IMPERIAL HOLDINGS LIMITED

RISK MANAGEMENT FRAMEWORK

CONTENTS:

1. PURPOSE

This document sets out the risk management framework of the IMPERIAL Group (IMPERIAL) as revised periodically and the process and procedures that shall be pursued to implement the framework.

2. BACKGROUND

IMPERIAL acknowledges the importance of risk management and corporate governance principles. Risk is an intrinsic part of all activities undertaken by IMPERIAL. The organisation is exposed to certain peculiar risks, which are influenced by its specific choices and actions.

In its commitment to implementing enterprise wide risk management IMPERIAL recognises the relationship as set out in the framework that was originally derived from principles contained in the Committee for Sponsoring Organisations of the Treadway Commission (COSO) and the Australian/ New Zealand Risk Management standard, ISO 31000:2009(E) / SANS 31000:2009, but has been updated to align with the requirements of Institute of Risk Management South Africa Guideline to Risk Management. The following framework is therefore used as the basis for developing Imperial's Risk Management Framework:

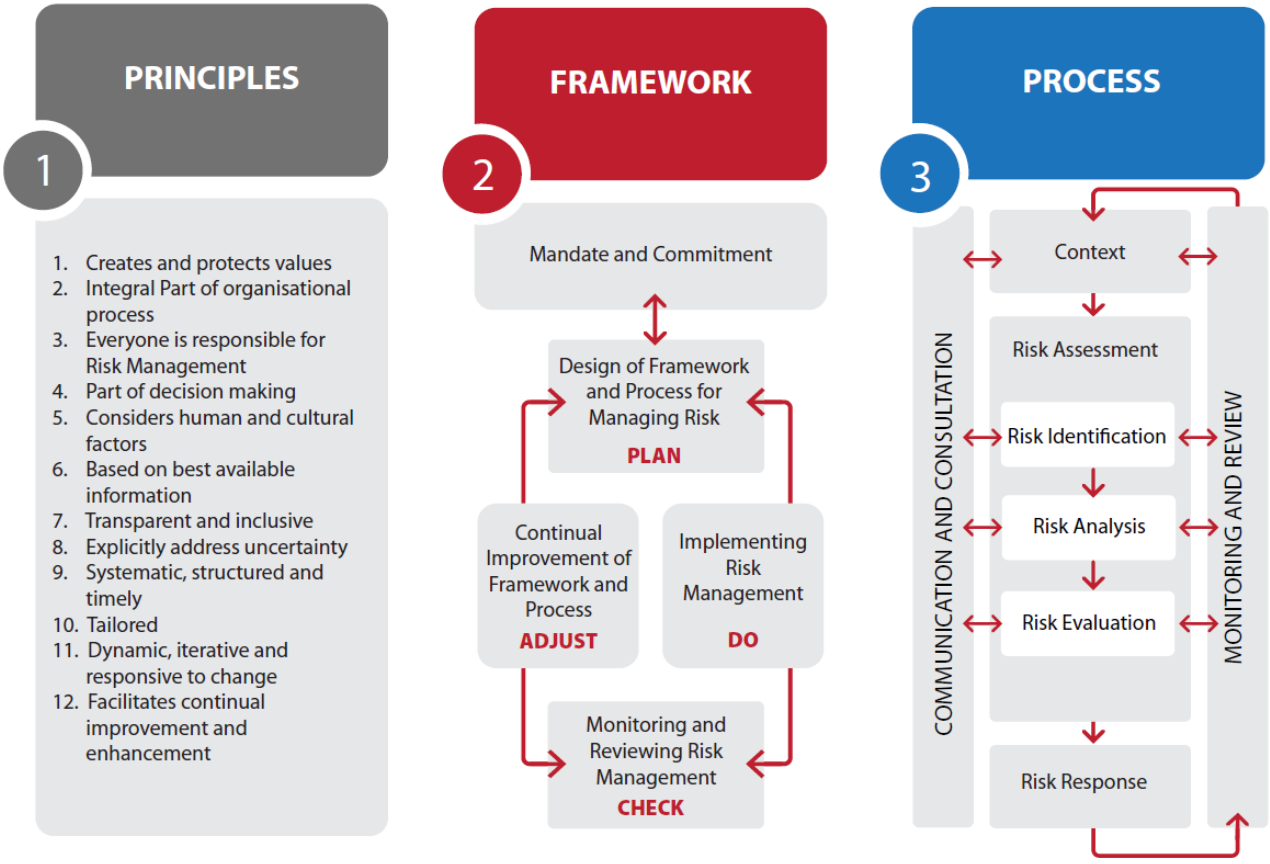


Figure 1: Risk Management Approach

Risk Management Principles

The effective implementation of risk management requires those responsible for managing risk to exhibit good sense and sound judgement when approaching the overall challenge of managing the organisation's risks. Various sets of principles exist; Imperial has adopted a set of general principles for risk management based on the ISO31000 in its vision of maintaining a world class risk management process.

These principles are to be complied with at all levels within the group for risk management to be effective and are documented under **section 6** of this framework.

Risk Management Framework
Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

The foundations include the policy, objectives, mandate and commitment to manage risk. The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. The risk management framework is embedded within the organization's overall strategic and operational policies and practices. **The risk management framework adopts the following structure**:

Table 1: Risk Management Framework Structure

Structure	Source/Reference	Responsibility/Owner	Frequency
Plan: is to establish the risk management framework	Risk Management Framework	• Chief Risk Officer • Group Risk Management Committee	Annual
Do: is to implement and operate it	• Risk Management Policy • Risk Implementation Plan	• All employees • Group Risk Management Committee	Continuously
Check: is to monitor and review is effectiveness	• Management monitoring and reporting • Risk Management Committee	• All employees • Risk Management Committee	Continuously
Adjust: is to maintain and continuously improve	Risk Management Framework	• All employees • Risk Management Committee	• Annually • Continuously

Risk Management Process
It is the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing context, identifying, analysing, evaluating, treating, monitoring and reviewing risk. This process as documented under **sections 7** of this framework serves as the core and heart of the process of ensuring effective enterprise wide risk management within the group.

