SURF LIFE SAVING
NORTHERN TERRITORY

Framework

Risk Management

Surf Life Saving Northern Territory Incorporated

ABN: 77 415 570 719

Head Office: 16 De Latour Street, Coconut Grove NT 0810

Date Implemented	31 July 2024
Review Date	31 July 2025
Last Amended	12 June 2024

Table of Contents

Risk Management Policy

Overview

Risk is the effect of uncertainty on achieving Surf Life Saving Northern Territory's (SLSNT) objectives.

SLSNT undertakes risk management processes to understand the risks it faces and to manage and mitigate uncertainty to a tolerable level. Every organisation must take on risk and SLSNT's risk appetite sets out the level of risk that it is prepared to accept in order to operate its business.

Every director, manager and employee of SLSNT is responsible for managing the risks arising within their areas of responsibility and across the business generally. Risks can be categorised in a number of ways but the key ones for SLSNT to be aware of are: Strategic Risk, Financial Risk, People Risk, Operational Risk, Technology Risk and Legal & Regulatory Risk.

This document sets out SLSNTs Risk Management Framework, Policy and Process. It outlines the expectations of the Board, CEO and Managers on how SLSNT will identify risk and implement adequate risk management measures, and who is responsible within the scope of business operations.

Board Mandate

The SLSNT Board of Directors (the Board) is committed to ensuring SLSNT maintains a practical, focused and current Risk Management Framework to identify, assess, monitor and manage material risks related to its activities within its risk appetite.

The Board endorses this Risk Management Framework for implementation across all parts of the organisation.

The Board expects that every director, manager, employee and member will be aware of and manage the risks arising in their areas of responsibility and more generally across SLSNT and to report material issues that come to their attention. The culture of the organisation must reflect a positive, proactive attitude to risk management, which will be viewed as an important part of everyone's roles and responsibilities.

Risk management and risk controls will be incorporated into all key business functions and processes. Risk discussions will be considered and implemented as an integral part in taking key strategic and operational decisions.

Risk management is one part of the overall governance functions that provide the foundations which allows SLSNT to continue to operate our business and is considered a fundamental component of how we operate.

Risk Principles

Risk management must:

- Both create and protect business value by assisting the organisation achieve business objectives
- Be everyone's responsibility and accountability
- Be an integral part of all business functions and processes across the organisation,
- Be an integral part of decision making to enable informed decisions
- Be systematic, structured and timely in its application and outcome
- Be based on best available information which has a business focus
- Be transparent and inclusive and deal with key stakeholder concerns
- Be dynamic, iterative and responsive to change so it is continually improving the organisation.

Risk Management Roles and Responsibilities

The Board

The Board acknowledges ultimate accountability for the establishment and approval of an effective risk management system and system of internal controls.

In particular, the Board will ensure that:

- A sound risk management culture is established and maintained throughout the organisation and the level of commitment to risk management activities is maintained at an appropriate level
- It approves the Risk Management Framework and Risk Appetite Statement and reviews these at least annually or upon identification of a material change
- The position description of the Chief Executive Officer and other identified senior staff includes risk and compliance management accountabilities and responsibilities
- The Chief Executive Officer takes the steps necessary to monitor and manage all material risks consistent with the strategic objectives, risk appetite and approved policies
- Policies and processes are developed for risk-taking that are consistent with the risk strategy and the established risk appetite.

Chief Executive Officer

The Chief Executive Officer (CEO) is responsible for implementing and maintaining a relevant and practical Risk Management Framework including appropriate monitoring and reporting activities, and for making appropriate training and communication programs available to ensure that all directors, managers, employees and members understand their roles and responsibilities in relation to risk management.

