**RISK AND CRISIS MANAGEMENT RESOURCE**

October 2020

# Background

New South Wales State Sporting Organisation (SSOs) boards and management (whether paid or volunteer) should turn their minds towards governance for recovery and not lose sight of their overarching role and responsibility for good organisational governance, purpose and strategic direction and planning.

There are many learnings from COVID-19 for boards and management of SSOs. Some areas for review for SSOs include:

# Planning

* How SSOs plan for future disasters/pandemics will have direct implications on the continuity and recovery of their sport as well as their long-term viability and sustainability.
* Crisis management plans (CMP) and business continuity plans (BCP) should be developed or reviewed and updated to reflect learnings from COVID-19. These plans should be updated frequently, to capture new information and COVID-19 measures around sport sector standards, best practice and any vulnerabilities or structural changes caused by COVID-19.
* In responding to the impact of COVID-19, what was done well and what was done poorly by your organisation?
* SSOs should review existing plans and develop new robust plans including a Sport BCP and Disaster Recovery Planning (DRP) to all operational areas of the sport business?

# Risk Management

* COVID-19 has caused significant risks to SSOs including financial stability, decline, suspending or terminating operational capability, decreased capacity to meet contractual obligations and commercial relationships and workforce layoffs.
* Risk management is a director and board responsibility. SSOs must 'speed up' day-to-day risk management to be more dynamic and forward-looking. It must remain relevant and play a more frontline role in general management and decision making by directors and boards of SSOs.
* Does your risk management framework cater for once in a generation events like COVID-19?
* Did COVID-19 highlight other risks, such as sport delivery, supply chain, operating model, financial or personnel risks that should be addressed by your sport?
* Can WH&S policies be updated as a positive long-term shift rather than a temporary reaction to COVID-19?

# Financial resilience

* Consolidating the SSO’s financial position is critical during times of crisis. This requires consideration around existing and future sources of funding as economic and political climates shift in response to COVID-19.
* SSOs should access their short, immediate, and long-term financials?
* Questions to ask include:
  + Review our operating model to better understand and be aware of their current trading and cash flow position.
  + What is our funding mix and how has COVID-19 impacted this?
  + What is the relative reliance on membership fees, government grants, corporate support, donations and philanthropy and event fundraising? Will support-in-kind become just as valuable as financial donations?
  + Is there sufficient cash to pay costs over the short and long term? Is it prudent to cut non-essential and discretionary expenditure?
  + Is it possible to move accepting income online?
  + Should we consider philanthropy or fundraising events as income streams other than direct sponsorships?
* What innovation initiatives can be developed and implemented to support and retain employees and members in the face of any future constraints?
* SSOs must regularly review cash reserves and understand what amounts are tied to grants and what amounts can be drawn upon if required. A detailed understanding of expenses in the sport business is critical, so decisions can be made on where to adjust spending to improve the forecast cash position.
* Within the risk management decision-making and reporting framework SSOs should regularly analyse their financial health.
* Making profits and accumulating wealth to invest in survival during the next disaster could be the new ‘norm’.

# Other SSO considerations

## Stakeholder relations and external communications

* COVID-19 has exposed the importance of SSOs relying on continued support from key stakeholders, whether in the form of financial support from members, sponsors, government, and pro-bono partners maintaining their existing commitments or engaging in productive dialogue with government and regulators.
* Boards must be more mindful of competing stakeholder expectations and ensuring an effective communication strategy is in place.
* What are stakeholders focused on? Does their focus align with your sport’s purpose, strategy, and business plan? The answer may be different for each stakeholder ranging from the interests of clients, employees, volunteers, sponsors to community partners.
* Will stakeholders support the SSO changing its focus, whether temporarily or permanently? Are they adequately updated on any significant changes to our organisation?
* Does the communication strategy focus both on the immediate response to the crisis, as well as longer term and post-COVID-19 purpose and strategy?
* Is the sport maintaining regular engagement with key regulatory agencies e.g. ACNC, ATO, ASIC and State OFT/Consumer Affairs – to ensure that any changes in regulatory focus do not come as a surprise?
* Is the sport complying with new and changing regulatory responses to COVID-19 whilst continuing to comply with existing legal and regulatory requirements?

## Digital presence, technology capabilities and cybersecurity

* SSOs must have a strong digital presence and technology capability.
* Does the sport’s technology platform support remote, flexible, or work from home arrangements for personnel (employees and volunteers)?
* Is the sport cyber secure to protect the organisation and its personnel?
* How have member behaviours changed – or digitisation trends been accelerated – because of COVID-19?

## Strategic partnerships and other opportunities

* Are there strategic partnerships – possibly with other SSOs, NFPs or community partners – that will support and strengthen the SSO into the future? This may deliver benefits ranging from consolidating and strengthening sport product and supply chains, cost reductions and the sharing of knowledge, expertise, or resources.
* Should your sport restructure? Reducing the number of ancillary services which are already better served by other SSOs or other NFPs organisations may resharpen the focus on core strategy and mission statement.
* Has COVID-19 presented any opportunities or challenges unique to our sport sector or organisation? How can your sport leverage or overcome these?
* SSOs should review and update existing SSO strategic and business plans to reflect the short-term impact of COVID-19 and changes to their organisation's operating environment, especially around changes in the focus and expectations of the community, members, and volunteers.
* SSOs should refocus their attention on their primary governance role. SSO boards must look forward and plan the 'road to recovery', ensure their mission statement, purpose and strategic direction remains fit for purpose and maintain adequate oversight and management of key risks and opportunities for the organisation beyond COVID-19.

