56	Organisational Risk Management Policy		
Version	APPROVAL	Effective Date	REVIEW DATE
001	Board	01 May 2024	Every 2 years

ASES Standard	**Standard 2: Planning** • Requirement 1.1 Strategic Planning Standard **Standard 2: Governance** • Requirement 2.4 Risk Management Standard **Standard 4: People** • Requirement 4.1 Human Resources Standards • Requirement 4.2 Work Health and Safety Standard
NRSCH Standard	**P O 2 Housing Assets d** **P O 4 Governance a, b, c** **P O 5 Probity c** **P O 7 Financial Viability c**
Contractual Obligation(s)	NSW FACS Specialist Homelessness Services (SHSs) Funding Agreement: Lead Entity and/or Joint Working Agreements
Related Policies	WHS Policy Emergency Management Critical Incidents Risk Management Incident Management Human Relations Business Continuity Planning Financial Management Governance Whisteblower Policy

Contents

1. SCOPE

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.

2. PURPOSE

The purpose of this policy is to:

- To establish a framework for Risk Identification. Risk Identification is the overall process of risk identification, risk analysis and risk evaluation.
- To establish a framework for communicating, managing and monitoring risks in SEARMS operations.
- To incorporate risk management into the strategic, operational planning and quality processes of SEARMS in order to mitigate the impact of high-risk activities.
- To ensure new opportunities are assessed for risk appropriately, thereby maximising innovation and growth and minimising adversity

3. POLICY

SEARMS has established risk management systems that apply to all key operational areas, including:

- human resources
- the reputation of the organisation
- IT
- financial management, viability and fraud
- workplace health and safety
- contracting, funding agreements, brokerage and purchasing
- insurances
- infection control
- disaster management/business continuity
- specialised service risk management).

4. 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:

- Supports effective decision making
- Ensures a consistent and effective approach to risk management
- Formalises its commitment to the principle of risk management
- Fosters and encourages a risk-aware culture where risk management is seen as a positive attribute of decision-making rather than a corrective measure
- Aligns and integrates SEARMS planning, quality and risk management systems across its operations; and,
- 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.

5. GENERAL PRINCIPLES OF RISK MANAGEMENT

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

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.

Risk management is an integral part of all organisational 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.

Risk management is part of decision making.

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

Risk management explicitly addresses uncertainty.

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

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.

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.

Risk management is tailored

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

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.

Risk management is transparent and inclusive.

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.

Risk management is dynamic, iterative and responsive to change.

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.

Risk management facilitates continual improvement of the organization.

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

6. 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.

7. FRAMEWORK

General

SEARMS effectiveness at risk management is dependent on the management framework that embed it throughout the organisation, at all levels.