All employees of the group at different levels are expected to take an active role in this process and therefore give full commitment in order to ensure that risk management is embedded in the group's culture and allows the organisation to realise the opportunities and benefits of effective risk management.

3. DEFINITIONS

This document documents the risk management framework of the IMPERIAL Group (IMPERIAL) as revised periodically and the process and procedures that shall be pursued to implement the framework. The terminology used through-out the document is defined under **Table 2**.

Table 2: Definitions

Term/Acronym	Definition
Group	Group" The Imperial Holdings Limited group of companies. This includes divisions, subsidiaries, joint ventures or any other entities where Imperial exercises control.
Risks	Risks are defined as the effect of uncertainty on the achievement of IMPERIAL's business objectives. A missed opportunity to enhance the efficiency, effectiveness and economy of IMPERIAL's performance shall also be construed as a risk.
Risk Management	Risk management are co-ordinated activities to direct and control IMPERIAL with regard to risk. It is designed to identify potential events that may affect the business and to manage risks to be within IMPERIAL's risk tolerance, to provide reasonable assurance regarding the achievement of IMPERIAL's objectives.
Risk Management Process	The Risk Management Process entails the planning, arranging and controlling of activities and resources to minimise the negative impacts of all risks to levels that can be tolerated by stakeholders whom the board has identified as relevant to the business of the company, as well as to optimise the opportunities, or positive impacts, of all risks
Risk Appetite	The level of residual risk that the company is prepared or willing to accept without further mitigation action being put in place, or the amount of risk company is willing to accept in pursuit of value.
Risk Response	It is a process undertaken to modify risk.
Risk Tolerance	The organisation's or stakeholders' readiness to bear the risk after risk response in order to achieve its objectives.
Risk-bearing capacity	It is the maximum financial loss that can be borne in the medium term without the organization having to change its strategic plans or financing requirements.
Risk Assessment	Overall process of risk identification, risk quantification and risk evaluation in order to identify potential opportunities or minimise loss
Control	A measure that is modifying risk.
Likelihood	The chance of something happening.
Impact (Consequence)	The outcome of an event affecting objectives. Consequences can be expressed qualitatively or quantitatively.
Risk Register	Record of information about identified risks.
Residual Risk	Risk remaining after risk treatment.
Risk Management Framework	Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. The foundations include the policy, objectives, mandate and commitment to manage risk. The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. The risk management framework is embedded within the organization's overall strategic and operational policies and practices.
Cross Functional Risk	Risks that transpire in a number of business units i.e. cross cutting or transversal risks.

Term/Acronym	Definition
Risk Communication	Exchange or sharing of information about risk between the decision-maker and other stakeholders. The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk

4. ESTABLISHING THE CONTEXT

4.1. Understand the organisation's operating model

The first step in risk management is defining the objectives that the organisation wants to achieve, how it intends to achieve these objectives (the operating model) and what might get in the way of achieving them (risks). It should describe as far as possible how the organisation actually reaches these objectives according to the following aspects:

- Operational activities
- Management systems
- Compliance, governance and management functions
- Services and/or products
- Strategic partnerships
- Supply chain
- Relationships with external stakeholders

4.2. Understand the external context

The external context entails the external environment in which the organisation seeks to achieve its objectives and over which it has no direct influence. **The following procedures should be followed:**

- Depending on the level at which the risk management process is being applied, identify the strengths, weaknesses, opportunities and threats.
- Perform an environmental PESTEL scan (Political, Economic, Social, Technological, Environmental and Legal) whether international, national, regional or local
- Establish the objectives and strategies to which the risk management process is being applied.
- Identify the key drivers and trends that influence the objectives of the organisation
- Effective external communication and consultation should take place throughout the risk management process to ensure that all the stakeholders have been identified and their interests considered

4.3. Understand the internal context

The internal context is the environment in which the organisation seeks to achieve its objectives. These factors lie wholly or mostly within the organisation's decision making capacity and the organisation can thus influence directly. **The following procedures should be followed:**

- Gain an understanding of the internal drivers that shape the organisation's ability and capacity to reach its objectives. Refer **Annexure A** for a list of factors to consider.

4.4. Apply the risk management process and determine internal risk thresholds

The organisation's risk management processes should be applied to identify various risks that the organisation must address and allow the executive leadership to establish the following internal risk parameters the organisation should follow:

- Risk appetite
- Risk tolerance
- Risk-bearing capacity

5. MANDATE AND COMMITTMENT

5.1. Our risk culture

5.1.1. The board is responsible for the governance of risk within Imperial and is fully committed to ensuring that risk management formal processes are implemented to ensure that risks facing the company are managed effective.

5.1.2. The Board of IMPERIAL along with its Executive and Management recognises that risk management is a critical management tool for ensuring that IMPERIAL achieves its objectives.

5.1.3. The board hereby appoint a risk committee to review the risk management progress and maturity of the company, the effectiveness of risk management activities, the key risks facing the company and the responses to address these key risks.

5.1.4. IMPERIAL commits itself to establishing, implementing and maintaining a systematic, comprehensive and robust system of risk management. Such commitment is motivated not only by the need to comply with the relevant legislative prescripts and recommended guidance but also by the desire to optimise the benefits of risk management for improved company's performance, effective and efficient service delivery.

5.1.5. The board commits to an annual review of the Risk Management Framework as part of its process of ensuring continuous improvement of the framework and the effectiveness of the risk management process.