Introduction to this resource

This resource has been prepared by the NSW Office of Sport to assist State Sporting Organisation (**SSOs**) respond to COVID-19 and assess the impacts, particularly long-term, of COVID-19 on SSO’s strategic objectives and their resilience to respond. It also seeks to assess SSOs’ response from a risk management perspective.

The document has been designed specifically for sport. It is a governance document and your board should take ultimate responsibility for it. It should however be able to be used by volunteers and personnel alike.

As with any legal document, this does not replace obtaining legal advice on your specific requirements.

SSOs are encouraged to use this resource in the management of their risk in the context of crisis and to adopt an organisational approach to risk and crisis management by encouraging affiliates and clubs to consider use of this resource.

Key definitions

**Business continuity planning** is the process of creating systems of prevention and recovery to deal with potential threats to an organisation. In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.

**Consequence** is the outcome of an event affecting objectives.

**Crisis** means a time of intense difficulty or danger.

**Crisis management** is the process by which an organisation deals with a disruptive and unexpected event that threatens to harm the organisation or its stakeholders.

**Disaster** means a sudden accident or natural catastrophe that causes great damage or loss of life.

**Likelihood** is the chance of something happening.

A **recovery plan** should enable an effective response if a crisis affects your organisation. It should shorten recovery time and minimise losses. A recovery plan contains information relating to planning for recovery as well as the resumption of critical business activities after a crisis has occurred.

**Risk** is the effect of uncertainty on objectives.

**Risk management** are coordinated activities to direct and control an organisation with regard to risk.

**Stakeholders** are persons and organisations that can affect, be affected by, or perceive themselves to be affected by, a decision or activity.

**Standard** means ISO 31000:2018 Risk management.

**DISCLAIMER:  
THE INFORMATION PROVIDED IN THIS RESOURCE IS FOR YOUR INFORMATION ONLY. THE AUTHORS AND NSW OFFICE OF SPORT ACCEPT NO RESPONSIBILITY FOR THE ACCURACY OF THE INFORMATION OR YOUR RELIANCE UPON IT.**

Reviewed (October 2020) by:  
  


|  |
| --- |
| PO Box 1059 Hampton North VIC 3188 Tel: 0428 082 087 E-mail: lexsportiva@icloud.com |

[Background 2](#_Toc54618132)

[1 Planning 2](#_Toc54618133)

[2 Risk Management 2](#_Toc54618134)

[3 Financial resilience 3](#_Toc54618135)

[4 Other SSO considerations 3](#_Toc54618136)

[4.1 Stakeholder relations and external communications 3](#_Toc54618137)

[4.2 Digital presence, technology capabilities and cybersecurity 4](#_Toc54618138)

[4.3 Strategic partnerships and other opportunities 4](#_Toc54618139)

[Introduction to this resource 6](#_Toc54618140)

[1 Risk management framework 10](#_Toc54618141)

[1.1 Leadership and commitment 10](#_Toc54618142)

[2 Preparing a risk management plan and business impact analysis 13](#_Toc54618143)

[3 Identify risks to your business 14](#_Toc54618144)

[3.1 Assessing your business 14](#_Toc54618145)

[3.2 Ways of identifying risk 14](#_Toc54618146)

[4 Analyse and evaluate the impact of risks 15](#_Toc54618147)

[4.1 Analysing the level of risk 15](#_Toc54618148)

[4.2 Evaluating risks 16](#_Toc54618149)

[5 Treat risks to your business 16](#_Toc54618150)

[5.1 Avoid the risk 16](#_Toc54618151)

[5.2 Reduce the risk 16](#_Toc54618152)

[5.3 Transfer the risk 17](#_Toc54618153)

[5.4 Accept the risk 17](#_Toc54618154)

[6 Review and update your risk management plan 17](#_Toc54618155)

[7 Conduct a business impact analysis 18](#_Toc54618156)

[7.1 Critical business activities 18](#_Toc54618157)

[7.2 Key questions in a business impact analysis 18](#_Toc54618158)

[8 RISK MANAGEMENT POLICY 19](#_Toc54618159)

[8.1 Rationale 19](#_Toc54618160)

[8.2 Introduction 19](#_Toc54618161)

[8.3 Risk responsibility 19](#_Toc54618162)

[8.4 Risk identification 20](#_Toc54618163)

[8.5 Risk management and compliance and control 20](#_Toc54618164)

[8.6 Assessment of effectiveness 20](#_Toc54618165)

[8.7 Reporting 20](#_Toc54618166)

[8.8 Review 20](#_Toc54618167)

[8.9 Risk Appetite 20](#_Toc54618168)

[8.10 Risk management 25](#_Toc54618169)

[8.11 Critical business area analysis 26](#_Toc54618170)

[8.12 Scenario planning 27](#_Toc54618171)

[8.13 Insurance 29](#_Toc54618172)

# Risk management framework

The components of the framework and the way in which they work together should be customized to the needs of the organisation.

