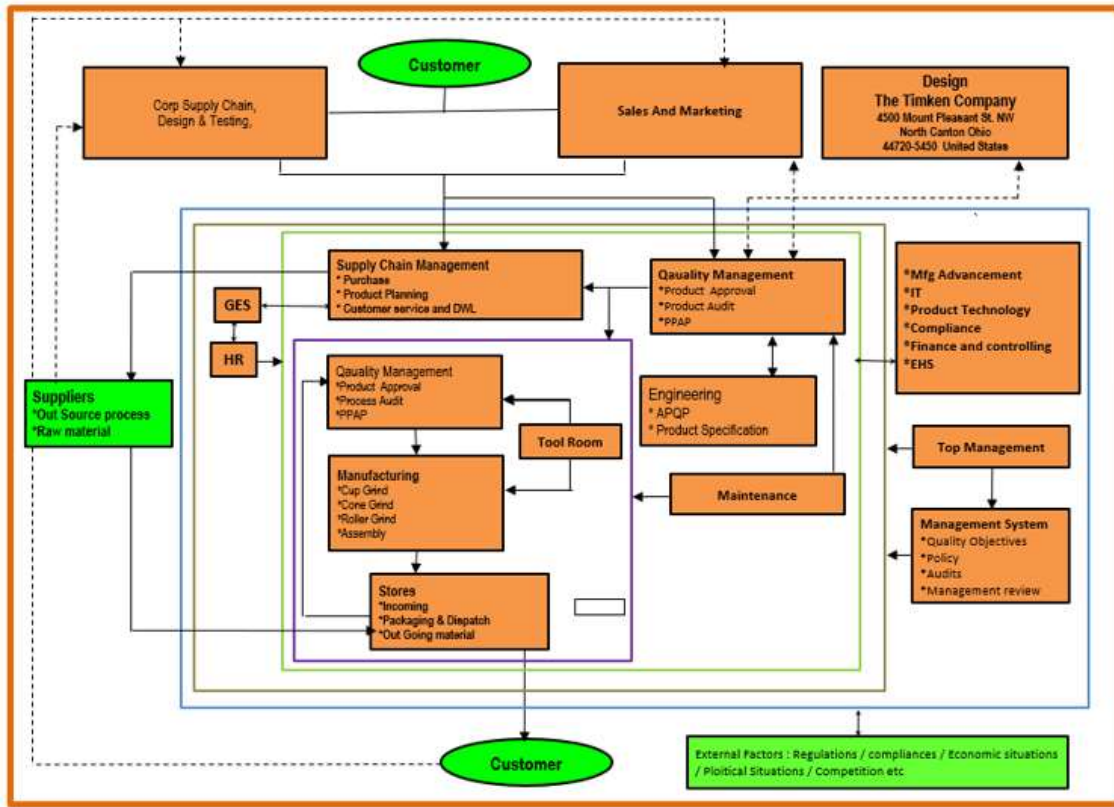


Figure 3.5 makes several key statements about risk management in Timken. First, the Company's Vision, Values and Goals have a major impact on Timken's risk and strategy frameworks. Our acceptance and rejection of risks all flow back to our Vision for the Company



Second, our risk management system needs to be integrated from the boardroom to the shop floor. We have different levels of risk, ranging from overall corporate risks such as the positive and negative impacts of making large investment decisions through to the risks associated with operating a particular product, equipment or a particular site. Our risk management system needs to allow an integrated and linked process of managing all these risks and reporting on these risks.

To this end, this policy framework needs to be companywide, able to be applied from the boardroom to each job site. To achieve this, the Risk Management Policy will be supplemented with a series of Risk Management Procedures. Each Risk Management Procedure will be relevant to the scope of operation to which it applies.

Third, the actual risk identification, risk analysis, risk evaluation and risk treatments will vary depending on the level of the organization at which the risk occurs. For example, the Board will maintain a corporate risk appetite and risk tolerance document. For each major division of the business, there will be business division risk appetite and tolerances. At each work unit, there will be a series of standardized risk management processes. Some of these risk management procedures will be based on specific

standards, such as ISO 9001, IATF 16949, ISO 14001 , ISO 45001 and Specific standards such as MI 1003 and IRIS

Fourth, the integrating feature of both the different levels of policies as well as the link between risk management and strategy is the Risk Register. The Risk Register is the means of recording risk management processes for identified risks. We intend to move to a system of an integrated Risk Register which allows the entering of risks and the reporting on risks at the different levels in the Company.

Fifth, this Risk Register will also be linked to the strategic processes of the Company. We currently have under development an integrated approach to strategy and strategic planning which commences with the overall corporate strategy and then proceeds to have a linked series of more detailed plans. At each level of planning, the strategies developed must be linked back to the risks identified for that level of the Company. Undertaking a risk identification/analysis/evaluation process can assist in the development of plans at all levels of Timken. The Risk Register will contain a cross reference to the specific strategies which discuss and address the risk.

Finally, we are moving to integrate the personal planning and KPIs with the strategic plans and their KPIs as well as the corresponding risks and Key Risk Indicators (KRIs). In this way we plan to have an integrated series of three management systems underlying the Company. These are:

- the risk management system
- the strategic planning and implementation system
- the performance management system for personnel.

3.5 RISK REGISTERS

The Risk Register is currently comprised of a series of unrelated spreadsheets across a combination of business units and risk types. The Company's intention is to move to an appropriate integrated risk management platform that is robust, easy to use and capable of upwards scalability to meet the needs of the Company's Vision.

Functional heads and risk owners identified by the functional heads have responsibility for maintaining risk registers for his/her areas of responsibilities. The registers are to:

- Use a system of unique Risk IDs that provide a linkage of risk to the Company's core strategies and functional business areas.
- List the risks which could cause losses to be incurred and possible causes.
- List the consequences.
- Provide an assessment of the inherent risks.
- Detail the existing risk mitigators.
- Provide an assessment of the strength of the mitigators.
- Provide an assessment of the residual risks.
- Detail any action plans to reduce residual risks.

Whenever any functions or systems are developed or changed, or new strategies, products or projects are considered, management is required to carry out a risk appraisal. This review is carried out using the procedures and tools set out in the Timken Risk Management Methodology. The respective Risk Register is to be updated accordingly.

3.6 INTERNAL AUDIT PROCESS

The Internal Audit function has been outsourced to one or more specialist audit services provider (Internal Auditor). The Internal Auditor carries out reviews of the various Company systems using a risk-based audit methodology. The risk registers maintained by each direct report are the foundation for all audits.

The Internal Auditor is responsible to the Board and is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas. The audit program is constructed having regard for the major risks of the business and the time since the last review was carried out on

these risks.

The Internal Auditor is responsible for reviewing the risks that have been identified, testing controls and following up to confirm that mitigation initiatives and recommendations have been implemented.

The Internal Audit function is the subject of an annual review by the Board having regard for information supplied by the external auditors and management as well as any third party, including regulatory authority reports.

3.7 RISK REPORTING

Risk is reported in the following ways:

Board Reporting

Board meetings generally convene quarterly. One function of Quarterly meetings is for the Board to be informed by management of current events, new developments and potential exposures to losses, as identified through the risk management system.

