# Introduction

## Purpose

The purpose of this procedure is to provide SAHMRI staff with guidance on how to apply consistent and comprehensive risk assessments. This procedure also provides information on how to identify, analyse, evaluate and treat risks based on the **Risk Management Policy (POL 0029).** In addition, it identifies other key activities needed for an effective risk management approach. The risk management process described in this procedure aligns with the standard for **Risk Management, AS/NZS ISO 31000:2009**. It also refers to the **ICH Harmonised Tripartite Guideline- Quality Risk Management (Q9) 2005, PICS Guide to the Manufacturing Practice for Medical Products, Part1 and OECD Principles on GLP** for GXP (GLP, GCP, GMP) activities undertaken at SAHMRI.

The objectives of a risk management framework are to:

* Provide a systematic approach to the early identification and management of risks;
* Provide consistent risk assessment criteria;
* Make available accurate and concise risk information that informs decision making including strategic direction;
* Adopt risk treatment strategies that are cost effective and efficient in reducing risk to an acceptable level; and
* Monitor and review risk levels to ensure that risk exposure remains within an acceptable level.

## Scope

This document sets out:

* The procedures followed by SAHMRI to manage risk
* The metrics used by SAHMRI to assess and manage risk
* The tools used to record and report risks

# Definitions

Refer to the **Risk Policy (POL 0029)**

# Responsibilities

Risk management is a responsibility of all members of SAHMRI community with specific duties being allocated to different groups and levels of the organisation. It is important to have complete and current risk information available as this will assist SAHMRI to make more informed decisions around both strategic direction and operational objectives.

The SAHMRI Board reviews the risk report endorsed by the Audit, Finance and Risk Committee.

The Chief Risk Officer (CRO) is tasked with presenting any new corporate risks, or escalating if necessary any current risks, to the Audit, Finance and Risk Committee for consideration.

The role of the Risk Coordinator is to prepare and draft the corporate risk reports for presentation to the Audit, Finance and Risk Committee.

Responsible staff must report to the CRO all High and Extreme residual risks.

# Procedure

## Benefits of Risk Management

SAHMRI considered and manages risks as well as opportunities.

Risks are managed with a focus on decreasing their likelihood, and minimising their impact if they should occur. Opportunities are managed to increase their likelihood, and to maximise their benefits if they should occur. This ensures a highly comprehensive approach to risk.

Where risks and opportunities overlap, the best appropriate method for managing them shall be ascertained, given the situation at hand.

Application of a consistent and comprehensive risk management (including opportunities) process will:

* Increase the likelihood of us achieving our strategic and business objectives;
* Encourage a high standard of accountability at all levels of the organisation;
* Support more effective decision making through better understanding of risk exposures;
* Create an environment that enables us to deliver timely services and meet performance objectives in an efficient and cost effective manner;
* Safeguard our assets – people, property and reputation; and
* Meet compliance and governance requirements.

## Relationship with Other Processes

Risk management is not a stand-alone discipline but requires integration with existing processes such as business planning and Internal Audit, in order to provide us with the greatest benefits.

The key processes with which risk alignment is necessary are:

* **Internal Audit** – Internal audit reviews the effectiveness of controls. Risk assessments conducted for each of the critical processes and projects help to identify and review auditing priorities.
* **Legal and Regulatory Compliance Framework** consists of the policies, processes, tools and structures that help to identify and manage the legal risks around meeting our objectives. Refer to the **Legal and Regulatory Compliance Framework** (DOC 0065).
* **Planning (including budget)** – Identifying risk during the business planning process allows us to set realistic delivery timelines for strategies/ activities or to choose to remove a strategy/ activity if the associated risks are too high or unmanageable. The impact of changing risk levels over the year can then be mapped to the relevant objective, enabling us to conduct more timely expectation management with key stakeholders.
* **Performance Management** – All risk responsibilities, whether a general responsibility to use the risk management process or specific responsibilities such as risk ownership and implementation of risk treatments should be included within the relevant individual or departmental performance plans.

## What to review?

Risks Analysis at all levels of the organisation should be conducted regularly for identified risks including:

* Making critical project related decisions
* Conducting day-to-day management including Work Health and Safety (WHS) considerations
* Establishing new activity or process, and
* Making purchases critical to Department/ Section operations.

The steps of the risk management process are described below in further detail.

## Key Risk Process Steps

The process for managing SAHMRI’s risks involves a number of key steps and includes feedback through monitoring, review, communication and consultation processes:

* Establish the context
* Identify risks
* Analyse risks
* Evaluate risks
* Treat risks
* Monitor and review
* Communicate and consult

It is important to follow this process when conducting risk management as this ensures that SAHMRI approach to risk management is both comprehensive and consistent.

**4.4.1 Risk Identification**

Risks are identified as part of the process to determine and understand external and internal issues that are relevant to SAHMRI strategic direction. This is undertaken by identifying and documenting the context of the risks including activities, products or services and the associated with them risks. Identification should include all risks which impact the achievement of the objectives.

Comprehensive identification of risks is important because a potential risk not identified at this stage will not be included in further analysis. There are many methods for identifying risk, including facilitated brainstorming, interviews, questionnaires, workshops and shelf data analysis.

As part of SAHMRI’s risk identification process, all risks are assigned to one of risk categories as set out in Appendix 1.

**4.4.2 Risk Analysis**

Establishing likelihood and consequence

Once all risks have been identified they are analysed in terms of how likely the risk event is to occur (Likelihood) and the possible magnitude of the risk event (Consequence), using established criteria. These criteria are documented in the rating scales developed by SAHMRI (see Appendix1)

**Likelihood** is rated from Rare to Certain based on an assessment of the risk event manifesting in a one year period.

**Consequence** is rated giving consideration to the impact on the organisation should the risk manifest from Insignificant to Catastrophic. It should be noted that Consequence is rated independently of the Likelihood of a risk manifesting.