## Leadership and commitment

Management and oversight bodies, where applicable, should ensure that risk management is integrated into all organisational activities and should demonstrate leadership and

commitment. Management is accountable for managing risk while oversight bodies are accountable for overseeing risk management.

Integration

Integrating risk management relies on an understanding of organisational structures and context. Structures differ depending on the organisation’s purpose, goals and complexity. Risk is managed in every part of the organisation’s structure. Everyone in an organisation has responsibility for managing risk.

Governance guides the course of the organisation, its external and internal relationships, and the rules, processes and practices needed to achieve its purpose. Management structures translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability. Determining risk management accountability and oversight roles within an organisation are integral parts of the organisation’s governance.

Integrating risk management into an organisation is a dynamic and iterative process, and should be customized to the organisation’s needs and culture. Risk management should be a part of, and not separate from, the organisational purpose, governance, leadership and commitment, strategy, objectives and operations.

Design

Understanding the organisation and its context

When designing the framework for managing risk, the organisation should examine and understand its external and internal context. Examining the organisation’s external context may include, but is not limited to:

* the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
* key drivers and trends affecting the objectives of the organisation;
* external stakeholders’ relationships, perceptions, values, needs and expectations;
* contractual relationships and commitments;
* the complexity of networks and dependencies.

Examining the organisation’s internal context may include, but is not limited to:

* vision, mission and values;
* governance, organisational structure, roles and accountabilities;
* strategy, objectives and policies;
* the organisation’s culture;
* standards, guidelines and models adopted by the organisation;
* capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
* data, information systems and information flows;
* relationships with internal stakeholders, considering their perceptions and values;
* contractual relationships and commitments;
* interdependencies and interconnections.

Articulating risk management commitment

Top management and oversight bodies, where applicable, should demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey an organisation’s objectives and commitment to risk management. The commitment should include, but is not limited to:

* the organisation’s purpose for managing risk and links to its objectives and other policies;
* reinforcing the need to integrate risk management into the overall culture of the organisation;
* leading the integration of risk management into core business activities and decision-making;
* authorities, responsibilities and accountabilities;
* making the necessary resources available;
* the way in which conflicting objectives are dealt with;
* measurement and reporting within the organisation’s performance indicators;
* review and improvement.

The risk management commitment should be communicated within an organisation and to stakeholders, as appropriate.

Assigning organisational roles, authorities, responsibilities and accountabilities

Top management and oversight bodies, where applicable, should ensure that the authorities, responsibilities and accountabilities for relevant roles with respect to risk management are assigned and communicated at all levels of the organisation, and should:

* emphasize that risk management is a core responsibility;
* identify individuals who have the accountability and authority to manage risk (risk owners).

Allocating resources

Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to:

* people, skills, experience and competence;
* the organisation’s processes, methods and tools to be used for managing risk;
* documented processes and procedures;
* information and knowledge management systems;
* professional development and training needs.

The organisation should consider the capabilities of, and constraints on, existing resources.

Establishing communication and consultation

The organisation should establish an approved approach to communication and consultation in order to support the framework and facilitate the effective application of risk management. Communication involves sharing information with targeted audiences. Consultation also involves participants providing feedback with the expectation that it will contribute to and shape decisions or other activities. Communication and consultation methods and content should reflect the expectations of stakeholders, where relevant.

Communication and consultation should be timely and ensure that relevant information is collected, collated, synthesised and shared, as appropriate, and that feedback is provided and improvements are made.

Implementation

The organisation should implement the risk management framework by:

* developing an appropriate plan including time and resources;
* identifying where, when and how different types of decisions are made across the organisation, and by whom;
* modifying the applicable decision-making processes where necessary;
* ensuring that the organisation’s arrangements for managing risk are clearly understood and practised.

Successful implementation of the framework requires the engagement and awareness of stakeholders. This enables organisations to explicitly address uncertainty in decision-making, while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.

Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities throughout the organisation, including decision-making, and that changes in external and internal contexts will be adequately captured.

Evaluation

In order to evaluate the effectiveness of the risk management framework, the organisation should:

* periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour;
* determine whether it remains suitable to support achieving the objectives of the organisation.

Improvement

The organisation should continually monitor and adapt the risk management framework to address external and internal changes. In doing so, the organisation can improve its value.

The organisation should continually improve the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.

As relevant gaps or improvement opportunities are identified, the organisation should develop plans and tasks and assign them to those accountable for implementation. Once implemented, these improvements should contribute to the enhancement of risk management.

Risk profile

The risk profile of an organisation informs all aspects of the approach to leading and managing its risks.  Every organisation will have its own risk profile. This is the starting point for determining the greatest risks for some SSOs the risks will be tangible and immediate safety or pandemic hazards, whereas in other organisations the risks may be health-related and it may be a long time before the illness becomes apparent.

A risk profile examines:

* the nature and level of the threats faced by an organisation
* the likelihood of adverse effects occurring
* the level of disruption and costs associated with each type of risk
* the effectiveness of controls in place to manage those risks.

The outcome of risk profiling will be that the right risks have been identified and prioritised for action, and minor risks will not have been given too much priority. It also informs decisions about what risk controls measures are needed.

# Preparing a risk management plan and business impact analysis

The process of identifying risks, assessing risks and developing strategies to manage risks is known as risk management. A risk management plan and a business impact analysis are important parts of your business continuity plan. By understanding potential risks to your business and finding ways to minimise their impacts, you will help your business recover quickly if an incident occurs.

