RISK MANAGEMENT POLICY

POLICY NAME:	Risk Management Policy
NUMBER:	
ORIGINAL DATE:	DRAFT July 2019
LAST REVIEWED:	

PURPOSE

This policy aims to ensure that the activities of Swan Districts Football Club are undertaken within Board approved risk appetite and tolerance.

In particular, the purpose of the risk management policy is to:

- ensure SDFC's business, football and community strategies and plans are appropriate in light of the risks associated with the economic, social, legal and regulatory environment in which the business operates;
- Provide a means of identifying priorities and allocating resources effectively and efficiently.

BACKGROUND

Swan Districts Football Club (SDFC) recognises that embedding risk management principles and practices into strategy development and day-to-day operational processes and decision-making is critical to achieving robust and proactive business, football and community outcomes – a balance between mitigating threats and exploiting opportunities.

Application of Policy

The Risk Management Policy applies to all Board members, Executives, Managers, employees, players, volunteers and contractors of SDFC.

Risk Management Framework

SDFC's Risk Management Framework comprises:

1. **A Risk Management Policy**.
   Adopted by the Board and outlining SDFC's risk management philosophy, which ensures risk management:
   (i) is a critical element of the governance and management of the organisation;
   (ii) becomes a way of thinking for everyone engaged in SDFC's operations; and
   (iii) is supported by guidelines and systems, the effective implementation of which is monitored and reviewed on an on-going basis.

2. Risk Management Guidelines.

These Guidelines outline SDFC's system of internal processes and procedures for implementing appropriate risk management practices. This includes:

(i) risk appetite and tolerances;

(ii) roles and responsibilities of key SDFC personnel; and

(iii) processes and procedures for identifying, communicating and managing risks.

3. Risk Register.

Developing and maintaining of a Risk Register is a critical step towards an effective risk management system.

The Finance and Risk Committee, established by the Board, oversees the management of the business risks of SDFC and will, amongst other things, monitor the development and maintenance of the Risk Register. The Chair of the Finance and Risk Committee is responsible for preparing and presenting the Risk Register to the Board.

Types of risk ratings

Under both ISO 31000:2009 and ISO Guide 73, the definition of "risk" is "effect of uncertainty on objectives".

1. Inherent risk rating

Inherent risk rating is the natural level of risk inherent in a process or activity without any controls or treatments.

2. Residual risk rating

Residual risk rating is the level of risk taking into consideration controls and treatments that have been implemented.

The concepts of Inherent and Residual Risk are linked to clearly understanding "Acceptable levels of risk" (based on Residual risk rating) and key control dependencies. A sizeable gap between Inherent risk rating and Residual risk rating indicates a key control is in place. It is important to ensure key controls are designed and operating effectively to ensure the residual risk rating can be relied upon.

POLICY/ PROCEDURE

1. SDFC recognises that risk management is an integral part of sound management practice and good corporate governance as it improves decision making and enhances outcomes and accountability;

2. SDFC will ensure risk management is an integral part of all our decision-making processes;

3. SDFC will use a structured risk management program to minimise reasonably foreseeable disruption to operations, harm to people and damage to the environment and property;

4. SDFC will identify and take advantage of opportunities as well as minimising adverse effects;

5. SDFC will raise the awareness of all Board members, executives, managers, employees, volunteers, players and contractors concerning risk management within the business;

6. SDFC will train our people to implement risk management effectively; and SDFC will strive to continually improve our risk management practices.

7. SDFC will identify and assess risks based on both inherent risk rating and residual risk ratings. Via the risk rating process, key controls will be identified and recorded. Key controls will be assigned an owner who will be responsible for ensuring the control continues to operate effectively.

8. SDFC will assess residual risk and describe controls in place for inherent risk.

9. Previously identified risks must be regularly reviewed for changes in the environment that may impact the inherent risk rating and therefore require management actions.

10. Tolerances will be defined for various levels of governance at which residual risk levels can be accepted. Residual Risks ratings beyond delegated tolerance levels must be either reduced further or reported to higher levels of governance.

Responsibilities

The Board has responsibility for risk management and for determining the acceptable level of risk for the SDFC. The Board will oversee risk management through the Finance and Risk Committee.

The Finance and Risk Committee will:

1. Advise and assist the Board in assessing risk factors and risk mitigation strategies;
2. Monitor the internal and external risk environments of SDFC; and
3. Review, at least annually, how effectively SDFC has implemented its Risk Management Policy, and report to the Board on its findings.

The Chief Executive Officer and Senior Team will ensure staff understand their responsibilities with respect to risk and will assist in fostering a risk aware culture within their area of responsibility.

Process
Risks will be managed according to the SDFC's Risk Management Guidelines which are set out in Appendix E.

Monitoring and Review
The Finance and Risk Committee will monitor and review the implementation of the Risk Management Framework including this policy.

Implementation & Review
The Chief Executive Officer is accountable for ensuring this Policy is implemented on behalf of the Board. The Chief Executive Officer and Finance and Risk Committee will review this policy as required.

Reporting
The Finance and Risk Committee is responsible for providing the board with monthly risk update reports and an annual risk report.