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.***

Mandate & commitment

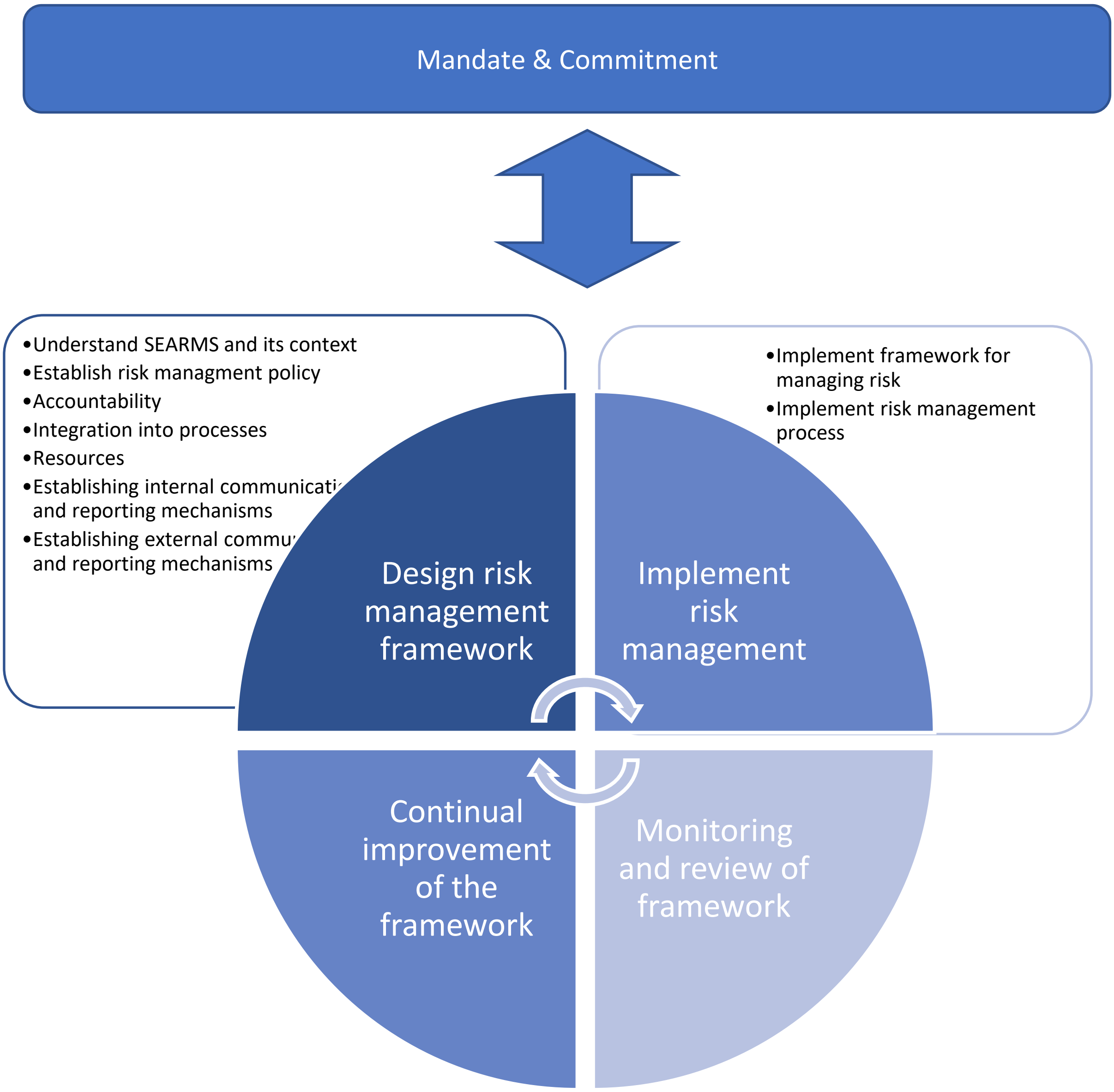
The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels.

Management should:

- define and endorse the risk management policy;
- ensure that the organization's culture and risk management policy are aligned;
- determine risk management performance indicators that align with performance indicators of the organization;
- align risk management objectives with the objectives and strategies of the organization;
- ensure legal and regulatory compliance;
- assign accountabilities and responsibilities at appropriate levels within the organization;

- ensure that the necessary resources are allocated to risk management;
- communicate the benefits of risk management to all stakeholders; and
- ensure that the framework for managing risk continues to remain appropriate.

Figure 1. Relationship between components of a Risk Management Framework


Mandate & Commitment
•Understand SEARMS and its context
•Establish risk managment policy
•Accountability
•Integration into processes
•Resources
•Establishing internal communicati
and reporting mechanisms
•Establishing external commu
and reporting mechanisms
•Implement framework for managing risk
•Implement risk management process
Design risk management framework
Implement risk management
Continual improvement of the framework
Monitoring and review of framework

8. PROCEDURE

1. The following principles guide SEARMS

- Risk management applies to all aspects of [Service Name]'s business and activity.
- All employees and Board members are responsible for risk management.

- Risk management is a continuous improvement process in which the organisation continually strives to reduce and manage the likelihood and negative effects of risks.
- All employees and Board members receive information and support to assist them in managing risk(s) in their roles and, if necessary, in their training.

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

SEARMs employees will be consulted and will participate in each step of the risk management process.

- 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.
- If SEARMs has a health and safety committee, SEARMS will engage the committee in the risk management process as well.
- 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.

2. Delegations

Table 7 below provides a list of delegations and actions for Board members and senior staff to manage risk(s).

Table 7: Actions for Managing Risks.

SEARMS Board members	• Endorse and monitor compliance with the Risk Management Policy, risk management plan, risk register and documented risk review cycle. • Ensure compliance with relevant legislation. • Lead and support the CEO in managing risk. • Monitor and contribute to internal risk treatment strategies and activities. • Retain risk management as a standing item on the Board’s agenda. • Identify and report risks.
Executive Officers]	• Comply with the Risk Management Policy. • Maintain risk management plan, risk register and documented risk review cycle and ensure that these documents are regularly updated. • Manage and monitor compliance with relevant legislation regarding risk management. • Ensure that processes are established throughout the organisation to manage and treat risk appropriately. • Ensure that staff are adequately trained to comply with risk management strategies and activities. • Lead the implementation of the Risk Management Policy. • Identify and assess new risks and implement risk treatments. • Lead, monitor and update identified risks and risk treatments. • Ensure that risk assessments and audits are undertaken. • Ensure the orientation of new staff members to the organisation risk management processes and activities. • Document risk management discussions and decisions from Board meetings. • Identify and report risks.