Types of risk vary from business to business, but preparing a risk management plan involves a common process. Your risk management plan should detail your strategy for dealing with risks specific to your business.

It is important to allocate some time, budget and resources for preparing a risk management plan and a business impact analysis. This will help you meet your legal obligations for providing a safe workplace and can reduce the likelihood of an incident negatively impacting on your business.

# Identify risks to your business

The first step in preparing a risk management plan is to identify potential risks to your business. Understanding the scope of possible risks will help you develop realistic, cost-effective strategies for dealing with them.

It's important that you think broadly when considering types of risks for your business, rather than just looking at obvious concerns (e.g. fire, theft, market competition).

## Assessing your business

Before you begin identifying risks, you need to assess your business. Think about your critical business activities, including your key services, resources and staff, and things that could affect them, such as power failures, natural disaster and illness. Assessing your business will help you work out which aspects you couldn't operate without.

## Ways of identifying risk

Once you have a clear picture of your business, you can begin to identify the risks. Review your business plan and think about what you couldn't do without, and what type of incidents could impact on these areas. Ask yourself:

* when, where, why and how are risks likely to happen in your business?
* are the risks internal or external?
* who might be involved or affected if an incident happens?

The following are some useful techniques for identifying risks.

Ask 'what if?' questions

Thoroughly review your business plan and ask as many 'what if?' questions as you can. Ask yourself what if:

* you lost power supply?
* you had no access to the internet?
* Key documents were destroyed?
* your premises was damaged or you were unable to access it?
* one of your best staff members quit?
* Your suppliers went out of business?
* the area your business is in suffered from a natural disaster?
* the services you need, such as roads and communications, were closed?

Brainstorm

Brainstorming with different people, such as your accountant, financial adviser, staff, suppliers and other interested parties, will help you get many different perspectives on risks to your business.

Event analysis

Think about other events that have, or could have, affected your business. What were the outcomes of those events? Could they happen again? Think about what possible future events could affect your business. Analyse the scenarios that might lead to an event and what the outcome could be. This will help you identify risks that might be external to your business.

Assess process

Use flow charts, checklists and inspections to assess your work processes. Identify each step in your processes and think about the associated risks. Ask yourself what could prevent each step from happening and how that would affect the rest of the process.

Consider worst case scenario

Thinking about the worst things that could happen to your business can help you deal with smaller risks. The worst case scenario could be the result of several risks happening at once. For example, someone running a restaurant could lose power, which could then cause the food to spoil. If the restaurant owner was unaware of the power outage or the chef decided to serve the food anyway, customers could get food poisoning and the restaurant could be liable and suffer from financial losses and negative publicity.

Once you've identified risks relating to your business, you'll need to analyse their likelilood and consequences and then come up with options for managing them.

# Analyse and evaluate the impact of risks

Once you have identified the risks to your business, you need to assess the possible impact of those risks. You need to separate minor risks that may be acceptable from major risks that must be managed immediately.

## Analysing the level of risk

To analyse risks, you need to work out the likelihood of it happening (frequency or probability) and the consequences it would have (the impact) of the risks you have identified. This is referred to as the level of risk, and can be calculated using this formula:

**level of risk = consequence x likelihood**

Level of risk is often described as low, medium, high or very high. It should be analysed in relation to what you are currently doing to control it. Keep in mind that control measures decrease the level of risk, but do not always eliminate it.

## Evaluating risks

Once you have established the level of risk, you then need to create a rating table for evaluating the risk. Evaluating a risk means deciding about its severity and ways to manage it.

Your risk evaluation should consider:

* the importance of the activity to your business
* the amount of control you have over the risk
* potential losses to your business
* any benefits or opportunities presented by the risk.

Once you have identified, analysed and evaluated your risks, you need to rank them in order of priority. You can then decide which methods you will use to treat unacceptable risks.

# Treat risks to your business

Treating risks involves working through options to deal with unacceptable risks to your business. Unacceptable risks range in severity — some risks will require immediate treatment while others can be monitored and treated later.

Your risk analysis and evaluation will help you prioritise the risks that need to be treated. When you are developing a plan for treating the risks, consider the:

* method of treatment
* people responsible for treatment
* costs involved
* benefits of treatment
* likelihood of success
* ways to measure the success of treatments.

How and why you have chosen to treat risks should be outlined in your risk management plan. It's important to review your plan regularly to consider any new risks associated with changes in your business or improvements in techniques for treating risks. The following are different options for treating risks.

## Avoid the risk

If it's possible, you may decide not to proceed with an activity that is likely to generate risk. Alternatively, you may think of another way to reach the same outcome that doesn't involve the same risks. This could involve changing your processes, equipment or materials.

## Reduce the risk

You can reduce a risk by:

* reducing the likelihood of the risk happening — for example, through quality control processes, auditing, compliance with legislation, staff training, regular maintenance or a change in procedures
* reducing the impact if the risk occurs — for example, through emergency procedures, off-site data backup, minimising exposure to sources of risk, or using public relations.