5.2. Mandate

5.2.1. Risk management policy

The Risk Management Policy for Imperial is an overarching policy for risk management throughout the group and this is documented under **sections 7** of this document.

5.2.2. Roles and responsibilities

In order to ensure that there is accountability, authority and appropriate competence for managing risk throughout the group, Imperial identified the following:

- Roles and responsibilities at all levels within the group. Refer **Annexure B.**
- Performance measurement metrics to evaluate the effectiveness of the risk management process, refer **Annexure C.**
- External and internal reporting and escalation processes, refer **Annexure D**.

5.2.3. Roles of internal audit function in risk management

- Internal Audit as an independent assurance provider, are to perform the following:
  - Review the efficacy of the overall system of risk management annually.
  - Review the adequacy, effectiveness and economy of controls introduced to mitigate risks as part of their internal audit coverage plan.
- Internal audit function will have unrestricted access to the risk management function and may carry out any work necessary to assist the board and executive management in assessing the effectiveness of the risk management process.
- Risk profiles developed as part of the risk management process should form input in the internal audit process and consideration of internal audit work.

5.2.4. Combined assurance model

- A combined assurance model should be used to coordinate and optimise the extent of assurance coverage from different providers regarding the various risks that might affect the company.
- The risk management committee is to ensure the appropriateness of the combined assurance model.

5.3. Commitment

Each individual in the company should understand and commit to meeting the specific risk management responsibilities that are commensurate with their positions. In order to strengthen commitment, Imperial has identified specific responsibilities under **Annexure B** that are to be fulfilled by all levels within the group.

6. PRINCIPLES OF RISK MANAGEMENT

6.1. Risk management creates and protects value

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

6.2. Risk management is an integral part of all organizational processes

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

6.3. Everybody in an organisation is responsible for risk management

Every individual member of an organisation, from executive director to the most junior employee is responsible for managing the elements of risk in their given sphere of influence.

6.4. Risk management is part of decision making

Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action and risk management principles should be applied across the entire organisation, at every level and opportunity.

6.5. Risk management takes human and cultural factors into account

Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives. The values that people place on different risks influence decision making and should be investigated and brought to light as explicitly as possible, wherever feasible.

6.6. Risk management is based on the best available information

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

6.7. Risk management is inclusive of all stakeholders

Appropriate and timely involvement of external stakeholders ensure that risk management remains relevant, by incorporating external forces that influence the organisation’s ability to achieve its objectives.

6.8. Risk management explicitly addresses uncertainty

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

6.9. Risk management is systematic, structured and timely

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

6.10. Risk management is tailored to the organisation

Risk management is aligned with the organization's own unique external and internal context and risk profile.

6.11. Risk management is dynamic, iterative and responsive to change

Good risk management is sensitive and responsive to changes in the organisation's context and environment. It should continuously adapt to take account of changing risks, through regular reviews and inclusion of emerging best practices.

6.12. Risk management facilitates continual improvement of the organization

Effective identification and management of risks allows an organisation to identify systematic improvements to its business and operating model. This is an iterative process in parallel with the maturation of the risk management framework itself.

7. RISK MANAGEMENT PROCESS

7.1. COMMUNICATION AND CONSULTATION

A risk communication and consultation strategy should be developed at the beginning of the risk management process. The leadership and management teams should also communicate and consult with external and internal stakeholders at every step of this process. The communication and consultation taking place should be truthful, relevant, accurate and understandable and must take into account confidentiality and person integrity.

To successfully obtain all the relevant information and in a timely manner, it is critical that a communication process should be structured to identify who (internally and externally) should receive what information, to generate the information required and to communicate it on time and in an effective manner. A consultative approach should:

- Help describe the context properly
- Ensure that stakeholders are thoroughly and appropriately identified.
- Lead to cross-functional cohesion during the analysis of risks.
- Ensure that different viewpoints are considered while defining the risk criteria, and evaluating the risks.
- Help obtain backing from leadership and other stakeholders for the risk response plan.
- Support change management actions if the risk management process recommends any organisational changes.
- Lead to improvement of the external and internal risk communication and consultation strategy over time.

7.2. RISK ASSESSMENTS

7.2.1. Risk identification

This process endeavours to provide reasonable assurance that all key risks that may affect or hinder the organisation from achieving its objectives are discovered for assessment. The following should be taken into consideration during this phase:

- Risk identification should be based on information gathered from establishment of the context (i.e. this should be the most reliable and robust data available).
- Risk identification should be undertaken by people with the appropriate knowledge and skills to identify risk.
- There are three basic approaches that can be adopted in identifying risk:
  - **Quantitative methods**
    This involves for example the accumulation and development of relevant historical or predictive data sets
  - **Qualitative methods**
    This involves use of but is not limited to market research, surveys, questionnaires, risk workshops

- **Semi-quantitative methods**
  This is the use of a combination of quantitative and qualitative methods.

- The risks identified are then documented in risk registers for continuous assessment and monitoring.

7.2.1.1. Categories/sources of risks that can be utilised to identify risk: Annex B

In identifying risk, the following sources can be used to ensure consistency or standardisation:

- External (using models such as SWOT analysis, PESTEL analysis)
- Operations (business process level risks, risk registers, business continuity plans)
- Information Technology (trends in technology)
- Strategic Information (strategic risk registers, competitor analysis, market trend analysis)
- Operational Information (audits, internal questionnaires, sales performance reports)
- Financial Information (financial reports, budgets)

7.2.1.2. Techniques that may be used to identify risk:

A range of tools can be used to identify risk at the various levels of the organisation. These include but are not limited to the following:

- SWOT analysis
- Scenario planning
- Peer group benchmarking
- Workshops
- Interview and focus group discussion
- Brainstorming
- Incidence analyses
- Questionnaires and surveys
- Flow charting and system analysis
- Decision trees
- Audit reports (internal, quality, compliance, external etc.)