In particular the CEO will ensure that:

- The Risk Management Framework and Risk Appetite Statement remain current, are regularly reviewed and are properly communicated to the organisation
- Identified Business Unit risks are analysed at the Business Unit levels, together with relevant risk treatments, controls and monitoring processes
- Risk management activities and controls are integrated into the existing business policies, procedures and processes
- Ongoing training support is provided for directors, managers and employees, including training tailored to specific roles such as responsible managers and people providing financial advice
- The inclusion of risk and compliance obligations in all position descriptions and key performance indicators is promoted
- A risk monitoring and reporting system is set in place, including establishing key risk/compliance performance indicators
- Processes for managing errors, incidents, breaches and complaints are developed and implemented
- Reviews are undertaken and performance is analysed to assess the need for corrective action
- Appropriate objective advice is provided to the organisation on risk management matters
- Manuals, tools and other resources are developed to assist with risk management activities

Managers and employees

Managers and employees are responsible for risk management within their areas of responsibility and must ensure that risk management activities are undertaken as part of the day-to-day operations.

In particular managers will ensure that:

- There is ongoing cooperation with and support of the CEO and their activities by the business and an understanding that risk is everyone's responsibility
- They will personally meet all their risk management obligations and responsibilities and be seen to be complying with the requirements for maintain risk management activities
- Risks are proactively identified and communicated within their operational areas and where corrective action is required ensure that it is undertaken in a timely and effective manner
- Employees are actively mentored, coached and supervised to promote appropriate risk management behaviours and to raise risk concerns
- They personally and actively participate in the management, reporting and resolution of material risk issues, errors, incidents and breaches
- Support relevant training requirements and encourage employees to attend relevant risk training
- Factor risk management responsibilities into job descriptions and integrate this into employee performance appraisals
- Risk management activities and controls are properly integrated into the existing business policies, procedures and processes and make sense in the business context

In particular, management and employees will ensure that:

- They adhere to the risk management requirements that are relevant to their position and duties
- They participate in training in accordance with the risk management processes
- They use available risk management resources
- They report all risk management concerns, issues and failures in a timely manner.

Risk Management Process

SLSNT's Risk Management Process is set out below and the following sections explain how it is implemented at a practical level within the organisation. This process is tailored to our business processes and follows the requirements of ISO 31000. It will be an integral part of management activities.