Risk Ratings
Risk Ratings should be assessed by estimating:

a) the likelihood of a risk eventuating (becoming an issue) and
b) the consequence to the business should the risk eventuate.

The rating can be determined by finding the corresponding position in the Risk Assessment Matrix. There is no exact science to scoring the likelihood and consequence ratings. The guidance tables and matrix in this Policy should be used as a guide to the assessment. The intention is to form a rating so that action can be taken where necessary in the best interests of the business.

Delegated tolerances
Tolerances are defined for various levels of governance at which residual risk levels can be accepted. Residual Risks ratings beyond delegated tolerance levels must either reduced further or reported to higher levels of governance.

APPENDIX A - GUIDANCE FOR ASSESSING RISK CONSEQUENCES

This rating guidance applies to assessing both the inherent risk and the residual risk (following treatments). A change in residual risk rating consequence will indicate that the treatment reduces the consequence of the risk.

Level	Descriptor	Description detail
5	Catastrophic	Death. Significant impact on the community lasting longer than 12 months. Severe reputational damage. Financial loss Over $500,000
4	Major	Extensive injuries. Serious Impact on community. Serious reputational damage. Major financial loss $200,000 - $500,000
3	Moderate	Medical treatment required. Moderate community impact. Moderate reputation risk with low media attention. Financial loss $50,000 - $200,000
2	Minor	First aid treatment. Low Community Impacts with no media coverage. Low reputation risk with possible complaint. Financial loss $5,000 - $50,000.
1	Insignificant	No injuries. Low financial loss. No reputation risk. No Community impact. Financial loss $1 - $5,000.

APPENDIX B - GUIDANCE FOR ASSESSING RISK LIKELIHOOD

This rating guidance applies to assessing both the inherent risk and the residual risk (following treatments). A change in residual risk rating consequence will indicate that the treatment reduces the likelihood of the risk eventuating.

Level	Descriptor	Description detail
5	Almost Certain	Likely to occur within a 1 year period.
4	Likely	Likely to occur within a 1 - 5 year period.
3	Possible	Likely to occur within a 5 - 20 year period.
2	Unlikely	Likely to occur within a 20 - 50 year period.
1	Rare	Not likely to occur within a 50 year period.

APPENDIX C - RISK RATING MATRIX

This rating guidance applies to assessing both the inherent risk and the residual risk (following treatments). Risks are rated as

- Low,
- Medium,
- High or
- Extreme

Based on the position of the Likelihood and Consequence ratings using the Risk Rating Matrix table below.

	Consequence				
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Rare	Low	Low	Medium	High	High
Unlikely	Low	Low	Medium	High	Extreme
Possible	Low	Medium	High	Extreme	Extreme
Likely	Medium	High	High	Extreme	Extreme
Almost Certain	High	High	Extreme	Extreme	Extreme

APPENDIX D – TOLERANCES FOR ACCEPTING RESIDUAL RISK RATINGS

This rating guidance applies to assessing both the inherent risk and the residual risk (following treatments).

Residual Risk Rating	Delegated Governance Level at which Residual Risk Rating can be Accepted (otherwise requires further Treatment)	Mandatory Reporting
Extreme	Board	Report immediately to CEO & Board President. President to advise Board ASAP
High	Board	Report immediately to CEO & Board President. President to advise Board at the next Board Meeting
Medium	Senior Management Team	Report Immediately to a Manager and CEO. Notify Board at CEO's discretion
Low	Employee	Report Immediately to Immediate Manager. Immediate Manager to use discretion in notifying CEO

APPENDIX E - RISK MANAGEMENT GUIDELINES

SDFC Risk Management Guidelines

The following is adapted from the Standards Australia's AS/NZS ISO 31000:2009 Risk management - Principles and Guidelines. There are six steps to consider in the development of an effective risk management plan:

1. Describe the activity / risk context
2. Identify the risks
3. Analyse the risks
4. Evaluate the risks
5. Manage the risks and reassess, and
6. Review