7.2.1.3. Key questions in risk identification

- What could prevent the achievement of objectives?
- When, where, why and how are the risks likely to occur, and who might be involved?
- What is the source/category of each risk?
- What resources are needed?
- What are the stakeholders' expectations?

7.2.1.4. Procedures of risk identification

- Confirm the division, department, process or project's objectives
- Determine the most appropriate method of identifying risks, more than one technique can be used
- Identify all the root causes/sources of those situations, trends, events or circumstances (risks) that may have an impact on the objectives
- Identifying areas of opportunities
- Capture all the information on a risk register

7.2.2. Risk analysis

Risk analysis involves developing an understanding of the risk. The causes and sources (both positive and negative consequences) and the likelihood that those consequences can occur taking into account the controls currently in place to mitigate the risk.

7.2.2.1. Key considerations in risks analysis

- What is the potential likelihood or consequence (i.e. characteristics) of the risk occurring after taking into account the existing/current controls?
- What are the potential impacts of the risks if they do occur taking into account the existing/current controls?
- What factors might increase or decrease risk?

Controls identification step involves obtaining an understanding of the existing controls (i.e. systems, procedures, processes, policies etc) currently in place to treat the risks. It further involves considering effectiveness and adequacy of those controls to determine the residual risk.

7.2.2.2. Key considerations in control identification

- What are the current controls which may prevent, detect or correct the consequences of potential or undesirable risks/events?
- How adequate are the current controls?
- Are there any opportunities or areas of improvement?

7.2.2.3. Procedures of control identification

Determine the current control or controls in place to address the risk

7.2.2.4. Procedures of risk analysis

For each risk identified the following should be done:

- Determine the impact and likelihood for the risk.
- Risk rating – this is a function of completing impact and likelihood, i.e.
- Determine the rating of risk

7.2.2.4.1. Analysing impact/consequences

The consequences of risk are the impacts of varying magnitude across a different range of different objectives. When analysing the consequences of a risk, the organisation should consider severity of its effects, where appropriate, on at least the following:

- Human and environmental well-being
- Financial stability of the organisation/activity
- Operational performance
- Governance and compliance
- Security, including financial, physical and IT
- Preservation of assets

7.2.2.4.2. Analysing likelihood and estimating probability

Several approaches may be used to estimate the probability (quantitative) or likelihood (qualitative) of an event. Expert judgement may be vital to ensure that the outputs of any modelling or extrapolative process are reasonable and robust. The various tools or techniques described can be classified according to the following types:

- **Extrapolation of historical data** – this is used to identify the root causes of events or situations that occurred in the past. The fundamental assumption is

that events will recur under similar circumstances and can therefore be reliably predicted. i.e. operational situations.

- **Probability modelling** – this is direct relevant information regarding a particular risk or situation may be inadequate or not exist. In this case, an appropriate model will be created based on the theoretical behaviour of the system to predict future events and situations. These may be calibrated using data from similar system, organisation, technologies or operational experience or externally published or available data.

NB. The fact that a predictive model may not incorporate system wide influences should be taken into account when evaluating risk using such a model.

- **Expert judgement** – the opinion of industry experts and specialists is regarded as invaluable and should be considered in estimating the likelihood of an event.

In order to ensure consistency and standard rating approach throughout the group, a Risk Rating Matrix has been developed to assist with the rating of impact, likelihood and determining the overall inherent and residual risk, refer **Annexure E**. This matrix should be applied as follows:

- The probability and consequences should be combined according to established criteria and categorisation of the risk. i.e. high, medium and low or applicable numerical rating scale that can be used to estimate the level of risk according to previously agreed formula or calculations.
- The calculated levels of risk will remain an estimate due to the fact that they are influenced by a range of factors which may include human bias in the valuation of the risk or even biases in the design of the risk scoring criteria of automated systems used.
- The level of accuracy and detail should not be advertently ascribed to the result but rather good sound judgement must be applied to the models used and a rational decision must be made based on information available.
- The insight and experience of specialists may be used to check the outputs of any modelling process used to make sure it makes sense.

7.2.2.5. Completing the risk register

All risks that have been fully described should be documented in the risk register or similar structure. This register should also include the risk responses that have been enacted and relevant controls that have been implemented to manage the risk, refer **Annexure F.**

7.2.3. Risk evaluation

The final step in the risk management process is to develop an understanding of the risk. This will involve consideration of the causes and sources of the risk (positive and negative consequences and the likelihood of occurrence. An evaluation should be performed by doing the following:

- Comparing the risk against pre-determined criteria, thus specifying the significance of the risk to the organisation's objectives.
- All available information should be used in the evaluation stage including the relevant risk thresholds the organisation has specified in terms of legal, ethical, financial or other constraints.
- The decisions to be taken at this stage should consider the following:
  - The priority of risk and the urgency with which it should be addressed
  - Any risk can be accepted only with the implementation of specific responses without further action, such as very low probability and very low impact
  - Immediate decisions to avoid risks that breach specific thresholds
- Where risks are accepted "as is" it is important to note any factors that may escalate them upwards and hence require a response. These should be documented and tracked so that the risk does not escalate without an appropriate response.

The risks identified are then prioritised so that resources may be allocated appropriately. Any residual risk that remains after taking into account the existing controls will subsequently be rated as critical, high, moderate or low depending on the probability of the risk occurring as per the risk assessment tables. [**Annexure G]**

7.2.4. Opportunity Assessment

The same methodology used to identify and evaluate risks should be used to collect business insights regarding opportunities. This assessment process should not be limited to the identification of positive aspects relating to threats. Changing business environments create both risks and opportunities to innovate or adapt the organisation to the new playing field.