Assessment of Effectiveness

Risk owners will provide an annual certification that risks have been managed in line with this Policy.

Internal Audit Reporting

The Internal Auditor provides the Audit committee with its annual internal audit plan which is following risk-based approach after completing its work program as per the scope of work agreed between the Internal Auditor, business unit management. Based on the approved plan, the internal audit is carried out during the year and its reports are discussed in every quarterly meeting.

The report describes the review undertaken and tests performed, conclusions reached, corrective action plan, personnel responsible to take corrective action and completion dates.

Preparation of the report includes management's review to confirm accuracy of facts.

Copies of the report are provided to the MD and CFO. Relevant sections of the report are also provided to managers responsible as applicable for areas reviewed.

Statutory Compliance

Board reporting includes incident reporting as a standing item. Managers are required to forward to the Company Secretary all details of statutory and regulatory non-compliance and ensure that letters and responses to regulatory authorities are maintained, and made available to the Company Secretary, if requested.

The relevant executive is given responsibility for tracking any matters through to completion.

Issues with the potential to affect the share price or financial performance of Timken are reported at the earliest possible time to all Board members.

Assurance Reporting

Functional heads or the risk owners identified by functional heads are required to provide the Chief risk officer (CFO) or its nominated manager with updates on investigations into non-compliances and remedial action being taken to address risks relating to non-compliance.

Risk Mitigation Action Plans

Actions to improve risk mitigation are documented in the Risk Register. The Chief risk officer is to monitor the progress of implementing mitigating initiatives and reporting progress to the Audit and risk Management committee.

3.8 RISK MANAGEMENT CONTINUOUS IMPROVEMENT

Timken assesses the effectiveness of its Risk Management Framework through a well- structured

TIMKEN

continuous improvement process to ensure risks and controls are continually monitored and reviewed. This includes appraisal of actions taken by risk owners to manage risks, input from the Internal Auditor and other assurance processes.

The Risk Management Methodology is aligned with the principles of continuous improvement. It requires management to continually identify, assess, mitigate, review and report risks within their business units so that all risks are mitigated and managed to an acceptable level in accordance with Timken's risk appetite statement.

The diagram below illustrates the continuous improvement cycle in relation to risk management.

Figure 3.6: Risk Management Continuous Improvement Cycle



3.9 CRISIS MANAGEMENT

The ability to react effectively at an operational and strategic level to crisis events forms a subset of the Timken risk management framework. The Company's approach is outlined in the Crisis Management Manual and Procedures, which incorporate emergency response, strategic response, disaster recovery, and business continuity planning.

4. DEFINITIONS

To be added

5. RESPONSIBILITIES

5.1 POLICY MANAGEMENT

The Risk Management Policy is a 'living' document that will be altered as required. Approval of the Policy is vested with the Board.

Reviews of the Policy are the responsibility of the Policy Owner and will be conducted annually.

Advice and opinions on the Policy will be given by the Audit and Risk Management Committee.

5.2 POLICY IMPLEMENTATION

Implementation of this Policy is the responsibility of the CMD.

6. PROCEDURE

The Risk Management Policy is supported by the Risk Management Methodology set out in Appendix 9.1.

7. REFERENCES

The Risk Management Policy defines principles related to risk management, requiring management to develop, implement and maintain a structured and documented approach to risk management that is integrated within the day-to-day business activities.

The Risk Management Policy is part of a suite of policies developed to define the principles which management is required to adopt in directing and controlling Timken's activities.

This Risk Management Policy is supported by, and linked to, specific Timken policies and procedures as issued from time to time and hosted on its website and maintained by functional heads / their designated employees for respective functions

8. APPENDICES

- 8.1. Risk Management Methodology
- 8.2. Recognize and Manage Risk
- 8.3. Major Policies
- 8.4. Risk Register Template

8.1 RISK MANAGEMENT METHODOLOGY

Introduction

The Risk Management Standard ISO 31000 forms the basis of our risk management methodology.

The Risk Management Methodology sets out the approved processes and tools to be used for the implementation and maintenance of an enterprise risk management system for Timken.

Risk Management is applied across all of Timken's functions enabling all classes of risk to be managed in an integrated manner. It is important to note that this does not mean adoption of uniform methods for all types of risk.

Why Do We Need Risk Management

The underlying premise for risk management is that all organizations exist to provide value for their stakeholders. All organizations face uncertainty and the challenge for the Board and management is to determine how much uncertainty the organization is prepared to accept as it strives to grow stakeholder value.

Risk management enables the Company to operate more effectively in environments filled with risk. More specifically risk management allows the group to:

1. Align the strategic direction to its risk profile.

The development and execution of the group strategy will be worthless, and possibly even dangerous, if the risks involved in the strategy are not understood and those risks are not compatible with the group's desired risk profile.

2. Allocate scarce resources.

A good system of risk management can greatly assist in the most effective allocation of scarce resources. The risks are prioritized which helps with the determination of the optimum utilization of resources.

3. Consistently monitor operations, ensuring a climate of 'no surprises'

A structured risk management process ensures that the risks of the business are fully understood by all personnel from operatives to the Directors. It makes it easier to monitor and report on the mitigation of these risks to the desired level. It also helps ensure a climate of 'no surprises' even though risk events will occur, and losses associated with these risks be incurred.

4. Have solid bases for decision making.

When the risks associated with various alternate solutions are understood, the Board and management will be capable of making better quality decisions. Good risk management will ensure that decisions implemented will have acceptable levels of risk relative to growth and return objectives. Also, consideration of areas where risk can arise will highlight areas where opportunities for improvements exist.

5. Satisfy regulators, markets, etc.

The existence of a proper system of risk management is a basic tenet of good corporate governance and is a recommended requirement for public companies quoted on the Indian Stock Exchange. It is a foundation for any continuous disclosure regime required by regulatory authorities including SEBI.

Key Documentation

Details of conducting a risk management system in accordance with ISO 31000, are found in the following documents.

Table 1: Risk Management Standards and Guidelines

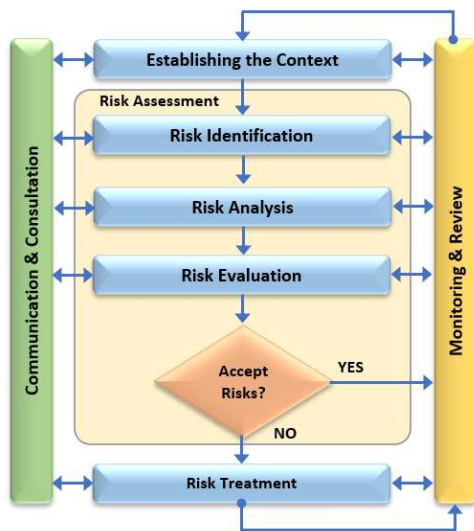
Reference No.	Title	Description
ISO 31000	Risk management – Principles and guidelines	This Standard provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000 is not specific to any industry or sector.
ISO Guide 73	Risk management - Vocabulary	Supporting standard for ISO 31000. Provides the definitions of generic terms related to risk management.
ISO 31010	Risk management - Risk assessment techniques	Supporting standard for ISO 31000. Provides guidance on selection and application of systematic techniques for risk assessment.
ISO 9001	Quality management systems -Requirements	Specifies requirements for Quality Management systems.
ISO 14001	Environment Management systems – Requirements	Specifies requirements for Environment Management Systems
ISO 45001	Occupational health and safety Management. System -Requirements	Specifies requirements for Occupational health and Safety management systems.
IRIS MI 1003	Industry specific requirements for Rail products	Specifies requirements for Specific industry specific requirements for Rail products for supplies to Europe and Americas

Copies of these documents are available on request from the Chief risk officer / CFO.