## Transfer the risk

You may be able to shift some or all of the responsibility for the risk to another party through insurance, outsourcing, joint ventures or partnerships. You may also be able to transfer risk by:

* cross-training staff so that more than one person knows how to do a certain task and you don't risk losing essential skills or knowledge if something happens to one of your staff members
* identifying alternative suppliers in case your usual supplier is unable to deliver
* keeping old equipment (after it is replaced) and practising doing things manually in case your computer networks or other equipment can't be used.

Make sure you have adequate insurance

Speak to your insurer to find out if you have the right insurance cover for your business. Be sure to clarify whether you are covered for the risks you have identified in your risk management plan. Keep in mind that insurance policies may have different definitions for certain incidents (e.g. flooding).

You should also check that you:

* have coverage for the loss of income you could incur if customers affected by the crisis stop ordering your product or service
* have appropriate insurance to cover other related issues such as on-site injuries to staff or visitors, or for loss of your customers' goods or materials
* have coverage in case your supplier/s are affected by a crisis and can't deliver necessary supplies for your business
* are meeting your workers’ compensation obligations in case any of your staff are injured in a crisis.

## Accept the risk

You may accept a risk if it can't be avoided, reduced or transferred. Other risks may be extremely unlikely and therefore too impractical or expensive to treat. However, you will need to develop an crisis response plan and a recovery plan to help you deal with the consequences of the risk if it occurs.

# Review and update your risk management plan

You will need to test, evaluate and update your risk management plan regularly as risks can change as your business, your industry and the environment you operate in change. Regularly reviewing your risk management plan is essential for identifying new risks and monitoring the effectiveness of your risk treatment strategies.

Your risk management plan should be part of a broader BCP that includes strategies for responding to and recovering from incidents if they do happen. Making sure your business continuity plan is reliable and up to date will help you resume operations quickly after an incident and reduce the impact to your business.

While you may be able to predict and deal with a large number of potential risks, there will be some that are unexpected or impossible to plan for. Preparing a crisis response plan and a recovery plan as part of your overall BCP can help you deal with these situations if they happen.

A risk management plan is the prevention step in the prevention, preparedness, response and recovery (PPRR) model of business continuity planning.

# Conduct a business impact analysis

Once you have developed a risk management plan, you can conduct a business impact analysis to assess the likely impact of these risks on your business operations. This is the preparedness step in the the prevention, preparedness, response and recovery (PPRR) model of business continuity planning.

## Critical business activities

A business impact analysis identifies the activities in your business operations that are key to its survival. These are referred to as critical business activities. You should consider things such as:

* the records and documents you need everyday
* the resources and equipment you need to operate
* the access you need to your premises
* the skills and knowledge your staff have that you need to run your business
* external stakeholders you rely on or who rely on you
* the legal obligations you are required to meet
* the impact of ceasing to perform critical business activities
* how long your business can survive without performing these activities.

As part of your business impact analysis, you should assign recovery time objectives to each activity to help determine your basic recovery requirements. The recovery time objective is the time from when an incident happens to the time that the critical business activity must be fully operational in order to avoid damage to your business.

Your business impact analysis will help you develop your recovery plan, which will help you get your business running again if an incident does happen.

## Key questions in a business impact analysis

To conduct a business impact analysis for your business, ask yourself:

* What are the daily activities conducted in each area of my business?
* What are the long-term or ongoing activities performed by each area of my business?
* What are the potential losses if these business activities could not be provided?
* How long could each business activity be unavailable for (either completely or partially) before my business would suffer?
* Do these activities depend on any outside services or products?
* How important are the activities to my business? For example, on a scale of 1 to 5 (1 being the most important and 5 being the least important), where would each activity fall in relation to the rest of the business?

As the risks to your business change, so too will their potential impacts. When you update your risk management plan, you will also need to conduct a new business impact analysis.

# RISK MANAGEMENT POLICY

## Rationale

This risk management policy has been developed to assist SSOs achieve the benefits of the identification and management of risks to which it is exposed; particularly in the context of COVID-19 or other crisis. It seeks to articulate the SSO’s focus on and commitment to managing risk.

## Introduction

The directors and administration of the SSO view risk management as integral to its strategic objectives of:

* providing for the conduct, encouragement, promotion and administration of the organisation and the sport;
* increasing participation in the sport;
* growing and diversifying the organisation’s revenues.

This document seeks to set the framework to manage the risks associated with achieving these core strategic objectives. It is designed to identify, assess, monitor and manage risk.

## Risk responsibility

The SSO Board is responsible for overseeing the establishment and implementation of risk management systems and reviewing their effectiveness. The Board’s role in relation to risk includes:

* overseeing the creation, implementation and maintenance of its risk management system and its internal-control framework, including information systems;
* establishing a risk profile and setting out both financial and non-financial material and/or strategic risks facing it;
* reviewing risks on a quarterly basis, including identifying new risks, changes to existing risks and retirement of previously identified risks (through a formal process);
* determining who owns risks, in accordance with function or expertise;
* regular reporting to the Board of the status of risks including relevant treatment(s);
* appraisal of risk owners’ actions taken to manage risk and correct inappropriate performance;
* internal compliance and control systems for the implementation of the risk management plan;
* consideration of non-financial audits; and
* compliance with regulatory requirements and best practice.

## Risk identification

Key risks will be identified and analysed by the organisation who will:

* define risks in the context of its strategic objectives;
* develop risk profiles, including a description of the material risks, the risk level and actions used to mitigate the risk;
* regularly review and update risk profiles.