Opportunities identified by top management should be communicated, validated and responded to by all the employees across the organisation (top-down). Employees should also be empowered to communicate their ideas for improvement, adaptation and innovation upwards through management structure of the organisation (bottom-up).

A wide range of opportunities should therefore be considered but not limited to the following:

- Create a new process, product or service
- Improve existing businesses, products or services
- Broaden the range of products or services (geography, target)
- Use of excess resources
- Generated from changing stakeholder demands.
- Reduce the use of various resources, including financial or natural
- Improve the reputation and trust which stakeholders have in the organisation.
- Improve health and safety performance.
- Build or strengthen alliances, partnerships and relationships with both new and existing stakeholders.

Several of these can be related to risk, such as reputational risk that is linked to opportunities to improve the organisation's public image.

7.3. RISK RESPONSE

Once risks have been identified, assessed and evaluated there will be enough information to begin the process of responding to the risks. **The following procedures should be followed:**

- Assessment of the current or proposed risk response for suitability and effectiveness
- Determination of whether the residual risk levels are acceptable and if not
- Consideration of what additional responses maybe required to ensure that risks are managed within the risk tolerance and risk appetite of the company.
- Determination of the cost-to-benefit ratio – balancing the effort and expenditure required with the benefits
- A response plan should be documented and clearly identify the order in which individual responses should be implemented, refer **Annexure G**.
- Assessment of secondary risks arising from the choice of response and inclusion into the risk response plan. The relationship between the original and knock-on risks should be identified and maintained.
- Monitoring of the risk response plan to ensure that the measures remain effective
- Integration of the risk response plan with other relevant management systems in the organisation and communication with the various relevant stakeholders

There are various strategies (i.e. **Table 3**) for treating risks in IMPERIAL environment. These risk responses options are neither mutually exclusive nor suitable in all circumstances. It is therefore required for responsible person to determine the most appropriate treatment option for each risk.

Table 3: Risk responses

Risk Responses available	Detail
Accept or Tolerate the risk	Take no action to further reduce or increase the risks that fall within acceptable tolerance parameters. This may occur if or when the management team believes that the costs of responding to the risk do not create or protect sufficient value to justify additional effort.
Avoid the risk	Completely avoid this specific risk by deciding not to pursue or continue the activity that gives rise to the risk exposure.
Remove the source of the risk	Where possible to remove the source of risk from the activity through disposal, substitution and/or replacement.
Changing the likelihood	Where possible adjust either the operating processes or human behaviour that give rise to a particular risk by improving or implementing preventative controls.
Changing the consequence	This involves a detailed understanding of the consequences and who experiences them, and implementation of corrective controls to alter the severity of a particular risk.
Transfer the risk	Transfer the risk (at a price) to another party or parties. This is entails the transfer of responsibility (but not accountability) for the activity that gives rise to the risk, in part or whole, to another party. For every risk to be transferred, the following should be done: • Risks should be allocated to the party which can exercise the most effective control over the risk. • Risk may also be transferred by insurance, legislation and administrative processes. • There should be proper communication to all relevant parties.
Exploit the opportunity	The allocation of additional resources to exploit and benefit from the uncertainty associated with positive risks.

7.4. MONITORING AND REVIEW

Monitoring and review activities should be undertaken to ensure that the risk management process actually works as set out according to the organisation's risk management framework, and that it happens at the appropriate level of cost and effort. These are an essential and integral step in the process for managing risk. It is necessary to monitor risks, the effectiveness of the plan, strategies and controls that have been set up to manage unacceptable risks.

Risks and the effectiveness of control measures need to be planned beforehand to ensure changing circumstances do not alter the risk priorities. The timing of the monitoring and review should be determined in terms of set intervals or impromptu or continous checking.

A risk management plan should be in place and must specify responsibilities for monitoring and evaluating which risk and must enable those responsible to reach the following goals:

- Designing and implementing effective (method-wise) and efficient (cost-wise and time-wise) risk responses.
- Improving the organisation's risk assessment over time as information comes to light.
- Analysing events as they happen (close calls as well) and learning from these events.
- Identifying changes, trends, successes and failures.
- Detecting changes in the organisation's external and internal contexts, which include changes to the risk criteria and the risk itself, leading to the revision of risk responses and priorities.
- Identifying any new or previously unrecognised risks.

The monitoring and review work should include planning, examining and evaluating, recording, communicating results and following up.

7.4.1. Planning the monitoring and review

Each monitoring activity should be properly planned, documented and should include:

- Established monitoring objectives and scope of work
- Background information obtained about the activities to be monitored.
- The resources (people and time) necessary to perform the monitoring should be determined.
- Identified and documented specific risks relating to the area concerned.
- Identified and documented existing controls in place to mitigate identified risks.
- Written monitoring program that responds to the risks identified or updated existing monitoring programs.
- Obtained approval of the monitoring work plan
- Regular update the progress on future controls to minimise the risk
- Risk must be the standing agenda item in the meetings
- All other updated risk information should be communicated to Risk Management

7.4.2. Examining and evaluating information

The responsible persons should collect, document, analyse and interpret the information gathered. The following process should be followed:

- A walkthrough of the activity should be performed and information collected on all matters related to the monitoring objectives and scope of work.
- Information obtained should be sufficient, competent, relevant and useful to provide a sound basis for monitoring findings and recommendations.
- Control operating effectiveness testing should be conducted.
- Monitoring issues identified should be documented with ratings.
- A close-out meeting should be held with management.

7.4.2.1. Key questions in monitoring and review

- Are the risk treatments effective in minimising the risks?
- Are the management controls adequate?
- Do the risk treatments comply with legal requirements, government and organisational policies including ethics and accountability?
- How can further improvements be made?