Risk Management Process

The risk management process is outlined in Figure 1 below.

Figure 1: ISO 31000 risk management process



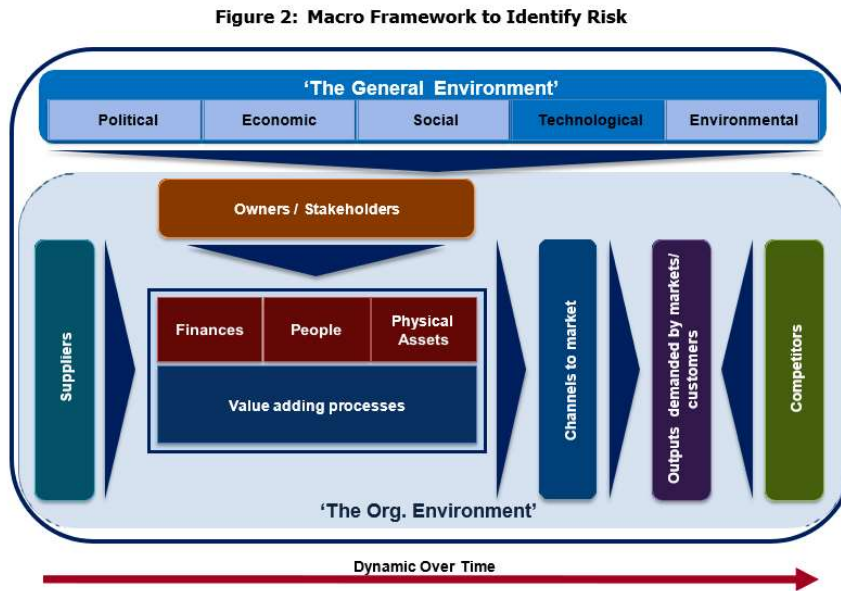
Step 1: Establishing the Context

(References: ISO 31000:2009, ISO : 31010)

'By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria'

The starting point to establish the risk context for Timken is the overall environment in which the Company operates. This is shown diagrammatically in Figure 2 and summarized below.

Figure 2: Macro Framework to Identify Risk



The Company, together with the industry, is impacted by the macro forces of the 'general environment'. These are:

- Political/regulatory environment
- Economic environment
- Social and demographic environment
- Technological environment
- Physical environment.

The industry or value chain is the next level of analysis. This involves identifying the risks inherent in the Company's:

- Suppliers
- Channels to market (both physical, e.g. rail, roads, ports, shipping, as well as intermediaries such as dealers / distributors and channel partners)
- The risks emanating from the markets in which the product is sold, and the risks associated with various segments of customers.
- The risks present due to the actual or potential actions of competitors.

The next level of risk analysis is the Company itself. For risk purposes, the Company can be considered as the stakeholders and owners, whose requirements must meet and the value adding structure of the Company.

The value adding structure of the Company comprises the three resources available to the Company:

- People
- Finance
- Physical assets.

The other component of the Company from a risk perspective is the value adding stages the organization undertakes in order to produce the products and services required by customers. In the case of Timken, this can be considered as:

- The development processes required to develop a new product.
- The process of manufacturing
- The systems which enable these value adding stages, e.g., human resource management, finance and accounting, supply chain etc.

Thus, the macro framework provides the overarching model to begin to establish the context for the identification and analysis of the risks facing Timken.

As such, the initial step in the risk management process is to conduct an environmental review. This review is normally conducted as part of the business planning process. The completion of this review ensures that the risk management process is aligned with

Timken's strategic direction and considers the total environment in which the company operates.

There are several tools that can help to develop an understanding of the risks facing the Company. These include, but are not limited to:

- SWOT Analysis
- PESTE Analysis
- Personal experience, corporate history, incident and events
- Audits or physical inspections
- Brainstorming
- Questionnaires
- Expert judgment.

Step 2: Identify Risks

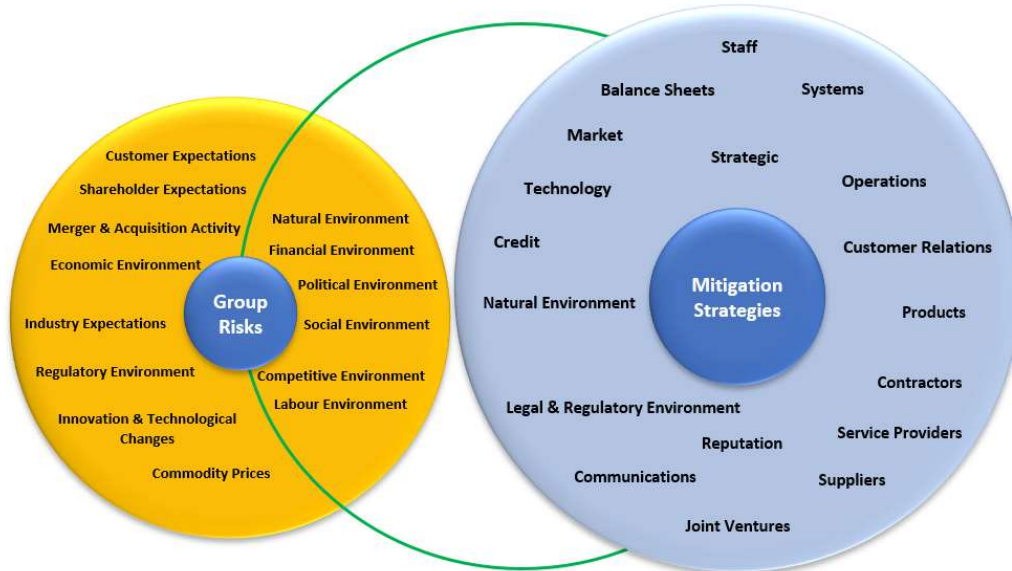
(References: ISO 31000, ISO: 31010)

'Risk identification is the process of finding, recognizing and recording risks' (ISO: 31010).

Risks that could impact operations and events that would result in the risk occurring need to be identified during this phase of the risk management process. Since the risk management process defines risk as 'the effect of uncertainty on objectives' (ISO 31000), it is helpful to link Timken's objectives to the risk identification.

To ensure that all risks have been considered, use the global and company risk areas set out in Figure 3 below.

Figure 3: Global and Group Risk Areas



The global risks which surround the group risks set out the uncertainties that have significant strategic impact on Timken. Global risks are normally difficult to manage.