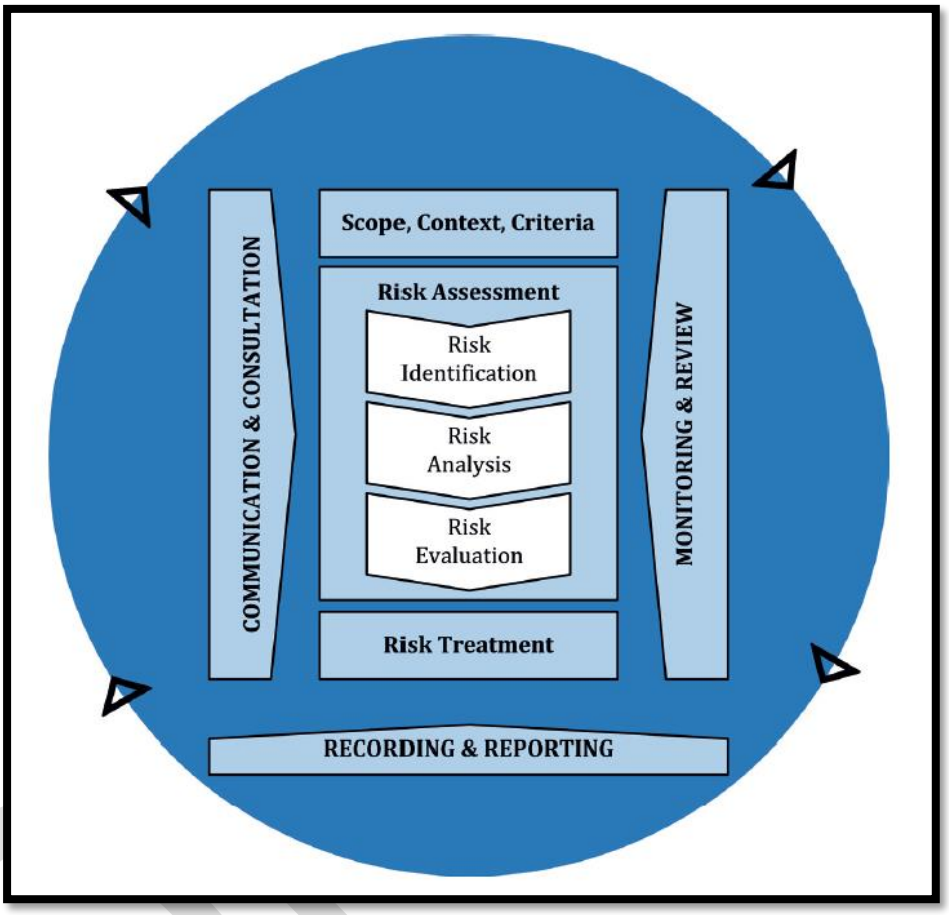

Image 1. Risk Management Process ISO 31000:2018

Communication and consultation

As SLSNT must "own" risk management within the organisation, it is important for the CEO to have open channels of communication across all levels of the business. The aim is to facilitate truthful, relevant, accurate and understandable two-way exchanges of information, considering confidential and personal integrity issues.

Communication and consultation will be established and encouraged as follows:

- The CEO will include staff to assist build the understanding of risk and compliance requirements and assist with documenting risk profiles, compliance plans and key controls
- Business unit risks and risk registers will be developed and maintained in conjunction with the business and based on business input and will be reviewed on an annual basis
- Regular compliance and risk management meetings will be held with the business units to report on risk and compliance performance, identify areas of concern and how to deal with them and provide general communication about risk and compliance activities

- Formal channels of communication and tools will include incident and breach management and escalation processes, whistleblowing processes, monitoring and review programs and regular reporting processes both business unit specific and up to the Board.

Scope, Context and Criteria

SLSNT exists to save lives. SLSNT is the Territory's peak water safety and rescue organisation. The mission is simple – We save lives and inspire Territorians to build better communities.

Risk is a necessary part of doing business. Not all risk can be treated or avoided, therefore, SLSNT has to accept some level of risk. SLSNT's appetite for risk is central to the way it does business and each level of the organisation needs clear guidance on the limits of risk they can take.

Risk Appetite Statement

Surf Life Saving Northern Territory (SLSNT) is the peak organisation for surf life saving in the Northern Territory and is affiliated with Surf Life Saving Australia.

SLSNT is responsible for the governance, development, promotion and administration of surf life saving throughout the Northern Territory and has the responsibility for servicing its 600 plus members and 3 clubs.

Our Vision is "zero preventable deaths in NT Coastal waters" and our Mission is to "we save lives and inspire Territorians to build better communities". As a volunteer emergency service, we operate in an environment where compliance enables us to save lives, as well as perform well financially.

Therefore, SLSNT generally has a low tolerance to risk, particularly in areas that impact on the safety and security of the public, members and staff.

Our objective is sustainable, incremental growth, so SLSNT has a moderate risk tolerance for investment and financial risk. However, decisions should be taken with the long-term interests of our member clubs and the broader membership base in mind.

SLSNT adopts the definitions for risk appetite and risk tolerance that are set out in the Standard - ISO 31000:2018 Risk Management - Guidelines.

Risk Identification

Risk identification involves identifying and classifying events, situations or actions that could have a negative effect on SLSNT's ability to achieve its strategy, objectives and goals.

Sources of risk

The following table outlines the tools and techniques that will be used by SLSNT to identify risks.

Source	Description
Risk registers and risk reports	Provide a foundation for evaluating existing risks and their potential risk to an objective.
Issues log	Record of issues faced, and the actions taken to resolve them. Any issues that were formally identified as risks should be analysed.
Audit reports	Independent view of adherence to regulatory guidelines including a review of compliance preparations, security policies, access controls and management of risks.
Internal & external reviews	Reviews undertaken to evaluate the suitability, adequacy and effectiveness of the organisation's systems, and to look for improvement opportunities.