7.4.2.2. Procedures in monitoring and review

- A review process for the entire organisation shall be done annually, in a systematic and rotational basis. This will provide an opportunity to:
  - Determine whether each risk previously identified is still relevant to the organisation.
  - Review of the adequacy of:
    - assessments given to impact and likelihood for each risk;
    - the risk rating;
    - existing systems and controls to manage risk;
    - the residual risk rating; and
    - the treatment strategies which previously have been considered.
- The review process also provides the opportunity to determine if there are any new risks which should be included, and undertake the risk assessment process for these new risks.
- Internal Audit conducts a review of risk assessment and adopts a risk-based approach to all audits.
- The review by all relevant assurance bodies

7.4.3. Recording the risk management process

The results of the monitoring and reviewing risk should be recorded and reported on (externally and internally) in an appropriate manner. It should also serve as input during the cyclical review of the risk management framework.

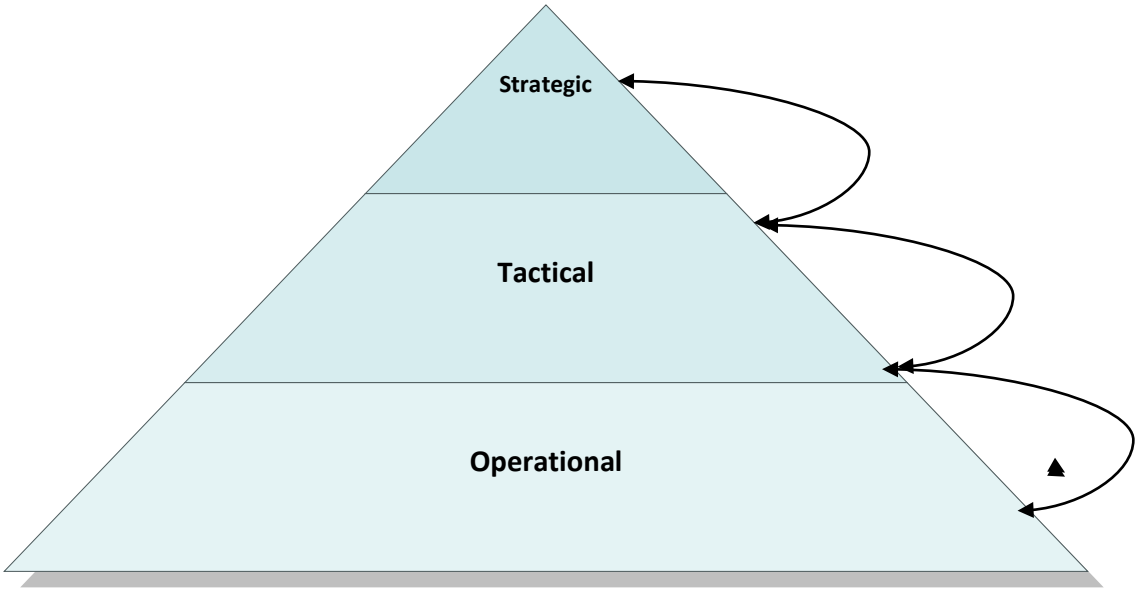
The following aspects should be taken into account:

- The cost and effort that creating and maintaining such records would entail.
- The legal, regulatory and operational requirements where records are concerned.
- How records would be accessed, how easy retrieval needs to be (backups included) and the type of storage media required.
- How long records should be retained.
- How sensitive is the information contained in the records.
- How reusing information would benefit management purposes.
- How the analysis of records could aid the organisation in its learning process.

7.4.4. Communicating results

The essence of risk reporting is that the right people at all levels (**Figure 2**) identified for Imperial) receive the right information at the right time. Risk reporting further entails reporting on the effectiveness of risk management processes within the company over the period concerned. Imperial has therefore identified the following reporting protocols:

- **Critical and high strategic risks** – these risks will be reported to the Risk committee after discussion with the Exco.
- **Critical and High tactical risks** – these risks will be reported to Executives and applicable Group Executives.
- **Critical and High operational risks** – these risks (status and treatment plans) will be reported to Executive.



- **Figure 2: Risk reporting protocols**

Responsible persons shall communicate the results through the issuing of monitoring reports and should:

- Prepare and issue a draft report
- Document the agreed management action plans
- Prepare and issue a final report

7.4.5. Follow-up

Responsible persons must follow up on reports to ascertain that appropriate action is taken after the findings and recommendations. It is vital to ensure that corrective action is taken and achieves the desired result, or that management has assumed the risk of not taking corrective action on reported findings.

8. MONITORING, REVIEW AND UPDATE OF THE FRAMEWORK

The Risk Management Committee assisted by the Chief Risk Officer is responsible for the monitoring, review and update of the risk management framework annually and as and when there are changes to the relevant guidelines which affect this framework.

9. ROLES AND RESPONSIBILITIES

In order for Risk Management to be effective throughout the organisation, each role player is required to fulfil specific responsibilities all aimed at embedding risk management practices into everyday business. Refer to Annexure B: Roles and Responsibilities for a detail of the different roles and responsibilities assigned to each player.