The group risks are those over which management exercises control and for which management implements specific mitigation actions.

It is critical in this analysis stage to ensure that the proper risks are identified and that risks are not confused with the triggers or the consequences.

A trigger is an event which can cause a risk to occur. A consequence is the impact on Timken resulting from the risk event. There may be more than one trigger that can cause a particular risk occurrence, so it is important to identify all likely triggers.

Proper identification of the risks ensures that appropriate and cost-effective mitigation measures can be applied.

If consequences are confused with risks, the mitigators of some of the likely consequences arising from a particular risk event could be excluded. Alternately, separate mitigators for the various risk consequences may be put in place at the expense of an overall risk mitigation strategy which could be more effective and less costly.

Techniques to be used to identify risks include:

- Brainstorming
- History and failure analysis
- Process mapping
- Comparison with industry standards and practices.

Step 3: Analyze the Risks

(References: ISO 31000, ISO : 31010)

Level of risk = consequence x likelihood

Risk analysis is the process of calculating the likelihood of an event and consequence if it were to occur. The product of these two variables is the risk rating.

Thus, the consequences of each identified risk event need to be determined. When considering the consequences, both monetary and non-monetary consequences need to be considered.

The analysis is calculated initially on an 'inherent risk' basis; that is, the likelihood of the event occurring and the consequences of that event, if no mitigation strategies were put in place.

The triggers for each risk should also be determined. Some triggers may have more than one consequence; some consequences will apply to more than one trigger.

Use the generic consequence list set out in Table 2 below as a checklist to ensure that all outcomes have been addressed.

Table 2: Consequence List

Consequence
Revenue / margin loss
Loss of sales
Loss of production
Loss of customers
Loss of capital
Loss of funds
Loss of assets
Loss of license
Increased costs
Write-off / write-downs
Penalties
Litigation / Judgment / Settlement Cost
Restitution / Compensation
Recovery Cost
Rework Cost
Cost of handling complaints
Injury / Stress Compensation Claims
Damaged reputation
Reduced share price

The next step requires an assessment of an Inherent Risk Rating.

The Inherent Risk Rating is based on the likelihood of the risk event occurring and the financial impact of the event.

Determining likelihood can be subjective, particularly where data are not available. However, historical data that consider frequency of exposure and statistical data are often available and can be used to determine whether the likelihood of an event is:

- Almost certain
- Likely
- Possible
- Unlikely
- Rare

The likelihood of the risk occurring is linked to probabilities. The higher the probability, the higher the likelihood. The likelihood rating scale in Table 3 has been developed as a tool to assist with the Likelihood assessment.

Table 3: Likelihood Rating

Likelihood Rating	Likelihood and Frequency
5	Almost Certain: Risk is expected to materialize multiple times over a 1-year period
4	Likely: Risk is expected to materialize once in a 1-year period
3	Possible: Risk is expected to materialize once in a 5-year period
2	Unlikely: Risk is expected to materialize once in a 10–12-year period
1	Rare: Risk is expected to materialize less often than once in a 12–15-year period

The impact of the risk event requires an assessment of the highest cost outcome, considering ancillary costs as well as direct costs that will be incurred if the risk event takes place. The Risk Impact Rating scale in Table 4 has been developed to assist with quantifying the impact.

The measurement of the consequences that do not have a natural monetary value, for example, reputation loss, need to be determined. Reputation loss, for instance, can be measured in loss of market value terms due to a reduction in share price. The main purpose of placing a value on the consequence is to get a feel for the magnitude of risk and its priority.

Table 4: Consequence and Impact Ratings

Impact Rating	Level of Consequence	Description	Financial Impact	Legal	Env & OH&S	License to Operate	Reputation
5	Catastrophic	Severely impairs the ability of the company to operate as a going concern	>\$10m	Major litigation, no settlement, maximum fine imposed on company, large fine imposed on individuals and potential imprisonment	Multiple fatalities, large numbers of severe injuries, Major issue of land / water contamination or environment Hazard going beyond internal controls	Will result in withdrawal of license s; prohibition to operate; delisting from BSE / NSE	Widespread negative community sentiment; withdrawal of public and/or political support for continued operations
4	Major	Will have a significant impact on the operations of the company; will likely require market disclosure	\$5m - \$10 m	Significant litigation, settlement unlikely, medium fine imposed on company, small fine imposed on individuals is possible	Death, extensive injuries, significant hospitalization or Major issue of land / water contamination or environment Hazard but can be managed internally	Warnings from statutory bodies; fines and/or court action to seek remedies for breach	Damage to reputation causing delays or interruptions to existing or planned projects
3	Moderate	Requires CMD and leadership intervention to manage and resolve; may consume considerable resources to manage taking attention from day-to-day Operations,	\$500k - \$5 m	Minor litigation, settlement possible, small fine imposed on company, no fine imposed on individuals	Long term medical treatment required, however no fatalities, some hospitalization, Minor issue of land / water contamination or environment Hazard managed internally, Minor deviation in EHS compliances but not affecting business	Infringement / Notices issued	Local or community issue involving political involvement or inconvenient operations

TIMKEN

2	Minor	Requires Executive-level intervention to manage and resolve; notification to MD if required	\$10k - \$500K	Possible litigation, settlement likely, fine imposed on company is possible but unlikely, no fine imposed on individuals	Small number of injuries, first aid or outpatient hospital treatment, trivial minor issues of EHS compliances and controls deployment but can be managed with existing controls and have no impact on business	Regulatory bodies notified of breach	Adverse media coverage with short term damage to reputation
1	Insignificant	Is expected and can be managed through already-approved operations	<\$10k	No litigation, claims covered by workers compensation and less than deductible for property damage, no fine imposed on company or individuals	Incident not requiring medical intervention and no Env violations including compliances	Managed through internal operations	Minor effects on internal relations. Event info limited to Timken only

Impact Rating	Level of Consequence	Description	Financial Impact	Legal	Env & OH&S	License to Operate	Reputation
5	Catastrophic	Severely impairs the ability of the company to operate as a going concern	>\$10m	Major litigation, no settlement, maximum fine imposed on company, large fine imposed on individuals and potential imprisonment	Multiple fatalities, large numbers of severe injuries, Major issue of land / water contamination or environment Hazard going beyond internal controls	Will result in withdrawal of license s; prohibition to operate; delisting from BSE / NSE	Widespread negative community sentiment; withdrawal of public and/or political support for continued operations
4	Major	Will have a significant impact on the operations of the company; will likely require market disclosure	\$5m - \$10 m	Significant litigation, settlement unlikely, medium fine imposed on company, small fine imposed on individuals is possible	Death, extensive injuries, significant hospitalization or Major issue of land / water contamination or environment Hazard but can be managed internally	Warnings from statutory bodies; fines and/or court action to seek remedies for breach	Damage to reputation causing delays or interruptions to existing or planned projects
3	Moderate	Requires CMD and leadership intervention to manage and resolve; may consume considerable resources to manage taking attention from day-to-day Operations	\$500k - \$5 m	Minor litigation, settlement possible, small fine imposed on company, no fine imposed on individuals	Long term medical treatment required, however no fatalities, some hospitalization, Minor issue of land / water contamination or environment Hazard managed internally, Minor deviation in EHS compliances but not affecting business	Infringement / Notices issued	Local or community issue involving political involvement or inconvenient operations
2	Minor	Requires Executive-level intervention to manage and resolve; notification to MD if required	\$10k - \$500K	Possible litigation, settlement likely, fine imposed on company is possible but unlikely, no fine imposed on individuals	Small number of injuries, first aid or outpatient hospital treatment, trivial minor issues of EHS compliances and controls deployment but can be managed with existing controls and have no impact on business	Regulatory bodies notified of breach	Adverse media coverage with short term damage to reputation
1	Insignificant	Is expected and can be managed through already-approved operations	<\$10k	No litigation, claims covered by workers compensation and less than deductible for property damage, no fine imposed on company or individuals	Incident not requiring medical intervention and no Env violations including compliances	Managed through internal operations	Minor effects on internal relations. Event info limited to Timken only

