



## Risk Management Policy

Version	Approved by	Approval date	Effective date	Next review
3.0	Board	02 August 2019	01 July 2019	July 2020
<b>Policy Statement</b>				
<b>Purpose</b>	<p>To establish a framework for Risk Identification. Risk Identification is the overall process of risk identification, risk analysis and risk evaluation.</p> <p>To establish a framework for communicating, managing and monitoring risks in SEARMS operations.</p> <p>To incorporate risk management into the strategic, operational planning and quality processes of SEARMS in order to mitigate the impact of high-risk activities.</p> <p>To ensure new opportunities are assessed for risk appropriately, thereby maximising innovation and growth and minimising adversity.</p>			
<b>Scope</b>	<p>It is the responsibility of all SEARMS Board members, Staff, Tenants and Contractors to identify, evaluate, respond, communicate and monitor risks associated with any activity, function, or process within their relevant scope, responsibility or authority.</p>			
<b>Policy Provisions</b>				

### Contents

1.	Introduction.....	2
2.	General principles of risk management .....	2
2.1.	Risk management creates and protects value.....	2
2.2.	Risk management is an integral part of all organisational processes.....	2
2.3.	Risk management is part of decision making. ....	2
2.4.	Risk management explicitly addresses uncertainty. ....	2
2.5.	Risk management is systematic, structured and timely.....	2
2.6.	Risk management is based on the best available information. ....	2
2.7.	Risk management is tailored.....	2
2.8.	Risk management takes human and cultural factors into account. ....	3
2.9.	Risk management is transparent and inclusive. ....	3
2.10.	Risk management is dynamic, iterative and responsive to change.....	3
2.11.	Risk management facilitates continual improvement of the organization.....	3
3.	Terms & Definitions .....	3
4.	Framework .....	3
4.1.	General .....	3
4.2.	Mandate & commitment.....	3
5.	Consultation .....	4

## 1. Introduction

SEARMS is committed to excellence and continual improvement. It will continue to encourage innovation whilst maintaining a low-risk profile. An effective risk policy:

- 1.1.1. Supports effective decision making
- 1.1.2. Ensures a consistent and effective approach to risk management
- 1.1.3. Formalises its commitment to the principle of risk management
- 1.1.4. Fosters and encourages a risk-aware culture where risk management is seen as a positive attribute of decision-making rather than a corrective measure
- 1.1.5. Aligns and integrates SEARMS planning, quality and risk management systems across its operations; and,
- 1.1.6. Ensures that robust governance practises are implemented while allowing innovation and new opportunities decision making

This policy should be appropriate to the nature and scale of SEARMS risks and will be reviewed periodically to ensure that it remains relevant and appropriate to the organisation.

## 2. General principles of risk management

For risk management to be effective, an organisation should at all levels comply with the principles below:

### 2.1. Risk management creates and protects value

- 2.1.1. 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.

### 2.2. Risk management is an integral part of all organisational processes.

- 2.2.1. 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.

### 2.3. Risk management is part of decision making.

- 2.3.1. Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

### 2.4. Risk management explicitly addresses uncertainty.

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

### 2.5. Risk management is systematic, structured and timely.

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

### 2.6. Risk management is based on the best available information.

- 2.6.1. 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.

### 2.7. Risk management is tailored

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

## **2.8. Risk management takes human and cultural factors into account.**

- 2.8.1. Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

## **2.9. Risk management is transparent and inclusive.**

- 2.9.1. Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views considered in determining risk criteria.

## **2.10. Risk management is dynamic, iterative and responsive to change.**

- 2.10.1. Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

## **2.11. Risk management facilitates continual improvement of the organization.**

- 2.11.1. Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

## **3. Terms & Definitions**

For the purposes of this document, the terms and definitions as detailed in the Definitions & Acronyms section at the end of this policy apply.

## **4. Framework**

### **4.1. General**

- 4.1.1. **SEARMS** effectiveness at risk management is dependent on the management framework that embed it throughout the organisation, at all levels.
- 4.1.2. The necessary components of SEARMS framework for managing risk and the way in which they interrelate in an iterative manner are shown at **Figure 1**.