10. REFERENCE

Enterprise Risk Management – Integrated Framework - COSO
AS/NZS 4360 – 2004: Australian / New Zealand Standard: Risk Management
ISO 31000:2009(E) / SANS 31000:2009 Edition 1: Risk management — Principles and guidelines
ISO GUIDE 73:2009 Edition 1 / ARP 070:2009 Edition 2: Risk management — Vocabulary
Institute of Risk Management – South Africa – Guideline to Risk Management

Annexure A: Levels and Categories [List of factors to consider]

Levels	Definition includes
Strategic	Risk that affects the achievement of IMPERIAL's strategic objectives.
Tactical	Risk that affects the achievement of a divisional or entity objectives
Operational	Risk that affects management ongoing processes
Project	Risk that may cause a failure to meet the project's objectives" or limits the achievement of the objectives as defined at the outset of the project

Category	Sub-category
External	Competitor
	Catastrophic loss
	Political
	Stakeholder relations
	Legal
	Regulatory
	Industry
	Capital availability
	Financial Markets
Operations	Customer Satisfaction
	Human resources
	Product development
	Efficiency
	Performance Gap
	Cycle Time
	Sourcing
	Obsolescence Shrinkage
	Compliance
	Business Interruption
	Product/ Service Failure
	Environmental
	Health and Safety
	Brand Name erosion
Empowerment	Leadership
	Authority
	Outsourcing
	Performance Incentives
	Culture
	Communications
Information Technology	Relevance
	Integrity
	Access
	Availability
	Infrastructure
Integrity	Management Fraud
	Employee Fraud
	Illegal Acts
	Unauthorised use

Category	Sub-category
	Reputation
Financial	Interest rate
	Currency
	Equity
	Financial Instrument
	Cash Flow
	Opportunity cost
	Concentration
	Credit default
	Settlement

Strategic Information	Environmental Scan
	Business Portfolio
	Valuation
	Performance Measurement
	Organisation structure
	Resource allocation
	Planning
	Life cycle
Operational Information	Pricing
	Contract commitment
	Performance measurement
	Alignment
	Regulatory reporting
Financial Information	Budget and Planning
	Accounting information
	Financial Reporting Evaluation
	Taxation
	Pension Fund
	Investment Evaluation
	Regulatory Reporting

Annexure B: Roles and Responsibilities

Role player	Responsibility
CEO / Board	• Communicate IMPERIAL's philosophy, attitude and approach to risk management at all levels within. • Take the lead in promoting an organisational culture that encourages and supports risk management by maintaining visibility in supporting risk management initiatives • Ensure that resources are allocated to risk management. • Determine the strategic approach to risk and set the risk appetite.
Group Risk Executive & Divisional Risk Managers	• Monitor and report on the status and progress of risk management within IMPERIAL. • Support the chief executive officer and risk management initiative through support and guidance on matters pertaining to risk management. • Facilitating the identification and assessment of risks in IMPERIAL. • Providing on- going support and guidance on risk management across all levels of IMPERIAL. • Undertake initiatives that aim to create and enhance risk management awareness throughout IMPERIAL. • Support implementation of the Risk Escalation and Reporting Procedure throughout the group by providing advice and guidance, as appropriate. • Regular maintenance of the Risk Register on behalf of the risk committee.
Group Risk Committee	• Provide an independent review on risk management process and the significant risks facing the company on behalf of the board. • The results of this committee's work must be reported to, and considered by, the board.
Group Internal Audit	• Review the efficacy of the overall system of risk management. • Review the adequacy, effectiveness and economy of controls introduced to mitigate risks.
Management	• Management is responsible for the implementation of risk management systems within their line functions. • In essence, managers are the actual managers of risk and shall ensure that risk management is incorporated into the activities within their areas of responsibility. • Manage the risk escalation process and maintain their respective risk registers.
All staff	• Every individual member of an organisation, is responsible for managing the elements of risk in their given sphere of influence. • Have a responsibility to familiarise themselves with the contents of this procedure and comply with it accordingly, through identification of risks.

Annexure C: Performance measurement metrics

Note - Currently under review – as need to align to divisional Performance management systems – with defined key performance areas and indicators

Annexure D: Escalation process

Risk Rating	Reporting Level	
Low	Company Risk Register	Adequately Controlled
Moderate	Divisional Risk Register	Adequately Controlled
High	Divisional Risk Register	Inadequately Controlled
Critical	Group Risk Register	Inadequately Controlled

Level of risk	Responsibility
Low	Managed at a departmental/company level. Local management to determine and develop risk treatment plans or to manage through routine procedures; and include all risk details in the company risk register.
Moderate	Managed at departmental/company level, unless escalated to divisional level. This will be considered for escalation to the Finance and Risk Review Committee.
High	Managed at divisional level, unless escalated to group level. This will be escalated to the Finance and Risk Review Committee.
Critical	Managed at divisional level. Risk Leads consider escalation and review at Risk Management Committee where consideration is given to placing the risk on the Key Issues Log. Consider bringing risks, as appropriate, to the attention of the Board

Annexure E: Risk rating matrix

RISK IMPACT DEFINITIONS

IMPACT		DESCRIPTION
1-NIL	**Low**	No impact on the organisation
2-NEGLIGIBLE		Negligible impact on the organisation (Consequences can be readily absorbed under normal operating conditions and will not affect achievement of objectives.)
3-MINOR		Minor impact on the organisation (Consequences can be readily absorbed under normal operating conditions and will have a minor effect on achievement of objectives.)
4-CONTAINABLE		Impact can be readily absorbed under normal operating conditions
5-SIGNIFICANT	**Medium**	Impact is can be absorbed, but management intervention is required.
6-MORE SIGNIFICANT		Impact can be contained, but significant management intervention is required.
7-VERY SIGNIFICANT	**High**	Impact that can be managed under supported operating conditions
8-SERIOUS		Event which will have a prolonged negative impact and extensive consequences
9-CRITICAL	**Critical**	Event which will have a prolonged negative impact and extensive consequences, beyond the company level.
10-CATASTROPHIC / FUNDAMENTAL		Impact with the potential to lead to the collapse of the organisation and is fundamental to the achievement of IH objectives.