SWOT analysis	Commonly used as a planning tool for analysing a business, its resources and its environment by looking at internal strengths and weaknesses and opportunities and threats in the external environment.
Brainstorming	Creative technique to gather risks spontaneously by group members. Group members verbally identify risks in a 'no wrong answer' environment. This technique provides the opportunity for group members to build on each other's ideas.
Scenario analysis	Uses possible (often extreme) future events to anticipate how threats and opportunities might develop.
Surveys / Questionnaires	Gather data on risks. Surveys rely on the questions asked.
Stakeholder analysis	Process of identifying individuals or groups who have a vested interest in the objectives and ascertaining how to engage with them to better understand the objective and its associated uncertainties
Working groups	Useful to surface detailed information about the risks i.e. source, causes, consequences, stakeholder impacted, existing controls
Corporate knowledge	History of risks provide insight into future threats or opportunities through: • Experiential knowledge – collection of information that a person has obtained through their experience. • Documented knowledge – collection of information or data that has been documented about a particular subject. • Lessons learned – knowledge that has been organised into information that may be relevant to the different areas within the organisation.
Process analysis	An approach that helps improve the performance of business activities by analysing current processes and making decisions on new improvements.
Other jurisdictions	Issues experienced and risks identified by other jurisdictions should be identified and evaluated. If it can happen to them, it can happen here.

Risk categories

The following table outlines the classification of risks based on the business activities of SLSNT.

Risk Category	Description
Strategic Risk	SLSNT undertakes a thorough and consultative planning process, which involves assessing risk of proposed strategic pillars. Generally, we have a low risk tolerance for strategic pathways that conflict with the core values and operational deliverables of the organisation. We may, however, accept a moderate amount of strategic risk in one or two projects that are designed to future-proof the business. We accept that we must consider changes in Government priorities and this may impact our strategic risk approach.
Compliance Risk	SLSNT has a low appetite for deliberate acceptance of operational risks that lead to material adverse regulatory or legal impacts. SLSA has no appetite for intentional, persistent non- compliance with legal and regulatory obligations; failure to report and address material misconduct (either deliberate or inadvertent) through

	appropriate channels; or failure to identify legal and regulatory changes that have a material impact on SLSNT.
Operational Risk	SLSNT has a low appetite for loss as a result of inadequate or failed internal processes, people, systems, or external events that disrupt the flow of business. Examples include insufficient workforce, IT systems failure, data breaches, loss of people, non-adherence to work health & safety processes. SLSNT will take reasonable steps to protect, detect and manage the likelihood and impact of unauthorised disclosure, modification or destruction of sensitive member/organisation information.
Brand and Reputational Risk	SLSNT has a low appetite for risk that may negatively impact its brand and reputation to any material degree. However, it may take a course of action that could potentially impact its reputation in the short term, if it is believed by the majority of directors to the ethical course of action, and the reputational damage will not be significant in the long term.
Financial Risk	SLSNT has a moderate appetite for financial risk, recognising that it must achieve sustained financial growth to support the growing needs of the movement and its component parts. We accept that there is potential volatility of funding, given available funding sources. However, SLSNT has no risk tolerance for actions that may cause it to fail to meet financial obligations due to lack of liquidity. It has low appetite for internal fraud and accepts a residual risk rating of low for external fraud.
People/Member Related Risk	SLSNT has a low appetite for non-compliance with people / member related policies and procedures. SLSNT has no appetite for misconduct, harassment, or discrimination by or towards our staff and members.

Risk Analysis

Risk analysis involves developing an understanding of the risk and involves consideration of the causes and sources of the risks, their positive and negative consequences and the likelihood that those consequences will occur.

Step 1: Determine the likelihood of the risk occurring

The following table is used to rate the "Likelihood" (a number from 1 to 5) of the risks, in the absence of any controls.