	• Report on risk management to the Board.
SEARMS Managers	• Comply with the Risk Management Policy. • Identify and assess new risks and implement risk treatments. • Document and file risk assessments and treatment plans. • Monitor and update identified risks and risk treatments. • Implement and review risk management plans. • Contribute to internal risk treatment strategies and activities. • Identify and report risks.
All staff/volunteers	• Comply with Risk Management Policy. • Contribute to risk identification, assessment and management processes. • Identify and report risks.

3. Establishing a risk context

The risk management process accounts for the context in which SEARMS operates and how that context influences and informs risk responses. Contextual factors include:

- the size, purpose and capacity of the organisation
- the needs, aspirations and characteristics of the client group
- the location and community profile through which the service operates
- the funding, legislative and regulatory environment.

4. Risk identification and management

SEARMS identifies risks through formal and informal processes, such as the strategic planning process, targeted consultation, the observation of workplace practice, the monitoring of regulatory requirements, organisational system reviews, regular audits, the analysis of information gathered in relation to incidents, and consumer feedback.

Organisational risks can be categorised and summarised as shown in Table 8.

Table 8: Organisational Risks.

Type	Area
Strategic and governance	• Strategic directions and organisational capacity to achieve them. • Organisational funding, resourcing and growth. • Reputation, industry and market positioning. • External stakeholder and partner relationships. • Quality management and improvement. • Capacity, continuity and performance of the governing body. • Capacity to adapt to changes in government policy, legislation, market conditions and changes to client profile or needs.
Compliance and contracting	• Legal and regulatory requirements, including: ○ Entity legislation requirements (e.g., incorporated association) ○ Employment legislation (see the Human Resources Policy) ○ Work and health safety legislation (see the Work Health and Safety Policy) ○ Other legislative requirements.

Type	Area
	- Contracting, funding agreements, brokerage and purchasing. - Insurance requirements. - Service and industry standards.
Financial and contractual	- Financial management. - Income, budget and expenditure processes. - Fraud prevention. - Charitable status requirements. - Taxation requirements. - Debt collection (if relevant).
Operational and organisational	- Service delivery (e.g., client and clinical risk management, management of programs and projects). - General equipment, assets, resources and facilities. - Human resource management and cultural safety. - Workplace health and safety. - Management expertise. - Workforce capacity. - Information management. - IT and social media management. - Website and marketing. - Business continuity, including: o Break-ins, theft, electrical outages and fire o Natural disasters or major storms. - Infection control.

5. Risk management

Risk identification

All identified risks are documented in the SEARMS Risk Register with dated, delegated and documented strategies to manage, control or minimise the identified risks. The Risk Register is located in [insert].

The CEO is responsible for monitoring the timely and effective implementation of the strategies in the Risk Register, until each identified risk has been eliminated or minimised to an acceptable level (with controls established for managing the risk in the future).

Risk rating

Each risk is rated as ‘high’, ‘medium’ or ‘low’, based on the CEO’s assessment regarding the severity of the risk and its potential negative effect, as well as the likelihood of the risk occurring/recurring. The strategy to address the risk and the time frame and delegation reflects the risk rating.

Participation of all staff

All staff are responsible for contributing ideas to improving risk management; they are also responsible for participating in and implementing the actions identified in the risk management register(s).

Six-monthly review of the Risk Register

The CEO, with any other staff (if relevant), undertakes a six-monthly review of the Risk Register to identify any common themes and patterns that require a more systemic response. Following this review, the CEO implements the required response.

Risk management plan

In addition to the Risk Register, which ensures a response to a specific and unidentified risk on an ongoing basis, the SEARMS also maintains a risk management plan that articulates the organisation’s broad strategies for managing risk in accordance with the categories outlined in Table 8 above.

6. In terms of risk audits

Audits (including document review, technical inspections, maintenance and electrical testing and tagging), are conducted at least every six months to provide assurance that risk management systems are established and effective.

7. In terms of communication and consultation

Communication and consultation are undertaken with SEARMS clients, staff and Board members to ensure understanding and engagement in risk management.