Speed of Risk

While not yet discussed in the Standard, an added element to risk analysis is an assessment of the speed of risk, which can be defined as how quickly a risk area goes from the onset of the risk to the impact of the risk. The use of this rating recognizes that traditional risk assessments which priorities risk on likelihood and consequence can be outpaced by the speed at which risks can move throughout an organization.

Table 7 sets out the ratings that can be incorporated into the Risk Register and inform the risk management process.

Table 5: Risk Speed Ratings

Rating	Description	Elaboration
1	Advanced warning	Event can occur from the onset of the risk to the impact of the risk in more than a year
2	Moderate warning	Event can occur from the onset of the risk to the impact of the risk in 6 months to one year
3	Some warning	Event can occur from the onset of the risk to the impact of the risk in 1 to 6 months
4	Minimal warning	Event can occur from the onset of the risk to the impact of the risk in 7 to 30 days
5	No warning	Event can occur from the onset of the risk to the impact of the risk in 7 days or less

A risk that achieves a rating of 4 or 5, i.e., the onset of the risk to the impact of the risk ranges from less than 7 to 30 days or less, should be incorporated into crisis management plans. Risks that are rated as having a Speed of 1-3 can be dealt with in the normal course of risk management.

The Speed of risk rating is incorporated into the Risk Register and monitored for any changes that warrant an escalation of the management of the specific risk.

The Inherent Risk Rating equals the multiplication of sum of the Likelihood Rating and the Impact Rating and added with Risk speed rating

Risk rating = (Likelihood rating X Impact Rating) + Speed of risk rating

The Inherent and residual Risk Rating is then classified as per Table 6.

Table 6: Risk Rating

Risk Rating	Classification	Required Action for Residual Risks
Greater than 20	Extreme	Advise Board and monitoring required by Risk Management Committee
16-20	High	Regular monitoring required Executive Management
11-15	Moderate	Regular monitoring required Executive Management
Below 10	Low	General monitoring required by staff in functional area

The risk matrix in Table 7 can be used to combine LIKELIHOOD and CONSEQUENCE to use formula as mentioned above to determine risk ratings.

Table 7: Risk Analysis Matrix for Determining Level of Risk

CONSEQUENCE	Catastrophic	Low1	Moderate2	High3	Extreme4	Extreme4
	Major	Low1	Moderate2	Moderate2	High3	Extreme4
	Moderate	Low1	Low1	Moderate2	Moderate2	High3
	Minor	Low1	Low1	Low1	Moderate2	Moderate2
	Insignificant	Low1	Low1	Low1	Low1	Low1
		Rare	Unlikely	Possible	Likely	most Certain
LIKELIHOOD						

A realistic assessment is required as ‘under’ or ‘over’ optimism regarding either the LikelihoodRating or the Impact Rating will have a major impact on the approach to mitigation.

The above evaluation process gives management and directors some feel for the magnitude of the inherent risk in running the business and will assist:

- The Directors to understand the potential risk profile of the entity, i.e., the losses to which the business will be exposed if no mitigation is put in place or if mitigation strategies fail.
- Prioritizing the risks to mitigate
- In determining a reasonable cost to allocate for the implementation and on-going maintenance of the mitigation strategies.

Any risk identified as having an Impact Rating of 5, irrespective of the Likelihood Rating, requires a mitigation strategy to be developed and monitored.

Tools and techniques for risk analysis can include but not limited to:

- Likelihood/consequence risk matrix
- Hazard and operability studies (HAZOP)
- Scenario analysis
- Cost/benefit analysis (CBA)
- Decision trees.

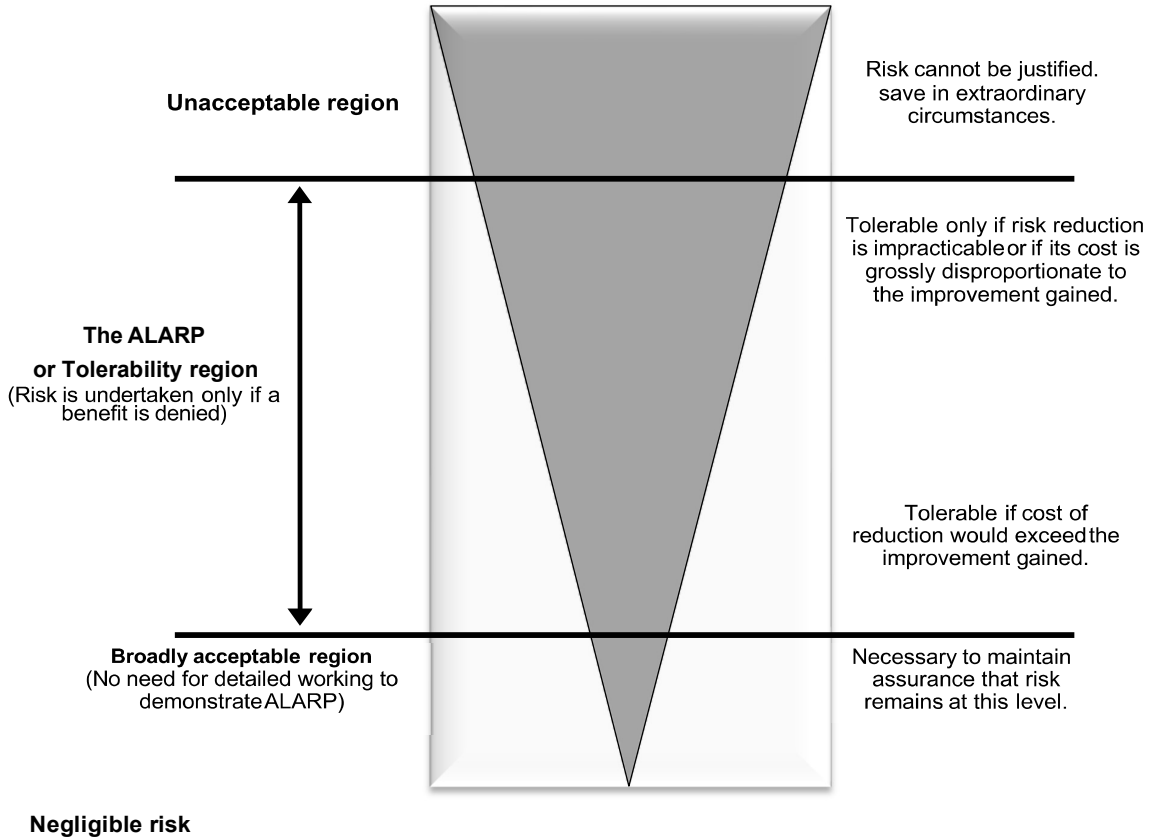
Step 4: Evaluate the Risks

‘The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation’

Having identified and analyzed the risk, the issue becomes how the risk is to be handled. Board, management and strategic priorities will generally determine how risks are prioritized for treatment. In doing so, the ALARP (‘As Low As Reasonably Practicable’) principle can be applied. The ALARP principle is used to determine how an organization can best reduce its risk exposures to within tolerable levels.