Level	Descriptor	Description
5	**Almost Certain**	• Will probably occur more than once • 100% chance of occurrence • Common or Frequent Occurrence • Is expected to occur in most circumstances

4	**Likely**	• High probability that will occur at least once • 1 in 10 chance of occurrence (10%) • Likely to occur or "has happened to us a number of times in the past" • Might occur in a 2-3 years' timeframe
3	**Possible**	• Reasonable likelihood that could occur more than once • 1 in 100 chance of occurrence (1%) • Could occur or "I've heard of it happening elsewhere" • Might occur in a 5 years' timeframe
2	**Unlikely**	• May occur once or less • 1 in 1000 chance of occurrence (0.1%) • Not likely to occur • Might occur in a 10 years' timeframe
1	**Rare**	• May occur in exceptional circumstances • Practically impossible • 1 in 10,000 chance of occurrence (0.01%) • Could happen but probably never will

Step 2: Determine the consequences of the risk occurring
This table rates the "Consequence" (a number from 1 to 5) of the risks.

	Insignificant	Minor	Moderate	Major	Catastrophic
Strategic	Ongoing issues that arise in the course of managing the timely delivery of strategic objectives, can be managed by those responsible	Minor threat of delay in delivery or timing of a strategic objective that can be addressed by those responsible	Delay or threat to timely delivery of a major component of a strategic objective with a need to review or revise Inadequate project forecasting of resources necessary to meet strategic objective	Failure to deliver a significant component of a strategy Significant delay in the timely delivery of strategic objective Inadequate provision of resources to meet strategic objective	Failure to deliver a strategy which is unmanaged and unmitigated and so unexpected Long term workforce / community harm Sudden/prolonged loss of significant proportion of key leadership
Compliance	Temporary breach unlikely to attract regulatory response or claim Can be managed through day-to -day activities Notification of authorities unlikely to result in action	Minor breach which may incur a non-compliance or improvement notice Notification to regulatory body is necessary	Breach of regulations or negligence involving investigation by or report to authority with prosecution powers Potential for moderate fine Breach of funding agreements terms and conditions	Major breach of funding agreement, legislation or regulations	Serious or wilful breach of regulations or negligence incurring significant prosecution, with potential for significant fines
	No effect on contract performance	Results in meeting with contractor in which contractor expresses concern	Receive verbal advice that, if breaches continue, a default notice may be issued	Receive written notice from contractor threatening termination if not rectified	Termination of Contract for default
Operational	An event, where the impact can be absorbed through business-as-usual activity IT systems do not operate efficiently	An event, where the consequences can be absorbed but management effort is required to minimise the impact	An event, that can be managed under normal circumstances, but requires additional resources and potential reallocation of resources	An event, which with proper management can be endured, but may involve some changes in management and require additional resources	An event so severe in nature it could lead to a significant restructure of the organisation or its major parts or a change in the management structure

	Issue/s quickly resolved No disruption to operations	Potential reallocation of resources IT systems are down for <3 days Operations disrupted <72 hours	Core IT systems are down for 3-7 days Operations disrupted for 3-7 days	Sensitive and personal data released to public Core IT systems are not available for 1-2 weeks Operations disrupted for 7-14 days	Large scale release of sensitive and personal information to public Core IT systems are not available for >2 weeks Operations disrupted for >14 days
	Member sustains minor cuts or abrasions requiring first aid treatment	Member sustains minor injury requiring medical attention Staff absences increase sufficiently to cause delay	Accident leads to member hospitalisation Skilled staff shortages lead to significant additional costs or delays	Accident leads to extensive or serious member injury or temporary disablement. Unable to attract any skilled staff	Death or serious permanent disablement of member
Brand and Reputation	No loss of stakeholder confidence Ad hoc negative mentions on social media No media enquiries Public concern restricted to local complaints	Minor loss of stakeholder confidence Ad hoc negative mentions or rumours of a negative event on social media Internal review of existing policies and practices instigated No impact on staff turnover	Significant loss of stakeholder confidence Substantial adverse publicity locally Minister enquiry received Risk event requires public SLSNT response Turnover of full-time staff exceeding 20% in one year	Serious loss of stakeholder confidence Territory public, political and media scrutiny / criticism Funding lost for many months Turnover of full-time staff exceeding 30% in one year	Complete loss of stakeholder confidence National public, political and media scrutiny / criticism Significant impact on funding for several years Turnover of full-time staff exceeding 30% in two successive years
Financial	Loss <$5,000 from annual budget – net profit	Loss $5,000-$20,000 from annual budget – net profit Costs and or loss unable to be consumed in Business Unit budget Fraud event <$500,000	Loss $20,000-$250,000 from annual budget – net profit Unauthorised spend <$20,000 Fraud event $50,000-$100,000	Loss $250,000-$500,000 from annual budget – net profit Fraud event $100,000-$250,000	Loss >$500,000 from annual budget – net profit Fraud event >$250,000 Key 3rd party withdrawal of funding
People/Member	Member complaints regarding non-compliance	Member complaints regarding minor non-compliance of policy, that	Member complaints regarding significant non-compliance of policy or	Member complaints regarding proven non-compliance of policy or	Serious or wilful breach of policies or negligence incurring significant

