St Vincent de Paul Society NSW

good works

Risk Management Policy

Approved by the St Vincent de Paul NSW Board on 1st February 2014.

Version Control

Contact names	Role / position	Version number	Date	Review date
Thomas Law	Internal Audit and Risk Manager	1	24 January 2014	2016

CONTENTS

Policy Statement

The Society recognises that Risk Management is a core component of governance.

The Society is committed to the concept and operational framework ensuring risk management procedures as part of the decision making process.

The Society recognises that an effective risk management process can increase community confidence and enhance the already positive reputation for the Society.

An effective risk management process can improve controls over the use of valuable resources which are of the greatest benefits to the Society.

Members, volunteers and employees shall comply with the Risk Management Policy.

Activities for managing risks should, whereas practical, be consistent with the principles outlined in the AS/NZS ISO31000:2009.

Purposes

The purposes of this policy are to:

- Develop risk awareness culture with the Society
- Facilitate the compliance with the risk management standard
- Develop a robust risk management system by continuously review and improve the risk assessment and management process
- Ensure strategic risks have been considered when making strategic management decisions
- Ensure operational risks have been considered when reviewing management processes

Principles

St Vincent de Paul Society NSW adopts the risk management principles and processes set out in the International Risk Management Standard ISO 31000:2009.

Risk management in St Vincent de Paul Society NSW is owned, operated and reported on by managers, including Chief Executive Officer, Executive Officers for State Support Office, Support Services and Central Councils and Internal Audit and Risk Manager. That is, responsibility for undertaking, assessing and monitoring risk

management as well as implementation and maintenance of internal controls is a management function. Management reports the status of material strategic and business risks to the Audit Risk and Finance Committee via Chief Executive Officer.

Effective risk management is necessary for competent strategic decision making and the conduct of efficient, effective and robust business processes that allow the Society to take up opportunities while meeting required standards of accountability, compliance, probity and transparency. Sound management practices based on expertise, innovation and contingency planning can reduce high inherent risk exposures to acceptable levels.

Scope

This policy applies to St Vincent de Paul Society NSW as a whole, including all special work facilities, retail centres, Conferences under State and Central Councils and St Vincent de Paul Support Service. It also applies to members, volunteers and employees of the Society.

This policy excludes workplace health and safety, which has been addressed in another policy.

Definitions

The Society has adopted the definitions provided in the Standards on Risk Management ISO 31000:2009. The definition for some key words for this policy document is as follows:

Risk - Effect of uncertainty on objectives

Risk Management – Coordinated activities to direct and control the Society with regard to risk

Risk Attitude – the approach to assess and eventually pursue, retain, take or turn away from risk

Risk Management Policy – Statement of the overall intentions and direction of the Society related to risk management

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

Risk Register – A document that includes identified risks which may have impact to the Society. Refer to the Risk Review Report

Risk Profile – Description of any set of risks

Risk Analysis – process to comprehend the nature of risk and to determine the level of risk

Risk Treatment – process to modify risk

Control – measure that is modifying risk

Residual Risk – risk remaining after risk treatment

Risk Appetite – the level of risk that the Society to accept whilst continuing to be a highly regarded charitable organisation by members, volunteers and employees, and be in a position to meet its strategic objectives

Roles and Responsibilities

Board

The Directors of the Board have the responsibilities of the following:

- Ensuring the compliance with the objects for which the Company was established
- Ensuring the Society is managed in a responsible and competent manner
- Providing strategic direction and effective oversight to the Society
- Ensuring the Society is accountable to all Company members and volunteers
- Ensuring all regulatory and financial reporting requirements are met
- Overseeing risk management and risk assessment across the Society
- Determining the risk appetite of the Society and the Society's attitude to risks with respect to particular major issues
- Reviewing risk management and compliance annually
- Approving major policies in relation to risk management
- Approving policies, standards and codes governing the operation of the Society
- Approving major decisions affecting the risk profile or exposure
- Establishing and maintaining adequate control environment and internal controls

- Monitoring financial performance to ensure informed and sound financial management
- Monitoring the overall effectiveness of the Society's services and operations
- Maintaining Public Benevolent Institution (PBI) and Deductible Gift Recipient (DGR) status
- Approving significant activities affecting the Society
- Providing the opportunity for Society Members and volunteers to improve their spiritual well being

Audit Risk and Finance Committee

The role of Audit Risk and Finance Committee is to serve as the central point of contact between the Board, external auditors, internal auditor and management. The Committee assists the Board in its oversight of the reliability of the Society's financial statements, effectiveness of its internal controls and risk management, compliance with laws and regulations and evaluation of the external and internal auditors.