ALARP is often used for risks that will have negative consequences, particularly those involving risks to people or the environment. For a risk to be ALARP, it must be possible to demonstrate that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained. The ALARP principle arises from the fact that it would be possible to spend infinite time, effort and money attempting to reduce a risk so that it is negligible. Deciding whether a risk is ALARP can be challenging because it requires the Board and management to exercise judgment.

Figure 4: As Low as Reasonably Practicable (ALARP) Principle



Adapted from ISO 31010

A cost/benefit analysis (CBA) is also tool often used in risk evaluation. The outcome of a CBA is only one of several considerations that go towards the judgment that a risk has been reduced to ALARP.

Other tools and techniques for risk evaluation include

- HAZOP
- root cause analysis
- Monte Carlo simulations.

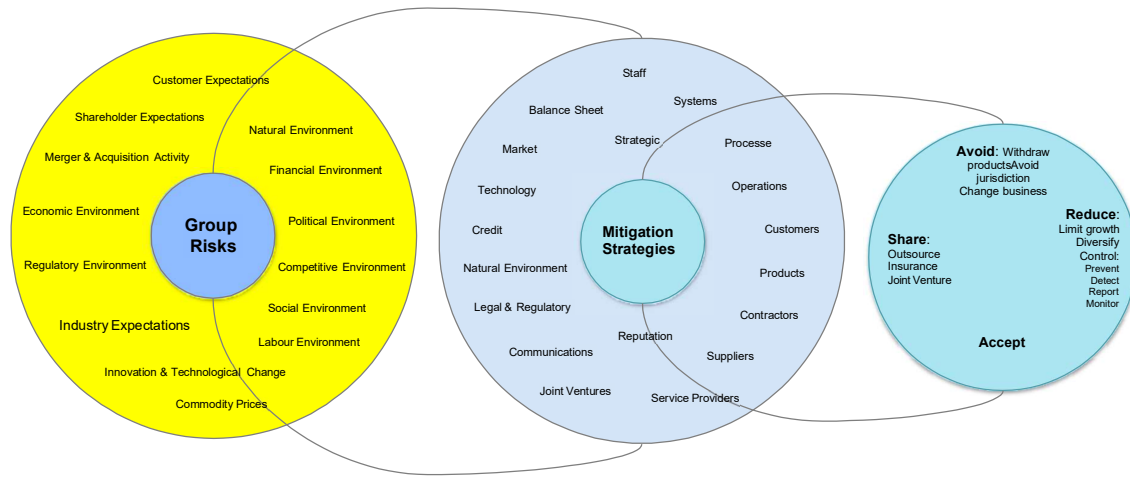
Step 5: Treat the Risks

'Risk treatment involves selecting one or more options for modifying risks, and implementing those options'

Once the quantum of risks is assessed, the necessary responses to the risks can be determined.

As highlighted in Figure 5, responses to risk fall within the categories of risk avoidance, reduction, sharing and acceptance.

Figure 5: Mitigation Strategies



If the return likely to be achieved is not worth the likely cost of the risk, steps to avoid the risk need to be taken. This can be done by:

- Withdrawing the specific business / products likely to cause the problems.
- Withdrawing from the problem jurisdiction
- Changing the business / operation model completely.

None of these are steps to be taken lightly.

If the likely return is acceptable having regard for the risk, but that the total risk to be assumed is too large for Timken's current resources, then the decision will be to share the risk with other parties.

The normal methods to share risks are to:

- Outsource certain processes to a third party.
- Share the business project with subsidiaries.
- Ensure the risk, either using normal causality insurance products or financial derivative

If a risk is shared, it does not mean that further risk mitigators, especially controls, are not necessary. It must be remembered that sharing current risks can create new risks, for example, credit risks or risks occasioned by lack of direct control of a process. If a risk is shared, a new risk assessment must be completed to identify, evaluate and, as necessary, mitigate the new risks assumed.

- Risks may be accepted without further mitigation if they are either within management's tolerable residual risk limits at the inherent level, or else it is a risk which cannot be avoided, for example, it is an essential part of a larger process. In the case of the latter reason, adequate detective controls and stop-loss limits will need to be put in place and there should be a sign-off by the Board that the risk will be accepted for strategic reasons.

Risks can be reduced. This can be done by:

- Limiting growth
- Diversifying into other products or other markets

establishing effective control mechanisms. There are different forms of controls including:

- 'Preventive controls' that reduce the likelihood of the risk event actually arising. They are proactive controls. Examples of preventive controls are separation of duties, proper authorization, adequate documentation, and physical control over assets.

- ‘Detective controls’ that identify when a risk event has occurred and allow action plans to be initiated to restrict the quantum of any consequence. Examples of detective controls are reviews, analyses, variance analyses, reconciliations, physical inventories and audits.
- ‘Advisory controls’ to ensure that the occurrence of the risk event is reported to management, the board, insurers, regulatory authorities, etc.
- ‘Restorative controls’ to assist in repairing the damage to the business arising from the risk event and recovering from the risk event.

The exact level of mitigation put in place will depend on the level of perceived risk, the level of acceptable risk and the cost of implementing and maintaining the required mitigation strategies.

The mitigators in place need to be assessed. The criteria for the assessment of Mitigation Effectiveness are set out in Table 8.

Table 8: Risk Mitigation Effectiveness

Measure	Result	Characteristics
Poor	Risk will not be controlled	<ul style="list-style-type: none"> • No mitigators exist to manage risks or else are ineffective
Limited	No guaranteed risk will be controlled	<ul style="list-style-type: none"> • Some informal risk management system, processes and procedures exist. • Staff not fully aware of, nor understand mitigators to manage risk
Basic	Basic risks will be controlled most of the time	<ul style="list-style-type: none"> • Documentation of some risk management systems, processes and procedures exist and are reasonably understood by staff. • Risk monitoring and management is informal • Promotion of control environment is informal. • Risk response action plans are informal
Good	Unexpected risk will be mitigated or detected in most circumstances	<ul style="list-style-type: none"> • Documentation of key risk management systems, processes and procedures exist and are understood by staff. • Risk monitoring and management is occurring but is less structured • Risk response action plans are identified and management ensures that controls are operating, although do not formally measure effectiveness of those controls. • Management actively promotes a good control environment
Strong	Unexpected risk will be prevented	<ul style="list-style-type: none"> • Risk management systems, processes and procedures are formally documented, current and well understood by staff. • Management ensures compliance with risk management policy and procedures. • Management regularly monitors risk and risk triggers. • Effectiveness of mitigators is formally monitored through use of predictive indicators. • Management activity promotes a strong control environment

The next step involves the determination of the expected Residual Impact, that is, the Inherent Impact calculated earlier reduced by the effect of the mitigators which limit the quantum of the impact and / or the probability.