Communication mechanisms include

- orientation processes for new staff and clients entering the service
- agenda items and discussions at staff and team meetings (e.g., WHS, budgets, client-related incidents, hazards identified)
- regular staff and supervisor meetings to review work plans and activities together with incident management
- SEARMS reporting to the Board and the regular review of the organisational risk register.

SEARMS implements diverse consultation methods to seek feedback from clients, staff, Board members, students and volunteers. This may include

- participation in policy development
- participation in risk management and risk incident reviews
- client meetings and focus groups
- workshops
- surveys.

Communication and consultation are undertaken with external stakeholders (if appropriate) as part of SEARMS business. Mechanisms include

- briefing and planning meetings as a part of project development, implementation and evaluation
- performance reports to funding bodies
- annual reports
- surveys and evaluations.

9. RESPONSIBILITIES

Responsibility	Delegation
Oversee the development and maintenance of the risk management plan	COO
Oversee the development and maintenance of the Risk Register	CBO
Oversee the development and implementation of risk audits	CBO
Perform risk identification	CBO
Perform communication and consultation	Executive Officers
Report risk(s)	CBO
Monitor outcomes	CBO

10.LEGISLATION

For more information on related legislation, please see:

- *Work Health and Safety Act 2011* No. 10 https://www.legislation.nsw.gov.au/inforce/f8df8095-a335-66a0-8828-f33d06042cb9/2011-10.pdf
- *Workers Compensation Act 1987* No. 70 http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol_act/wca1987255/
- *Workplace Injury Management and Workers Compensation Act 1998* No. 86 https://www.legislation.nsw.gov.au/~/view/act/1998/86
- *Workers Compensation Legislation Amendment Act 2012* No. 53 https://www.legislation.nsw.gov.au/acts/2012-53.pdf
- *Work Health and Safety Act 2011* No. 137 https://www.legislation.gov.au/Details/C2011A00137
- *Work Health and Safety Regulations 2017* (Cwlth) https://www.legislation.nsw.gov.au/#/view/regulation/2017/404/whole
- *Corporations (Aboriginal and Torres Strait Islander) Act 2006*
- *Community Housing Providers (Adoption of National Law) Act 2012 - NSW*

11.APPENDICES

- Appendix 1: Risk Management Plan.
- Appendix 2: Risk Register.

12.FURTHER RESOURCES

- Local Community Service Association: Sector Development, Policy Development https://www.lcsansw.org.au/
- Institute of Community Directors: Policy Bank

https://www.communitydirectors.com.au/icda/policybank/

Version	APPROVAL	Reason	Effective Date	REVIEW DATE
Version 001	Board	Review and reformat for ASES	1 May 2024	Every 2 years

13.DEFINITIONS & 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 ***events*** and ***consequences*** 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 ***likelihood*** 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, ***monitoring*** (2.28), reviewing and continually improving ***risk management*** (3.1.2) 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.
Risk management policy	statement of the overall intentions and direction of an organization related to ***risk management***
Risk management plan	scheme within the ***risk management framework*** specifying the approach, the management components and resources to be applied to the management of ***risk.*** 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.
Risk owner	person or entity with the accountability and authority to manage a ***risk***
Risk management process	systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, ***monitoring*** and reviewing ***risk***.
Establishing the context	defining the external and internal parameters to be taken into account when managing risk, and setting the scope and ***risk criteria*** for the ***risk management policy***
External context	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 ***stakeholders***.

Internal context	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.
Communication and consultation	continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with ***stakeholders*** regarding the management of ***risk*** . The information can relate to the existence, nature, form, ***likelihood***, 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.
Stakeholder	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.
Risk assessment	overall process of ***risk identification***, ***risk analysis*** and ***risk evaluation***.
Risk identification	process of finding, recognizing and describing ***risks***. Risk identification involves the identification of ***risk sources***, ***events*** , their causes and their potential ***consequences***. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and ***stakeholder's*** needs.
Risk source	element which alone or in combination has the intrinsic potential to give rise to ***risk***. Risk source can be tangible or intangible
Event	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 ***consequences*** can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.
Consequence	outcome of an ***event*** 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.
Likelihood	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.

Risk profile	description of any set of ***risks***. The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined
Risk analysis	process to comprehend the nature of ***risk*** and to determine the ***level of risk***. Risk analysis provides the basis for ***risk evaluation*** and decisions about ***risk treatment***. Risk analysis includes risk estimation
Risk criteria	terms of reference against which the significance of a ***risk*** is evaluated. Risk criteria are based on organizational objectives, and ***external*** and ***internal*** context. Risk criteria can be derived from standards, laws, policies and other requirements.