For risk management, the Committee is responsible for:

- Monitoring risk assessment by the Society, and the internal control systems in place to underpin this assessment including monitoring the effectiveness of risk management processes, and recommending management action to improve risk management
- Evaluating whether Management is setting the appropriate 'control-conscious environment" by communicating the importance of internal control and the management of risk, and ensuring that all employees have an understanding of their roles and responsibilities, all in the context of the Society's operations
- Ensuring both internal and external auditors informing the Committee about fraud, illegal acts, deficiencies in internal control and other audit related matters
- Ascertaining how management is maintaining systems and controls that safeguard the Society's assets, minimise fraud and produce reliable monthly management records
- Understanding how management is effectively managing and reporting the current areas of greatest financial risk
- Reviewing any legal matters which could significantly impact the financial reports
- Reviewing reporting processes, especially in the area of financial reporting, with special reference to accounting and auditing standards
- Reviewing the annual budget

- Reviewing the significant findings and recommendations made by the external auditors are received, discussed and responded to by management on a timely basis
- Monitoring the adequacy of IT systems and their ability to provide relevant, accurate and timely information
- Reviewing proposals and submissions with risk analysis from management and make recommendations to the Board
- Regularly updating the Board about the Committee activities and make appropriate recommendations

Chief Executive Officer (CEO)

The CEO is responsible to the Board for the overall operational management and performance of the State Support Office, St Vincent de Paul NSW Support Services, Ozanam Industries and managers in accordance with the strategy, plan and policies approved by the Board and under the direction of the President (Chairman)

For risk management, the CEO is the champion of the risk management process and is accountable to the Board for risk management and responsible for ensuring:

- Establishment of effective risk management and internal control systems
- Development and implementation of operational policies and procedures for risk management
- Identification and management of the strategic risks
- Identification and management of operational risks throughout the Society
- Report material strategic and business risks to the Audit Risk and Finance Committee
- Review of policies and procedures on a regular basis to ensure they remain effective
- Take timely actions to mitigate/minimise the major risks identified in the risk management process

Executive Officers (including State Support Office, St Vincent de Paul Society NSW Support Services and Central Councils)

- Identify and determine appropriate actions to address operational risks within their area of responsibility
- Monitor progress of risk mitigation action plans for areas that report to them
- Report to the Chief Executive Officer of significant emerging or residual risk
- Ensure all capital works activities contain a risk assessment as part of the approval and implementation process

Managers

- Be accountable for the management of risk within the area of responsibility
- Report to Executive Officers of significant emerging or residual risk
- Manage staff to comply with the Society's policies

Members, Volunteers and Employees

- Report to Managers of significant emerging or residual risk
- Comply with the Society's policies and procedures

Internal Audit and Risk Manager

- Provides advice on the implementation of the Risk Management Policy and to monitor the effectiveness of the policies and procedures for managing risk in the Society
- Maintains the Society's risk register (risk review report)
- Facilitates the risk assessment process in line with the Risk Management Standard
- Develops and implement an effective enterprise wide risk management system, tools and other supporting system
- Reports to the Audit Risk and Finance Committee on the effectiveness of controls in mitigating the risks

Risk Appetite Statement

As defined by the Institute of Risk Management, risk appetite is defined as "the amount of risk the Society is willing to seek or accept in the pursuit of its long term objectives".

In accordance with the level of risk appetite identified in the Statement, the Society is expected to be able to identify and manage the risks associated with activities and opportunities in an effective manner. The Society, in general, is determined to maintain **very low** to **low** risk profile.

The Society recognises the risk appetite / tolerance level for the following areas as very low, which is generally intolerable and should be avoided:

- Legal and compliance – serious breach of legislation and regulatory requirements leading to prosecution and/or fine
- Workplace health and safety – major incidents leading to fatalities or serious injury to members, volunteers and employees

- Fraud and theft – committing internal fraud, collusion, theft by members, volunteers and employees which have significant negative impact to Society's reputation

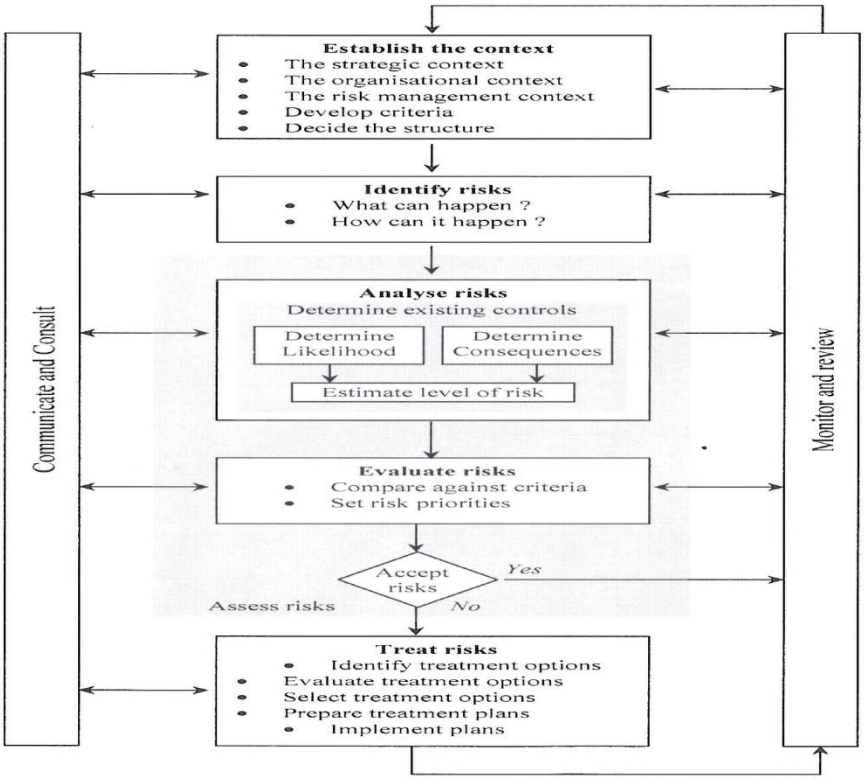
The Society recognises the risk appetite / tolerance level for the following areas as low, which is undesirable and can only be tolerated if it is not reasonably practicable to reduce the risk further:

- Financial and resource management – improper management leading to significant waste of Society's funds
- Information technology strategy and infrastructure – system failures and security breaches resulting disruption of service and leaking of sensitive information
- Investment management – not adopting investments in line with the National Council's Investment Policy plus NSW Addendum
- Physical security – significant loss of assets and resources to fulfil the Society's mission and strategies

The Risk Appetite Statement is reviewed every two years. Further details on risk appetite and risk profiles are noted in the Risk Management Review Report (Risk Register).

Risk Management Process

This risk management process is based on AS/NZS ISO 31000: 2009.



Establish the context

This relates to the strategic and/or operational organisational environments where the Society establishes objectives in order to meet its corporate vision. The context at project level, such as capital projects, relates to internal and external impacts upon each project's objectives.

Risk Identification

Risks can be internally or externally driven. Examples of risks which are internally driven are recruitment, people skills, fraud, investment strategy and governance etc.

Examples of risks which are externally driven are change of accounting standards, investment/economic environment, new technology development and change of Government policy etc.

Risk Analysis

Identified risks are analysed to determine the contributing factors and to consider what the raw impact may be should the risk has realised.

Refer to the Risk Management Review Report for details on the contributing factors and the raw impact for the potential risks identified

Risk Evaluation

The assessment of risk within the Society has been performed under two categories: Strategic Risk (S) and Operational Risk (O). For each risk identified, the review has, with the assistance of management, sought to identify the risk management processes pertaining to each risk.

- **Impact:** the amount of loss or damage if the risk happened (EXTREME, HIGH, MEDIUM, LOW). "Extreme" means "Risk almost sure to happen and/or to have very dire consequences. "High" means "Risks likely to happen and/or to have serious consequences. "Medium" means "Possible this could happen and/or have moderate consequences. "Low" means "Unlikely to happen and/or have minor or negligible consequences".

- **Likelihood**: chance of the risk happening (HIGH, MEDIUM, LOW). "High" means "almost certain". "Medium" means "high probability it will happen once a year". "Low" means "unlikely, but not impossible".

- **Manageability**: how easily could the system/process be managed to improve controls (HIGH, MEDIUM, LOW), e.g., a process requiring high degree of management and/supervision would have a manageability of "HIGH".

Having identified the risks involved, Chief Executive Officer and Executive Officers need to be assessed or measured in terms of the chance (likelihood) they will occur and the severity or amount of loss or damage (impact) which may result it they do occur. The residual risk associated with an event is a combination of the chance (likelihood) that the event will occur and the seriousness of the damage (impact) it may do as well as the manageability of the risk, i.e., how is the risk being managed and/or minimized.

Risk Treatment

Risk treatment process involves identifying the options to deal with the risks, assessing those options, preparing risk treatment plans and implementing them. Options may include:

- Avoid the risk by not undertaking the activity
- Take or increasing risk in order to pursue an opportunity
- Take actions to reduce likelihood and consequences
- Sharing the risk with another party e.g. insurance company / security company

The risk appetite from the Board provides a directive for the risk treatment option for each risk category.

Monitor and Review Risks and Controls

Risks must be continuously monitored and reviewed. The effectiveness of controls to mitigate the risk can be reviewed via the internal audit process.

Performance Evaluation

The Audit Risk and Finance Committee will monitor and evaluate the performance in relation to risk management. This will be done via the internal audit covering:

- The effectiveness of the implementation of risk management policies and procedures
- Awareness of managers of their responsibilities in relation to risk management
- The currency and validity of risk assessment / rating

Authority

This Policy is approved by the Board after consultation with the Audit Risk and Finance Committee.

Review

The effectiveness of this policy will be reviewed after two years of coming into operations by the Internal Audit and Risk Manager or as per instruction by the Audit Risk and Finance Committee.

Related Policies

St Vincent de Paul Society NSW, Risk Management Framework, 2013

St Vincent de Paul Society NSW, Risk Management Review Report, 2011

References

AS/NZS ISO: 31000:2009 Risk Management – Principles and Guidelines

St Vincent de Paul Society NSW, Audit Risk and Finance Committee Charter, September 2012

St Vincent de Paul Society NSW, Board Charter (Governance Statement), June 2013