The methodology used to determine the Residual Risk is similar to that used to determine the Inherent Risk. The only difference is that the Likelihood Rating and Impact Rating are determined after consideration of the influence of controls in place to reduce the likelihood and / or consequence.

The Residual Risk is then classified as Extreme, High, Moderate or Low using the scale used for Inherent Risk.

The tolerance for the Residual Risk needs to be determined. Tolerance is the amount that can be foregone each year in respect of the risk. This amount must be aligned with the group risk appetite approved by the Board.

TIMKEN

For controllable risk, the residual risk would normally be expected to be within tolerance where the effectiveness of the mitigation strategies was assessed as either 'Good' or 'Strong'.

If the Residual Risk is in excess of the tolerance for any risk, an Action Plan setting out the steps to be taken to reduce the risk to tolerable levels together with a reasonable time frame in which the Action Plan will be implemented must be prepared for management approval.

Step 6: Monitor and Review the Risks

Predictive Indicators should be identified to help monitor risks and the effectiveness of mitigators on an on-going basis.

A Predictive Indicator is a measurement indicator for monitoring the operation of mitigators against pre-set tolerances. In most cases, Predictive Indicators are Key Performance Indicators for the risk or its mitigation, for example, quality controls, expenses, etc. They could also be symptoms of poor performance, for example, customer complaints, negative media reports, poor staff morale, etc.

Predictive indicators can help management foresee problems which may lie ahead and assist in preventing losses or unfavorable outcomes through earlier management intervention.

Whatever process is introduced, it needs to be able to indicate very early if a problem is arising and the process should be documented and applied consistently.

Change to Business and / or Business Environment

Whenever there are changes to the risk environment, a risk assessment needs to be undertaken to determine what responses are required, both immediately and in the future. If the changes are major, use the Risk Environment Change Model included in Table 9 below to identify the changes which require analysis and the areas which may be impacted.

Table 9: Risk Environment Change Model

FORCES OF CHANGE	External			Internal	
	REGULATION	MARKET	OTHER	ORGANISATION	OTHER
	New/proposed legislation: <ul style="list-style-type: none"> • International • Central government • State government • Local bodies 	Competitors	Shareholders	New strategies/policies	Employee demands
	Court/tribunal decisions	Customers	Third party commentators: <ul style="list-style-type: none"> • Ratings agencies • Company analysts 	Organizational changes: <ul style="list-style-type: none"> • M & A activity • Structure • Resourcing 	Changes in assets or their ownership
New/proposed regulatory action: <ul style="list-style-type: none"> • Enforceable • Voluntary 	Suppliers: <ul style="list-style-type: none"> • Goods • Services • Capital 	Community activist groups: <ul style="list-style-type: none"> • Environment • Consumer • Labor 	New systems and processes		

Impacts of change	Strategies		People		Processes		Performance	
	Risks	Response	Risks	Response	Risks	Response	Risks	Response
Current								
Future								

Step 7: Communication and Consultation

'Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process'

As risks are interrelated, it is essential that communication and consultation with stakeholders across the Company takes place at each stage of the risk management process. A number of risks are the responsibility of one area while the mitigation is the responsibility of another area or function.

Communication should address the risk itself and the process to manage it.

Effective internal and external communication is important to ensure that those responsible for implementing the risk management system and those with a vested interest understand the basis on which decisions are made and why particular actions are required.

Communication is a two-way process; it must flow upwards through management to the Board, and downwards to all staff from the Board.

Risk Registers

The information gathered at each stage of the Risk Management Process should be documented in the group Risk Registers.

In creating the Risk Register, the risk owners (i.e. the persons who are actually accountable for managing the risk and its consequences) can satisfy themselves that they have defined and properly addressed the real risk. It makes it easier to review the risks and ensure that they continue to be complete, relevant and accurate having regard for both internal and external changes.

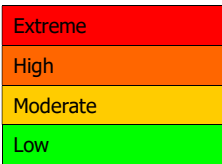
Documentation of 'who does what and when', especially in respect of mitigators and monitoring programs and processes, ensures that the knowledge is not lost or degraded on loss of current staff.

Documentation of risks is the foundation for any meaningful verification process by senior management, the Board, Audit and Risk Management Committee or other Committees of the Board, internal and external auditors and regulatory authorities of the ongoing existence and relevance of, and compliance with, the risk management process.

Documentation may also be required evidence in insurance claims, court actions, etc.

Risk Registers should be dynamic documents; that is, as any risk, consequence, probability, mitigator or predictive indicator changes, the Register should be updated to reflect the current situation. Appendix 9.4 below contains a register template. Table 10 includes an overview of the information required to complete a register.

Table 10: Risk Register Overview

Risk ID #	Unique identifier assigned to each risk in the register.	
Category	<p>The category the risk fits into under the strategic risk categories identified:</p> <ul style="list-style-type: none"> • Financial • Sales & Customers • Rail & Port • Project Evaluation • Operations • Environment • Strategy • People • Reputation 	
Generic Risk	Based on the category, describe the risk in general terms, e.g. workforce shortage, debt, currency fluctuations	
Specific Risk	Describe the risk in detail	
Triggers	How can it happen?	
Consequence	Describe what will happen if the risk eventuates	
Speed of Risk	Rates how quickly a risk area goes from the onset of the risk to the impact of the risk	
Predictive Indicators	The measurement indicator for monitoring the operation of mitigators against pre-set tolerances – the KPIs	
Inherent Risk	Likelihood Rating	The chance of the risk/event happening if uncontrolled
	Impact Rating	The impact of the risk before any control(s) has been implemented
	Risk Rating	The inherent risk rating represents the level of risk/impact associated with a risk BEFORE the controls have been implemented to reduce the risk/impact
	Risk Level	<p>Color coding based on level BEFORE control(s):</p> 
Risk Owner	<p>Who will monitor this risk and its treatment, i.e. who is the risk owner? Risk ownership is a fundamental principle of risk management. Risk owners must remain fully aware of:</p> <ul style="list-style-type: none"> • Risk exposures (i.e. incidents) • Pending risk assessments • Outstanding reviews and actions • Allocation of actions to be completed • Breaches of risk tolerance 	
Risk Tolerance	Measure	How the risk tolerance is measured (which KPI)
	Metrics	The level set by the board/management for maximum tolerance of the risk (KPI threshold limit)
Preventative Controls	The control(s) that reduce the likelihood of the risk event arising	