## Risk management and compliance and control

To develop a culture of risk management, the organisation will determine appropriate responses to manage risk, including implementing risk action plans and a risk register.

Through its Board SSO will:

* implement a systematic process to identify, assess, treat and monitor risk(s);
* provide the necessary tools and resources to support the effective management of risks;
* review and communicate risk management best practice on a regular basis.

## Assessment of effectiveness

The organisation will assess how effective its risk management plan is by undertaking structured continuous improvement processes. This will ensure continual monitoring and review of risks and controls. The appraisal of risk owners in managing risks should be included in these processes.

## Reporting

The organisation will ensure that its Board is regularly informed of significant risk management issues and the actions undertaken to manage risks on a regular basis.

## Review

The Board will review this policy as often as is necessary and will make any changes it determines necessary or desirable.

## Risk Appetite

Introduction

SSO is established to [INSERT]. The activities undertaken in fulfilment of its responsibilities are overseen by [INSERT].

SSO is charged with carrying out its objects in accordance with its Constitution and relevant legislation (Act).

This risk appetite statement considers the most significant risks to which SSO is exposed and provides an outline of the approach to managing these risks. All strategic plans and business plans for functional areas need to be consistent with this Statement.

General Statement of Appetite

SSO faces a broad range of risks reflecting its objectives. These risks include those resulting from [INSERT eg COVID-19, other event], as well as its day-to-day operational activities.

SSO is also exposed to some significant financial risks.

SSO has a low appetite for risk to operational issues. SSO makes resources available to control operational risks to acceptable levels. SSO recognises that it is not possible or necessarily desirable to eliminate some of the risks inherent in its activities. Acceptance of some risk is often necessary to foster innovation and efficiencies within business practices.

The Risk Management Framework

SSO's risk management framework seeks to ensure that there is an effective process in place to manage risk across SSO. Risk management is integral to all aspects of SSO's activities and is the responsibility of all staff. Key staff as well as SSO directors have a particular responsibility to evaluate their risk environment, to put in place appropriate controls and to monitor the effectiveness of those controls. The risk management culture emphasises careful analysis and management of risk in all business processes.

These risks are identified, assessed and managed at both an enterprise level (‘top-down’) and business level (‘bottom-up’). The SSO Board and/or RMC, has oversight of these processes. Such a committee should meet several times a year and provides a report on its activities to the Board.

Coverage

SSO's attitude towards its key strategic, financial, people and operational risks is described below.

Strategic Risks

SSO aspires to [INSERT SSO’S STRATEGIC OBJECTIVES FROM STRATEGIC PLAN]. SSO has a low appetite for threats to the effective and efficient delivery of these initiatives. It recognises that the actual or perceived inability to deliver strategic initiatives could have a significant impact on its ability to achieve its objectives as well as its reputation.

Impact on SSO’s strategic objectives and major response initiatives will be discussed by SSO's Board at every board meeting. A framework is in place to ensure that these initiatives are prioritised appropriately, and that the associated risks are well managed and reported on a consistent basis.

Financial Risks

SSO has a very low appetite for financial risk. SSO manages this risk carefully by applying a strict set of financial management criteria to its operations.

Integrity

SSO has no appetite for any behaviour which is likely to effect the integrity and reputation of SSO and its Sport. SSO is committed to deterring and preventing such behaviour. It takes a very serious approach to cases, or suspected cases, of fraud or corruption perpetrated by its staff, and responds fully and fairly in accordance with provisions of its codes of conduct and relevant integrity policies.

People and Culture Risks

SSO's significant people and culture-related risks include:

* **Calibre of People** – SSO relies on motivated, diverse and high-quality staff and volunteers to perform its functions. It aims to create an environment where staff are empowered to the full extent of their abilities.
* **Conduct of People** – SSO expects staff to conduct themselves with a high degree of integrity, to respectfully strive for excellence in the work they perform and the outcomes they achieve, and to promote the public interest. The appetite for behaviours which do not meet these standards is very low. SSO takes any breaches of its Code of Conduct very seriously.
* **Work Health & Safety (WHS)** – SSO is committed to creating a safe working environment for all of its staff, where people are protected from physical or psychological harm. It has a very low appetite for practices or behaviours that could be expected to lead to staff being harmed while at work.

Operational Risks

SSO's appetite for specific operational risks is detailed below. Risks are carefully analysed in all of SSO's operational activities, including to ensure that the benefit of the risk control measures exceeds the costs of these measures.

Information Technology (IT)

IT risks cover both daily operations and ongoing enhancements to SSO's IT systems. These include:

* **Technology Service Availability – Prolonged outage of a core system:** SSO has a very low appetite for risks to the availability of systems which support its critical business functions.
* **Security – Cyber-attack on systems or networks:** SSO has a very low appetite for damage to assets from threats arising from malicious attacks. To address this risk, SSO aims for strong internal processes and the development and continuous improvement of robust technology controls.
* **Technology Change Management:** The implementation of new technologies creates new opportunities, but also new risks. SSO has a low appetite for IT system-related incidents which are generated by poor change management practices.

Physical Security

SSO provides a secure environment for its people and assets by ensuring its physical security measures meet high standards. SSO has a very low appetite for the failure of physical security measures.