From this analysis the level of **Inherent Risk** can be determined. It is important to note that the Inherent Risk analysis is determined in the absence of any controls which may already be in place.

Establishing the inherent risk rating

The Inherent Risk rating for each risk is calculated by using the Likelihood and Consequence response scores and the SAHMRI’s Risk Rating Matrix as set out in Appendix 1. The Matrix provides the following overall risk ratings:

* Extreme risk- immediate action required along with senior management commitment
* High risk- senior management attention and development of an action plan is required
* Medium risk- Management responsibility must be specified (i.e. accountability defined)
* Low risk- manage by routine procedures

**4.4.3 Risk Evaluation**

The purpose of the Risk Evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment as well as the priority for treatment implementation. The evaluation involves comparing the level of risk to the SAHMRI risk criteria. Based on this comparison the need for treatment can be considered.

**4.4.4 Risk Tolerance**

SAHMRI’s Risk Tolerance is to manage all risks to a risk level of medium or low. Accordingly, all Inherent Risks ranked as extreme or high require detailed analysis of controls and mitigating practices to determine the Residual Risk rating.

Consider any controls or mitigating activities that reduce the level of risk. These controls or mitigating activities need to be identified, documented and assessed based on criteria established by SAHMRI.

**4.4.5 Assessment of Controls**

In order to determine the extent to which controls/ treatment practices reduce the level of risk, it is necessary to consider their effectiveness in the context of:

* Design
* Communication
* Operation
* Application
* Documentation
* Defined responsibility and accountability
* Monitoring and review processes

SAHMRI’s internal audit process will provide required assurance in regards to the effectiveness of the assigned controls and implemented treatment plans. The identified controls are documented in the Risk Register (ref. Intelex System).

**4.4.6 Residual Risk Assessment**

Once controls have been identified and their effectiveness assessed, the risk is re-rated based on the SAHMRI Risk Matrix (Appendix 1.), i.e. determining the **Likelihood** and **Consequence**. At this stage however consideration is given to the effect of the controls in place in reducing the Likelihood or Consequence of the risk. This analysis is referred to as the **Residual Risk** assessment.

Any Residual Risks which remain rated as extreme or high require further consideration in terms of this Framework. As such it is necessary to consider options to treat these risks, evaluate the options and develop and document Risk Treatment action plans for implementation.

* + 1. **Risk Treatment**

Risk Treatment involves choosing the ways of modifying risks. The Risk Treatment options may include the following:

* Avoiding the risk
* Taking or increasing the risk in order to pursue an opportunity
* Removing the risk source
* Changing the Likelihood
* Changing the Consequence
* Sharing the risk with another party
* Retaining the risk by informed decision

# Monitor and Review

It is necessary to incorporate monitoring and review process into day- to- day operational and management activities in order to capture any new risks arising from changing circumstances. To achieve this SAHMRI employs the following practices:

* Risk monitoring and review takes place across the organisation on an ongoing basis. Frequency of risk monitoring:
* should be determined by the Responsible Manager and
* recorded in Risk Management application of the Intelex database
* may vary for various “Activities, Products or Services” however,
* should be appropriate to the type of risk, controls and treatments assigned and residual risk rating.
* New risks and changes to risks, risk ratings, controls or treatment plans are timely communicated to the Senior Manager or Head of the Department/Section for recording in the Risk Register

# Communicate and Consult

Communication and consultation are important elements during each step of the Risk Management process. Effective communication is essential to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which risk management decisions are made and why particular actions are required.

It is important that a communication approach recognises the need to promote risk management concepts across a broad spectrum of management and staff, from executive management to administrative and research staff.

SAHMRI seeks to achieve this by embedding the risk management processes in the regular business of the organisation and by including risk management on the agendas of existing committees and management teams. Communication is also recorded on the Intelex System through task and action notifications associated with the risk record.

# Associated Documents

## External

* AS/NZS ISO 31000:2009, Risk Management, Principles and Guidelines
* ICH Harmonised Tripartite Guideline- Quality Risk Management (Q9) 2005,
* PICS Guide to the Manufacturing Practice for Medical Products, Part1
* OECD Principles on GLP

## Internal

* PRO 0012, QA Program for SAHMRI
* PRO 0113, Internal Audits

## Appendices

* Appendix 1. Risk Rating Metrics

**Appendix 1. SAHMRI Risk Rating Metrics**

**Risk categories**

|  |  |
| --- | --- |
| **Category** | **Description** |
| Strategic | Risks that could have a significant effect on the ability of the organisation to meet one or more of its strategic goals |
| Financial | Risks that cash flows and funding are not managed cost-effectively to maximise availability of cash and funds and reduce uncertainty of funding, interest rate, credit and other financial risks |
| Operational | Non-compliance with or inability to adapt to changes in the regulatory environment, exposing the organisation to fines, penalties, potential loss of reputation or litigation |
| Research | Risk that the organisation’s management processes and infrastructure is ineffective or inefficient in enabling the organisation to deliver its research objectives |

**Risk Rating Criteria: Likelihood for SAHMRI**

|  |  |
| --- | --- |
| **Rating** | **Description** |
| Certain | The event will occur within the next 3 years |
| Probable | The event is likely to occur within the next 3 years |
| Possible | The event may occur within the next 3 years |
| Unlikely | The event is not likely to occur in the next 3 years |
| Rare | The event will only occur in exceptional circumstances |

****

**Risk Matrix- Function of Consequences and Likelihood**

****

**Risk Rating**

|  |  |  |  |
| --- | --- | --- | --- |
| **Extreme** | **High** | **Medium** | **Low** |