	of policy, that are not upheld	result in grievance or mediation procedures	legislation that result in SLS sanctions and/or potential civil lawsuit	legislation that result in civil lawsuit or criminal prosecution.	criminal prosecution with outcomes (fines and/or sentencing) or significant payments under civil lawsuit

Risk Evaluation

The objective is to assess the potential risk exposure in qualitative and quantitative terms and examine the frequency and the size of the loss/issue.

Step 3: Determine the rating for the inherent risk

An Inherent Risk rating will be defined as High, Significant, Medium and Low based on the combination of likelihood and potential consequence. This rates the risk regardless of any measures in place to control it.

		Consequence				
Likelihood		1. Insignificant	2. Minor	3. Moderate	4. Major	5. Catastrophic
	5. Almost Certain	M	S	H	H	H
	4. Likely	M	S	S	H	H
	3. Possible	L	M	S	S	H
	2. Unlikely	L	M	M	S	S
	1. Rare	L	L	L	M	M

H = High	S = Significant	M = Medium	L = Low

Step 4: Identify existing controls already in place

Identify the controls in place to reduce the likelihood and consequences of the risk and assess their effectiveness.

Step 5: Rate the existing controls – how good are they?

Rate the existing controls using the following table.

Level	Descriptor	Description
4	Excellent	System is effective in reducing risk, responsibility clear, well documented, regularly reviewed
3	Good	Systems and documentation in place but room for improvement
2	Fair	Some controls in place but incomplete
1	Poor / Unsatisfactory	Ad hoc and poorly documented processes, or no controls at all

Step 6: Use matrix to determine a Residual Risk rating for the risk

The Residual Risk rating assesses the business risk considering the controls that are already in place. The Risk Priority rating for the risk is obtained by using the inherent risk rating, the control rating and the table below.

This will then determine the priority for managing and dealing with the risk.

Inherent Risk	Existing Controls			
	1	2	3	4
High	H	H	S	M
Significant	S	S	M	L
Medium	M	M	M	L
Low	L	L	L	L

H = High	S = Significant	M = Medium	L = Low

Risk Level	Residual Risk Management Actions
HIGH	Discontinue activity - Immediate correction required • Activity must not be commenced, or is to be discontinued if started, until level of risk is reduced to within tolerable levels. • Risk must be immediately reported to Chief Executive Officer. • A plan outlining the additional controls or mitigation strategies needed to manage the risk to an acceptable level must be developed prior to commencing activity. • Regardless of position held, employees must exercise risk separation before proceeding (i.e. a second set of eyes must assess the risk and agree the proposed controls will reduce the risk to within tolerable levels).
SIGNIFICANT	Corrective action required • Risk must be immediately reported to Unit Manager. • Review controls to ensure there is nothing else that can be reasonably done to reduce the probability and/or impact of the risk. • If level of risk is 'as low as possible' the activity can continue with CEO approval and constant monitoring of the risk to ensure the risk level does not increase further. • A plan outlining the additional mitigation needed to manage the risk to an acceptable level must be developed before activity starting. • Ensure all controls are in place and are effective prior to commencing the activity.
MODERATE	Attention needed • Risk must be reported to Unit Manager. • Review controls to ensure there is nothing else that can be reasonably done to reduce the probability and/or impact of the risk. • If level of risk is 'as low as possible' the activity can continue with CEO approval and constant monitoring of the risk to ensure the risk level does not increase further. • Cost effective mitigation strategies should be strongly considered to lower risk to acceptable level. • Activity can continue using standard operating procedures, industry codes of practice, ongoing monitoring and review of risks.
LOW	No changes required - generally considered to be at a level that SLSNT can accept • Ensure existing controls remain in place and are effective.