Compliance

SSO is committed to a high level of compliance with relevant legislation, regulation, industry codes and standards as well as internal policies and sound corporate governance principles. Identified breaches of compliance will be remedied as soon as practicable. SSO has no appetite for deliberate or purposeful violations of legislative or regulatory requirements.

Information Management

SSO is committed to ensuring that its information is authentic, appropriately classified, properly conserved and managed in accordance with legislative and business requirements. It has a very low appetite for the compromise of processes governing the use of information, its management and publication. SSO has no appetite for the deliberate misuse of its information.

Implementation of SSO's Risk Appetite

All staff are responsible for the implementation of, and compliance with, this statement.

Communication

SSO's Risk Appetite Statement is published on SSO's intranet and SSO's website.

Risk Assessments

SSO maintains a Risk Register of the business risks it faces in its day-to-day operations and the control framework which is in place to mitigate risks. These Registers consider risks from within SSO and external sources, and are reviewed regularly. Risk Registers are also updated where necessary when there are key changes in policies, structures or functions and in response to incidents.

All risks which are judged as unacceptable are reported to the RMC and remedial action plans to reduce these risks to acceptable levels are reported, where appropriate, to the Board.

All risks which are judged as having a residual risk equal to medium or above are reported to the RMC annually.

Staff are required to manage their specific operational risks in a manner which is consistent with this Statement, and to manage and address any risks outside appetite or agreed tolerance levels. Risk appetite settings in Risk Registers for groups of risks with a similar nature must also be consistent with this Statement.

Reporting & Monitoring

Reporting systems are maintained to provide assurance that the risk appetite is effectively incorporated into management decisions.

Review

This Risk Appetite Statement is reviewed biennially, or whenever there is a significant change to SSO's operating environment. This review is coordinated by the RMC. Changes to the Risk Appetite Statement must be approved by the RMC and the Board.

## Risk management

*[List the potential risks to your business (in order of likelihood) and any mitigation/contingency strategies.]*

| Sport Business risk | Impact | Likelihood | Mitigation strategy | Contingency plan |
| --- | --- | --- | --- | --- |
| *[Description of the risk and the potential impact to your business.]* | *[High, Medium, Low.]* | *[Highly Unlikely, Unlikely, Likely, Highly Likely.]* | *[What actions will you take to minimise/mitigate the potential risk to your business?]* | *[What is your contingency plan in the event that this risk happens?]* |
| *[Description of the risk and the potential impact to your business.]* | *[High, Medium, Low.]* | *[Highly Unlikely, Unlikely, Likely, Highly Likely.]* | *[What actions will you take to minimise/mitigate the potential risk to your business?]* | *[What is your contingency plan in the event that this risk happens?]* |
| *[Description of the risk and the potential impact to your business.]* | *[High, Medium, Low.]* | *[Highly Unlikely, Unlikely, Likely, Highly Likely.]* | *[What actions will you take to minimise/mitigate the potential risk to your business?]* | *[What is your contingency plan in the event that this risk happens?]* |
| *[Description of the risk and the potential impact to your business.]* | *[High, Medium, Low.]* | *[Highly Unlikely, Unlikely, Likely, Highly Likely.]* | *[What actions will you take to minimise/mitigate the potential risk to your business?]* | *[What is your contingency plan in the event that this risk happens?]* |
| *[Description of the risk and the potential impact to your business.]* | *[High, Medium, Low.]* | *[Highly Unlikely, Unlikely, Likely, Highly Likely.]* | *[What actions will you take to minimise/mitigate the potential risk to your business?]* | *[What is your contingency plan in the event that this risk happens?]* |

## Critical business area analysis

*[Identify the critical areas of your business (e.g. product refrigeration process) and any protection strategies.]*

| Rank | Critical business areas | Impact if failed | Current protection strategies |
| --- | --- | --- | --- |
| 1 | *[Description of what you can't do without: people, suppliers, documents, systems or even procedures.]* | *[Describe the potential impact on your business if this critical area fails.]* | *[What strategies do you have that minimise the impact to your business? e.g. Training employees in multiple areas of the business will reduce key person risk.]* |
| 2 | *[Description of what you can't do without: people, suppliers, documents, systems or even procedures.]* | *[Describe the potential impact on your business if this critical area fails.]* | *[What strategies do you have that minimise the impact to your business? e.g. Training employees in multiple areas of the business will reduce key person risk.]* |
| 3 | *[Description of what you can't do without: people, suppliers, documents, systems or even procedures.]* | *[Describe the potential impact on your business if this critical area fails.]* | *[What strategies do you have that minimise the impact to your business? e.g. Training employees in multiple areas of the business will reduce key person risk.]* |
| 4 | *[Description of what you can't do without: people, suppliers, documents, systems or even procedures.]* | *[Describe the potential impact on your business if this critical area fails.]* | *[What strategies do you have that minimise the impact to your business? e.g. Training employees in multiple areas of the business will reduce key person risk.]* |

## 

## Scenario planning

*[Once you have completed your critical business areas table and ranked them, complete a more detailed scenario based on each of your top three critical business areas.]*