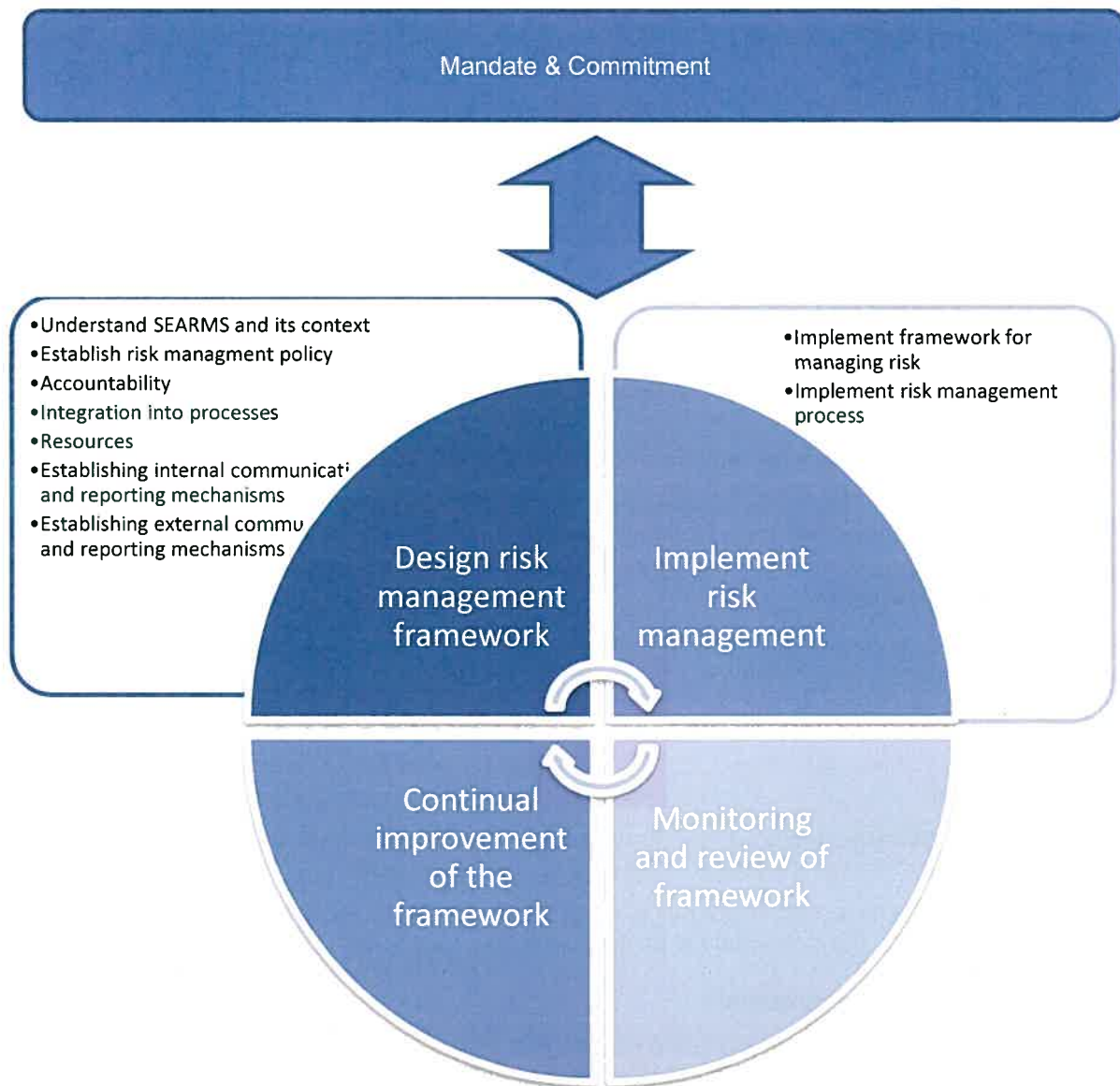
### **4.2. Mandate & commitment**

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels.

Management should:

- 4.2.1. define and endorse the risk management policy;
- 4.2.2. ensure that the organization's culture and risk management policy are aligned;
- 4.2.3. determine risk management performance indicators that align with performance indicators of the organization;
- 4.2.4. align risk management objectives with the objectives and strategies of the organization;
- 4.2.5. ensure legal and regulatory compliance;
- 4.2.6. assign accountabilities and responsibilities at appropriate levels within the organization;
- 4.2.7. ensure that the necessary resources are allocated to risk management;
- 4.2.8. communicate the benefits of risk management to all stakeholders; and
- 4.2.9. ensure that the framework for managing risk continues to remain appropriate.



**Figure 1. Relationship between components of a Risk Management Framework**



## 5. Consultation

Consultation will occur at and between all levels of the organisation as required.

- 5.1.1. SEARMS employees will be consulted and will participate in each step of the risk management process.
- 5.1.2. SEARMS employees must follow safety instructions and procedures, and report any hazards, health and safety issues immediately so that risks can be managed before an incident occurs.
- 5.1.3. If SEARMS has a health and safety committee, SEARMS will engage the committee in the risk management process as well.
- 5.1.4. SEARMS contractors are also required to follow safety instructions and procedures, and report any hazards, health and safety issues immediately so that risks can be managed before an incident occurs when they are engaged by SEARMS to carry out works.