The Risk Management Process

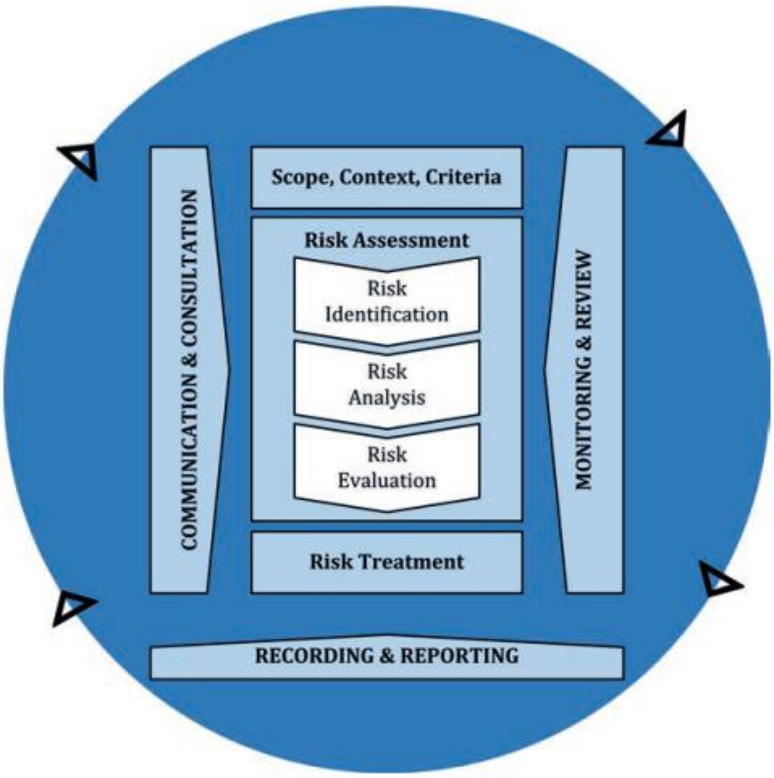

Figure 4 — Process

Establish the risk context

This step establishes the strategic, organisational and risk management context for the rest of the process.

- The strategic context defines the relationship between the organisation and its environment covering financial, operational, competitive, social, political, customer, legal and cultural aspects. The risk management is closely linked to the enterprise's mission or strategic objectives.
- The organisational context describes the organisation and its capabilities.
- The risk management context determines the goals, objectives, strategies, scope and parameters of the activity.
- Risk assessment criteria i.e. decisions concerning risk acceptability and risk treatment, are established for likelihood, consequences and controls; and the level of tolerance to risk is established.
- The framework for risk management is defined:
  - The classification of risks and key consequences are defined;
  - The scope, objectives, terminology and methodology are clarified;
  - The available budget/financing is determined.

Identify risks

This step identifies the risks to be managed:

- Identify the risks that can happen
- Describe risks by determining the possible causes and scenarios.

Techniques used to identify risks include checklist, records, experience, brainstorming, structured workshops, systems analysis and scenario analysis.

Analyse risks

The objective of risk analysis is to classify from minor to major:

- Assess the relative likelihood of occurrence of the risk
- Identify the existing and new controls that reduce the likelihood or consequence of the risk;
- Identify the potential consequences and assess their severity in terms of magnitude for each risk.
- Identify the cost of controls;
- Assess the adequacy and evaluate the importance and benefits of the controls;
- Produce the estimated risk level by combining the assessment of likelihood and consequences, in the context of existing control measures.

The initial priorities of the risks are then determined using a matrix to combine likelihood and consequence included in the Risk Matrix.

Techniques should be used to determine the consequences and the likelihood of events: past records, experience, industry practice, statistics, market research, experiments, models, judgements.

Risk analysis may be qualitative, semi-quantitative or quantitative:

- qualitative analysis uses descriptive scales to describe the magnitude of potential consequences (minor, moderate, major) and the likelihood of occurrence (likely, possible, unlikely).
- semi-quantitative analysis allocates numbers to the descriptive scales, allowing the use of formulas for prioritisation
- quantitative analysis uses numerical values: consequences are expressed in terms of monetary or other criteria and likelihood as a probability, a frequency or a combination of exposure and probability

Evaluate risks
Risk evaluation will determine a prioritised list of risk for further action:
- Compare risk exposure levels against predetermined tolerance level;
- Assess existing levels of exposure in terms of the levels of exposure reduction that are achievable;
- Rank the risks to establish management priorities.

Treat risks
Risk treatment consists of determining what will be done in response to the identified risks.
- Treatments are selected from the following treatment option:
  - Accept risk;
  - Avoid risk by deciding not to proceed with the activity;
  - Transfer risk (partially or fully) to another party e.g. insurance, joint ventures, partnerships;
  - Reduce likelihood of occurrence;
  - Reduce consequences; and
  - Retain the risk. After risk treatment, a residual risk may be retained.

- Asses treatment options:
  - Consider feasibility costs and benefits. The costs must be reasonable with the benefits obtained.
  - Recommend treatment strategies. A combination of treatment options will often be required.
  - Select treatment strategies by priority ordering based on risk ranking or cost-benefit analysis.
- Treatment plans are developed by considering responsibilities, schedules, available budget, benefits arising from actions/controls, performance measures.
- Manage and monitor the implementation of the action plan.

Monitor and review
Monitoring and reviewing is an integral part of the risk management treatment plan.
- Monitor the effectiveness of the mitigation task through the treatment plans, strategies and management information systems;
- Review all steps in the process identifying any new risks and changes to the current assessments and existing position.
- Ongoing evaluations to verify that the mitigation plan remains relevant, when circumstances are changing.

A risk register database is the main management tool for monitoring risk. It contains a ranked list of risks, references to associated risk action plans and names of individuals responsible for each risk. Regular updating of the risk register should be part of the ongoing project management process.

Communicate and consult
Communication and consultation are important element of the risk management process:
- Undertaken at each step of the process;
- Involves internal and external stakeholders; and
- Clarify the responsibilities of each stakeholder.

References:
• Policy and Procedure Framework • Risk Management Guidelines ASNZ ISO 31000:2009

Version	Date Approved	Approver	Description of revision
1			