Scenario 1: [Name of scenario]

| Question | Details |
| --- | --- |
| **Critical failure** | *[Provide a short description of a critical area that could be interrupted.]* |
| **Background** | *[Provide any relevant background information that is essential to restoring the critical area.]* |
| **Impact to business** | *[Provide an estimate of the impact to your business. This can be in terms of percentage of sales or a dollar figure.]* |
| **Immediate actions** | *[List what needs to be completed immediately to ensure loss is kept to a minimum.]* |
| **Secondary actions** | *[Once immediate actions have been completed, what secondary actions can be completed until your business has recovered completely?]* |
| **Responsibilities** | *[List the people who are responsible and for what during this critical business scenario.]* |
| **Resources needed** | *[What resources will you need to ensure you recover well in this sort of scenario? For example: cash flow, staff, service providers]* |

Scenario 2: [Name of scenario]

| Question | Details |
| --- | --- |
| **Critical failure** | *[Provide a short description of a critical area that could be interrupted.]* |
| **Background** | *[Provide any relevant background information that is essential to restoring the critical area.]* |
| **Impact to business** | *[Provide an estimate of the impact to your business. This can be in terms of percentage of sales or a dollar figure.]* |
| **Immediate actions** | *[List what needs to be completed immediately to ensure loss is kept to a minimum.]* |
| **Secondary actions** | *[Once immediate actions have been completed, what secondary actions can be completed until your business has recovered completely?]* |
| **Responsibilities** | *[List the people who are responsible and for what during this critical business scenario.]* |
| **Resources needed** | *[What resources will you need to ensure you recover well in this sort of scenario? For example: cash flow, staff, service providers]* |

Scenario 3: [Name of scenario]

| Question | Details |
| --- | --- |
| **Critical failure** | *[Provide a short description of a critical area that could be interrupted.]* |
| **Background** | *[Provide any relevant background information that is essential to restoring the critical area.]* |
| **Impact to business** | *[Provide an estimate of the impact to your business. This can be in terms of percentage of sales or a dollar figure.]* |
| **Immediate actions** | *[List what needs to be completed immediately to ensure loss is kept to a minimum.]* |
| **Secondary actions** | *[Once immediate actions have been completed, what secondary actions can be completed until your business has recovered completely?]* |
| **Responsibilities** | *[List the people who are responsible and for what during this critical business scenario.]* |
| **Resources needed** | *[What resources will you need to ensure you recover well in this sort of scenario? For example: cash flow, staff, service providers]* |

## Insurance

*[What insurance policies do you currently hold to cover your business risks?]*

| Insurance type | Policy coverage | Policy exclusions | Insurance company and contact | Last review date | Payments due |
| --- | --- | --- | --- | --- | --- |
| *[e.g. Building, Contents, Car, Business Interruption]* | *[e.g. Damage from fire, flood, theft, Cyclone]* | *[e.g. Fraud, terrorism, tsunami, landslide]* | *[e.g. XYZ Insurance, D.Higgins (Area code) Number]* | *[Day/Month/Year]* | *[Amount you pay and frequency. e.g. Monthly, yearly]* |
| *[e.g. Building, Contents, Car, Business Interruption]* | *[e.g. Damage from fire, flood, theft, Cyclone]* | *[e.g. Fraud, terrorism, tsunami, landslide]* | *[e.g. XYZ Insurance, D.Higgins (Area code) Number]* | *[Day/Month/Year]* | *[Amount you pay and frequency. e.g. Monthly, yearly]* |
| *[e.g. Building, Contents, Car, Business Interruption]* | *[e.g. Damage from fire, flood, theft, Cyclone]* | *[e.g. Fraud, terrorism, tsunami, landslide]* | *[e.g. XYZ Insurance, D.Higgins (Area code) Number]* | *[Day/Month/Year]* | *[Amount you pay and frequency. e.g. Monthly, yearly]* |

Property & infrastructure

*[What have you done to make your property and infrastructure less vulnerable to damage? Is your property secured with alarms, security personnel or video surveillance from unlawful entry? Do you have fire retardant or flood resistant building materials? Is leaf litter grass and gutters maintained regularly to minimise fire risk?]*

'Business as usual' planning

Temporary office accommodation

*[Identify temporary office accommodation you can quickly access in a Crisis situation. Consider attaching a map of your accommodation to the back of your plan]*

| Rank | Type | Address | Equipment available | Resources needed |
| --- | --- | --- | --- | --- |
| 1 | *[e.g. Private residence, hotel, temporary business centre.]* | *[Enter the address of your temporary office site.]* | *[List all the equipment available at the site. e.g. Computers, furniture, photocopiers, phones, paper]* | *[List all the resources you will need in order to use this site as a temporary office. e.g. Software, backups, staff, and any other equipment not already available at the location.]* |
| 2 | *[e.g. Private residence, hotel, temporary business centre.]* | *[Enter the address of your temporary office site.]* | *[List all the equipment available at the site. e.g. Computers, furniture, photocopiers, phones, paper]* | *[List all the resources you will need in order to use this site as a temporary office. e.g. Software, backups, staff, and any other equipment not already available at the location.]* |
| 3 | *[e.g. Private residence, hotel, temporary business centre.]* | *[Enter the address of your temporary office site.]* | *[List all the equipment available at the site. e.g. Computers, furniture, photocopiers, phones, paper]* | *[List all the resources you will need in order to use this site as a temporary office. e.g. Software, backups, staff, and any other equipment not already available at the location.]* |