Accountabilities	
Issuing Officer/s	Chair, Board and Chief Executive Officer  
Contact Officer	Chief Executive Officer
Supporting Information	
Legislative Compliance	This Policy supports SEARMS compliance with the following legislation: <a href="#">Corporations (Aboriginal and Torres Strait Islander) Act 2006</a> <a href="#">Community Housing Providers (Adoption of National Law) Act 2012 - NSW</a>
Supporting Documents	Fraud and Corruption Control Policy Financial Management Policy Code of Conduct Policy Delegations of Authority Policy Delegations Schedule <a href="#">NRSCH Evidence Guidelines</a> <b>Performance Outcome 2: Housing Assets (d)</b> <b>Performance Outcome 4: Governance (a, b, c)</b> <b>Performance Outcome 5: Probity (c)</b> <b>Performance Outcome 7: Financial Viability (c)</b> AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines
Related Documents	Risk Management Plan Risk Register
Superseded Documents	NIL
File Number	[For Governance Use]
Definitions and Acronyms	
Risk	effect of uncertainty on objectives. Deviation can be positive and/or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Risk is often characterized by reference to potential <b>events</b> and <b>consequences</b> or a combination of these. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated <b>likelihood</b> of occurrence.
Risk management	coordinated activities to direct and control an organisation with regard to risk
Risk management framework	set of components that provide the foundations and organizational arrangements for designing, implementing, <b>monitoring</b> (2.28), reviewing and continually improving <b>risk management</b> (3.1.2) throughout the organization. The foundations include the policy, objectives, mandate and commitment to manage <b>risk</b> . 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.

<b>Risk management policy</b>	statement of the overall intentions and direction of an organization related to <b>risk management</b>
<b>Risk management plan</b>	scheme within the <b>risk management framework</b> specifying the approach, the management components and resources to be applied to the management of <b>risk</b> . Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.
<b>Risk owner</b>	person or entity with the accountability and authority to manage a <b>risk</b>
<b>Risk management process</b>	systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, <b>monitoring</b> and reviewing <b>risk</b> .
<b>Establishing the context</b>	defining the external and internal parameters to be taken into account when managing risk, and setting the scope and <b>risk criteria</b> for the <b>risk management policy</b>
<b>External context</b>	external environment in which the organization seeks to achieve its objectives. External context can include: – the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; – key drivers and trends having impact on the objectives of the organization; and – relationships with, and perceptions and values of external <b>stakeholders</b> .
<b>Internal context</b>	internal environment in which the organization seeks to achieve its objectives. Internal context can include: – governance, organizational structure, roles and accountabilities; – policies, objectives, and the strategies that are in place to achieve them; – the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); – information systems, information flows and decision-making processes (both formal and informal); – relationships with, and perceptions and values of, internal stakeholders; – the organization's culture; – standards, guidelines and models adopted by the organization; and – form and extent of contractual relationships.
<b>Communication and consultation</b>	continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with <b>stakeholders</b> regarding the management of <b>risk</b> . The information can relate to the existence, nature, form, <b>likelihood</b> , significance, evaluation, acceptability and treatment of the management of risk. Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is: – a process which impacts on a decision through influence rather than power; and – an input to decision making, not joint decision making.
<b>Stakeholder</b>	person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. A decision maker can be a stakeholder.
<b>Risk assessment</b>	overall process of <b>risk identification</b> , <b>risk analysis</b> and <b>risk evaluation</b> .
<b>Risk identification</b>	process of finding, recognizing and describing <b>risks</b> . Risk identification involves the identification of <b>risk sources</b> , <b>events</b> , their causes and their potential <b>consequences</b> . Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and <b>stakeholder's</b> needs.
<b>Risk source</b>	element which alone or in combination has the intrinsic potential to give rise to <b>risk</b> . Risk source can be tangible or intangible

<b>Event</b>	occurrence or change of a particular set of circumstances. An event can be one or more occurrences, and can have several causes. An event can consist of something not happening. An event can sometimes be referred to as an "incident" or "accident". An event without <b>consequences</b> can also be referred to as a "near miss", "incident", "near hit" or "close call".			
<b>Consequence</b>	outcome of an <b>event</b> affecting objectives. An event can lead to a range of consequences. A consequence can be certain or uncertain and can have positive or negative effects on objectives. Consequences can be expressed qualitatively or quantitatively. Initial consequences can escalate through knock-on effects.			
<b>Likelihood</b>	chance of something happening. In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.			
<b>Risk profile</b>	description of any set of <b>risks</b> . The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined			
<b>Risk analysis</b>	process to comprehend the nature of <b>risk</b> and to determine the <b>level of risk</b> . Risk analysis provides the basis for <b>risk evaluation</b> and decisions about <b>risk treatment</b> . Risk analysis includes risk estimation			
<b>Risk criteria</b>	terms of reference against which the significance of a <b>risk</b> is evaluated. Risk criteria are based on organizational objectives, and <b>external</b> and <b>internal</b> context. Risk criteria can be derived from standards, laws, policies and other requirements.			
<b>Revision History</b>				
<b>Version</b>	<b>Approved by</b>	<b>Approval date</b>	<b>Effective date</b>	<b>Sections modified</b>
0.2	Board	23 Sept 2016	23 Sept 2016	

<b>Further Information</b> This section is not published on the final PDF document. It is for website purposes only	
<b>Keywords for search engine</b>	Policy will be housed within the Quality Assurance directory. Include keywords to assist location using the 'search' function.
<b>FAQs and answers</b>	Include any Frequently Asked Questions and answers to be included with the Policy (in a separate tab or section) in the Quality Assurance directory.