Risk Treatment

Step 7: Identification of action required

Risk treatment involves selecting one or more options for modifying risks and implementing those options. Once implemented, treatments can either become or modify existing controls and will change the control rating. Risk treatment options can include one or more of the following:

- accept the risk by informed decision
- reduce the risk through mitigation strategies and implementation of controls
- share the risk with another party – insurance or counterparty
- avoiding the risk by deciding to stop, not to start or not to continue the activity

Step 8: Risk Treatment Plan

The top 15-20 Key Material Risks at a corporate and each business unit level will be documented in a Risk Profile which will incorporate the Risk Treatment Plan (see Appendix A Sections 1-3) to bring that risk back into an acceptable Risk Appetite level and the controls that will be implemented to manage and monitor that risk. These risks and the progress of the Risk Treatment Plan will be monitored and reported on a monthly basis.

All other identified risks and the outcome of the risk assessment process will be documented in a Risk Register.

Recording and reporting

Each Priority Risk will be allocated Key Risk Indicators (**KRI**) by the Manager responsible for that risk. The Manager will be accountable for ensuring that that Treatment Plan for the Priority Risk is implemented and completed and for monitoring the KRIs on a regular basis to ensure that the business is operating within Risk Appetite. Where KRIs are not being met, the Manager must ensure further action is taken to address the risk and update the Risk Profile.

The CEO will undertake regular monthly monitoring of the Priority Risks, the KRIs and the progress against any Risk Treatment Plan and report back to the Risk Committee and the Board.

An 'issue' is a risk that has crystallised and is negatively impacting business strategy, operations or outcomes. An issue includes:

- Errors – operational mistakes of a one-off, more minor nature, that are easily and quickly rectified
- Incidents – failure to meet operational / compliance / ethical / other business requirements or legal / contractual obligations that could potential result in damage or loss and either reflect a negative trend of errors, are less easy to fix or are otherwise more significant
- Breach – breach of a legal or compliance obligation that must be reported to a regulator.

Each Manager will be accountable for ensuring that issues arising within their business areas are identified, reported and addressed in an appropriate and timely manner.

A Quarterly Incidents Report will be prepared by the CEO with the assistance of the Business Managers. The CEO will address any issues with the Board.

Monitoring and Review

Review of Corporate and Business Unit Risk Profiles

The CEO is responsible to initiate the risk management process and review the Risk Profiles on an six monthly basis or sooner where there are significant changes to the business or its operating environment. The purpose of this activity is to ensure that the key risks identified and mitigated continue to be in line with the business strategy and priorities and within the Risk Appetite.

Each Manager will be accountable for ensuring that their team works with the CEO to review and update the Risk Profile of their Business Unit and recognises this as a personal accountability.

Risk management training

The Risk Management Framework and policies are presented to all employees during the induction program, on-site training and mandatory compliance training and can be discussed during the individual appraisal. This communication increases the employee awareness about Risk Management within SLSNT and contributes to the development of a strong risk culture and addresses the management of risk by the business.

On the job risk management training occurs at the regular sessions undertaken to identify the Business Unit's Risk Profile. All staff are encouraged to take part in the process and contribute their views.

Review of Risk Management Framework

Internal review

A review of the Risk Management Framework is conducted by the CEO on an annual basis or earlier if there are material changes in the organisation's operating environment. Any changes must be reviewed and endorsed by the Board.

The CEO will ensure that any recommendations are considered and implemented as agreed with the Board.

External review

A comprehensive external review of the effectiveness and adequacy of the Risk Management Framework will be undertaken at least every 2 years. The results of the review performed by external auditors will be presented to the Board.

The CEO will ensure that any recommendations are considered and implemented as agreed with the Board.