Detective Controls	The control(s) that identify when a risk event has occurred and to allow action plans to be initiated to restrict the quantum of any consequence				
Effectiveness of Controls	Describe how adequate current controls are using the categorization set out in Table 6 of the Risk Management Methodology, i.e.: <ul style="list-style-type: none"> • Poor • Limited • Basic • Good • Strong 				
Residual Risk	Likelihood Rating	The chance of the risk/event happening AFTER it is controlled			
	Impact Rating	The impact of the risk after the control(s) has been implemented			
	Risk Rating	The residual risk rating represents the level of risk/impact associated with a risk AFTER the controls have been implemented to reduce the risk/impact. It is expected that this score should be lower than the raw risk assessment			
	Risk Level	Color coding based on level after control(s): <table border="1" style="margin-left: 20px;"> <tr><td style="background-color: red; color: black;">Extreme</td></tr> <tr><td style="background-color: orange; color: black;">High</td></tr> <tr><td style="background-color: yellow; color: black;">Moderate</td></tr> <tr><td style="background-color: green; color: black;">Low</td></tr> </table>	Extreme	High	Moderate
Extreme					
High					
Moderate					
Low					
Is Residual Risk Tolerable?	Yes or no?				
Action Plan for Improvement	Describes how the chosen treatment options will be implemented				
Related Corporate Strategy	What corporate strategy or strategies does this risk relate to?				

8.2 RECOGNISE AND MANAGE RISK

Companies should establish a sound system of risk oversight and management and internal control.

Risk management is the culture, processes and structures that are directed towards taking advantage of potential opportunities while managing potential adverse effects.

A risk management system should be designed to: identify, assess, monitor, and manage risk.

Identify material changes to the company's risk profile.

This structure can enhance the environment for identifying and capitalizing on opportunities to create value.

Recommendation 7.1

Companies should establish policies for the oversight and management of material business risks and disclose a summary of those policies.

Recommendation 7.2

The board should require management to design and implement the risk management and internal control system to manage the company's material business risks and report to it on whether those risks are being managed effectively. The board should disclose that management has reported to it as to the effectiveness of the company's management of its material business risks.

8.3 MAJOR POLICIES

[Policy on disclosure of material events and information](#)

The Disclosure Policy requires all price sensitive information to be released to the market through a structured process complying with continuous disclosure rules and that third party briefings are only conducted by authorized personnel.

[Investment Policy Applicable to Short Term Investments](#)

The Short-Term Investments Policy is to ensure that liquidity is maintained to meet operational requirements, that adequate credit controls are maintained to minimize loss of capital and that only authorized investment products are used.

[Foreign Exchange Hedging and Foreign Exchange Hedging Product Policies](#)

The Foreign Exchange Policy specifies the foreign exchange hedging limits to minimize exposure to currency risk caused by foreign exchange rate volatility.

[Intercompany Internal Interest and Management Charges Policy](#)

The Internal Interest and Management Charges Policy sets out the methodology for intra-group charges between Timken and its controlled entities.

[Environment health and Safety \(EHS\) Policy](#)

The EHS Policy specifies the need for Timken's operations to be carried out at all times in compliance with all environmental and safety related legislative requirements, adhering to all relevant business codes of practice and having due regard to acceptable environmental and safety standards.

[Whistleblower Policy](#)

Timken operates with a zero-tolerance policy regarding fraud and corruption. The Fraud and Corruption and Whistleblower Policy recognizes the need for Timken to protect its revenue, property, information and other assets from any attempt by employees, contractors or members of the public to gain by deceit any financial or other benefit, and to provide a confidential and anonymous mechanism for reporting of potential or actual fraud and corruption.

[Quality Policy](#)

The Quality Policy requires management and staff to run Timken's operations by driving quality as core value.

[Timken India Code of conduct, Insider trading policy](#)

The Share Trading Policy specifies the need for all trading in the company's securities by employees and directors to accord with Common Law, the Corporations Act and Listing Rules to prevent employees benefiting from information which has not been released to the financial market.

[Treasury Policy](#)

The Treasury Policy is Timken's governing document for financial risks managed by the Commercial department.

[Data privacy Policy](#)

This policy describes protecting the security and confidentiality of the data people entrust to us. This includes the data provided by our fellow associates, as well as information we receive from our customers, suppliers and other third parties with whom we do business.

8.4 RISK REGISTER TEMPLATE

ERMS HV H Vamanamoorthy

Risk Query Record Count: 12 Search Export

Risk Detail Query

Process: COMPLIANCE Risk Category: COMPLIANCES Internal Risk ID: Generic Description of Risk/Specific Risk/Risk Trigger/Predictive Indicator: Status: All

Risk ID	Internal Risk ID	Process Desc	Sub Process	Risk Category	Generic Description of Risk	Specific Risk	Risk Trigger	Consequence	Risk Speed	Risk Speed Rating	Predictive Indicator	Likelihood Freq	Likelihood Rating	Impact Area	Impact Nature	Impact Rating	Risk Rating	Risk Owner	KPI measure Toleranc
P01001	Compl-09	COMPLIANCE WITH LAWS AND POLICIES	COMPLIANCES	COMPLIANCES	Non Compliance with Policies	Non adherence of Code of Conduct	careless approach of associates	Damaged reputation	Moderate warning - Event. Can occur from the onset of the risk to the impact of the risk in 6 months to one year	2	Feedback from internal team or behaviour of associate	Possible - Risk is expected to materialize once in a 5 year period	3	Legal	MODERATE	3	11	Company Secretary & Chief Compliance	Feedback team or assessment
P01002	Compl-10	COMPLIANCE WITH LAWS AND POLICIES	COMPLIANCES	COMPLIANCES	Non Compliance with Laws	change in laws having adverse effect	new notification about change in law is announced.	Litigation / Judgment / Settlement Cost	Moderate warning - Event. Can occur from the onset of the risk to the impact of the risk in 6	2	Ongoing discussion on particular area from government bodies, agencies, industry in public forum	Likely - Risk is expected to materialize once in a 1 year period	4	Legal	MINOR	2	2	Company Secretary & Chief Compliance	Impact on process

Risk Management Policy

Timken Management is committed to adopt integrated risk management practices into all organizational activities and is committed to,

- Develop, deploy and improve a Risk Management Systems by customizing and implementing all components of risk management framework.
- Adopting ISO 31000 and applicable company laws as a basis for establishing our risk management approach covering all aspects of enterprise manner in an integrated way
- Providing required resources in organization to support in managing risks.
- Providing required authorities, responsibilities, and accountability at appropriate levels of the organization to identify, manage, mitigate and control risks.
- Aligning risk management to the strategy, objectives and culture of the organization
- Managing risks across Enterprise function to protect and improve our brand value and brand image.
- Comply to all statutory, regulatory and governance laws as per applicable framework.
- Promote systematic monitoring of risks and keep risk management framework always relevant to context of the organization.
- Continually work to communicate the value of risk management to relevant stakeholders.
- Utilize talent and potential of our associates in designing , developing , managing and improving risk management process in our enterprise .

Sanjay Koul
Chairman and Managing director
Timken India Limited