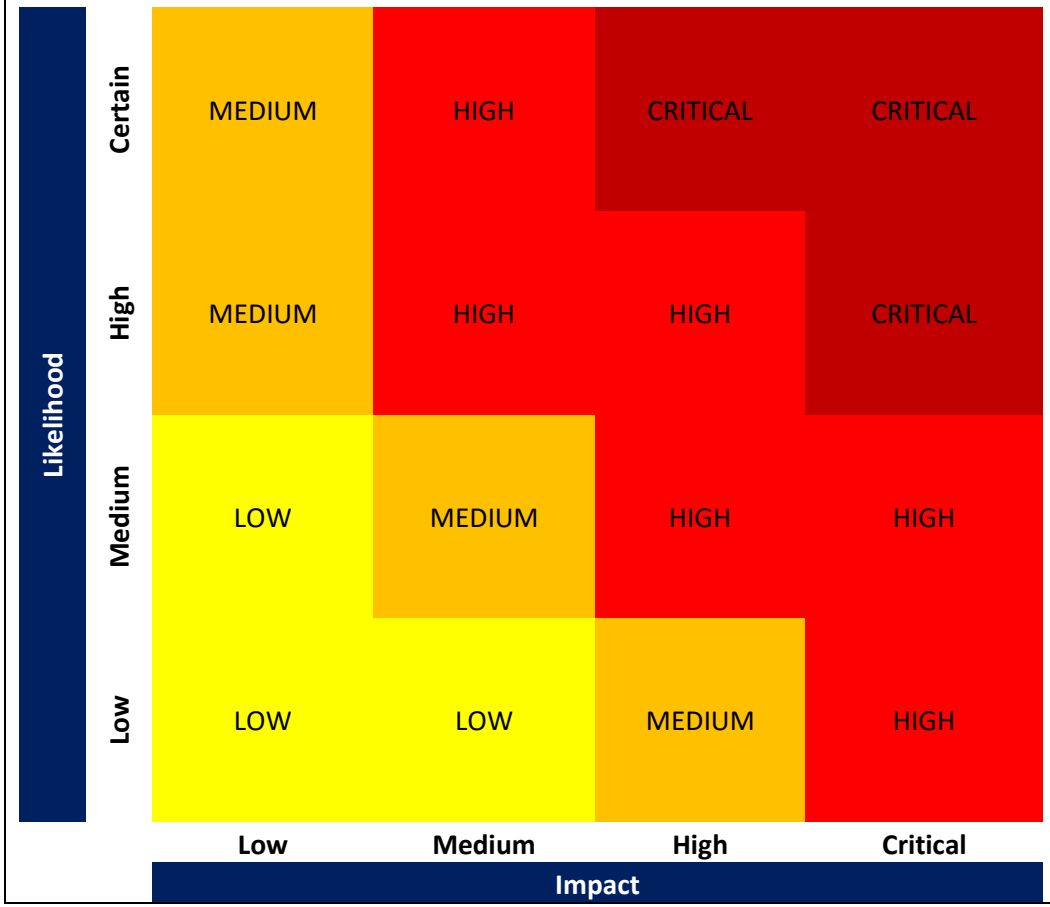
RISK LIKEHOOD DEFINITIONS

LIKELIHOOD		DESCRIPTION
1-NEGLIGIBLE	**Low**	Risk never happened in the industry or in a similar organisation, but could happen due to external factors.
2-RARE/REMOTE		Risk may occur only in exceptional circumstances.
3-EXTREMELY UNLIKELY		Extremely unlikely within the next 12 months, but the event could occur within a 3 year business cycle.
4-VERY UNLIKELY		Very unlikely within the next 12 months, but the event could occur within a 3 year business cycle.
5-UNLIKELY		Unlikely within the next 12 months, but the event could occur within a 3 year business cycle.
6-MODERATE/FEASIBLE	**Medium**	Unlikely within the next 12 months, but confidently expected within a 3 year business cycle.
7-PROBABLE		Probable within the current financial period. The risk should occur within a 2 year period.
8-EXPECTED/LIKELY	**High**	Expected within the current financial period. The risk will probably occur in the next 12 months.
9-CONFIDENTLY EXPECTED	**Certain**	Confidently expected in this financial period.
10-CERTAIN		The risk will happen in this financial period.

Note: Risk Scoring is not intended to be precise mathematical measures of risk, but is useful when prioritising control measures for the treatment of different risks.

Risk Prioritisation Map

The next step involves combining the Impact and Likelihood rating to determine the inherent risk (i.e. risk without controls) rating and the residual risk (i.e. risk after taking into account the current controls) to determine the risk priority rating, as shown below.



Combined Risk Rating

Risk Rating	Risk Rating Definitions
Critical	Risk with potential to lead to collapse of business and is fundamental to the achievement of objectives (this action may neutralise the objectives and functions of the department/operation resulting in serious damage to key operations)
High	Risk which can be endured but which may have a prolonged negative impact and extensive consequences (this action may disrupt the objectives and functions resulting in disruption of services and relationships in the department/operation with clients, partners and other stakeholders.)
Moderate	The risk may harm the objectives and functions resulting in loss of effectiveness and reputation to the department/operation (Major events, which can be managed but requires additional resources and management effort).
Low	Event, which can be managed under normal operating conditions (will affect achievement of objectives or frustrate operations such that achievement of objectives is affected.)

In order to apply the above matrix, determine the level of likelihood and Impact as applicable definitions under **Annexure E**, then where the two points meet gives the combined rating. Reference can then be made to **Combined Risk Rating table** to establish the definition of the combined rating.	

Annexure F: Risk Register

Objective (A)	Categories of risks (B)	Risk name (C)	Risk description (D)	Risk owner	Current control (corrective /detective/preventive)	Impact	likelihood	Risk rating	Risk strategy	Future controls	Task owner	Due date

Annexure G: Risk Response plan

Risk	likelihood	impact	Current control	Response chosen (B)	Secondary risk, possible benefits and effects on stakeholders (C)	Responsibility: • Implementation • Approval (D)	Proposed Actions	Required resources	Contingencies, performance measures and constrains	Reporting and monitoring requirements	Timing and schedule