

1 PURPOSE

- 1.1 Paddle Australia (**PA**) is committed to managing organisation-wide risks and to establishing clear responsibilities to maximise strategic and operational achievement.
- 1.2 PA is committed to implementing AS ISO 31000:2009 Risk Management - Principles and Guidelines to provide a strategic, consistent and structured enterprise-wide approach to risk management. This approach will allow PA to effectively manage opportunities for gain and minimise the impact of threats causing losses.

2 SCOPE

- 2.1 This policy is applicable to all PA Workers.

3 DEFINITIONS

- 3.1 **“Risk Management”**, as defined by Australian Risk Management Standard (AS ISO 31000:2009), is coordinated activities to direct and control an organisation regarding risk.
- 3.2 **“Worker”** includes employees, independent contractors or representatives of independent contractors, work experience students and other volunteers.

4 KEY OBJECTIVES

- 4.1 Risk can manifest itself in many forms and has the potential to impact the health and safety, environment, community, reputation, regulatory, operational, and financial performance of PA and, thereby, the achievement of the organisation’s objectives. By properly understanding and managing risk, PA can provide greater certainty and confidence for stakeholders, Workers, participants, and for the broader community.
- 4.2 PA will use risk management capabilities to maximise the value from assets, projects, programs and other business opportunities and to assist in fostering participation and/or performance in PA.
- 4.3 Risk management will be embedded into business activities, functions and processes. Risk understanding and tolerance for risk will be key considerations in decision making.
- 4.4 Risk issues will be identified, analysed and ranked in a consistent manner. Common systems and methodologies will be used.
- 4.5 Risk controls will be designed and implemented to reasonably assure the achievement of organisational objectives. The effectiveness of these controls will be systematically reviewed and, where necessary, improved.
- 4.6 Risk management performance will be monitored, reviewed and reported. Oversight of the effectiveness of our risk management processes will provide assurance to executive management, the Board and relevant stakeholders.
- 4.7 The effective management of risk is vital to the continued growth and success of PA.

5 POLICY

- 5.1 Risk management will be incorporated into the strategic and operational planning processes of PA.

- 5.2 Risk assessments will be conducted on all new ventures and projects prior to commencement to ensure alignment with the PA risk appetite and organisational objectives.
- 5.3 Utilising the online RiskLabHQ risk management framework which includes the PA risk register (“**RiskLab**”), risks will be:
- a) identified, reviewed and monitored on an ongoing basis;
 - b) assessed and evaluated; and
 - c) assigned an owner, whose responsibilities are outlined in clause 9 of this policy.
- 5.4 PA will assess the effectiveness of its risk management plan through structured continuous improvement processes to ensure risks and controls are continually monitored and reviewed. This includes ongoing feedback loop via regular senior management meetings and appraisal of risk owners’ actions taken to manage risks via employee performance management.
- 5.5 PA senior management, via the Chief Executive Officer (“**CEO**”), on a regular basis shall inform and advise on significant risk management issues and the actions required to effectively manage these risks. The following reporting process is to be followed:
- a) management will regularly review RiskLab with their teams and update the mitigation strategies and perceived level of risk as appropriate;
 - b) new risks will be added to RiskLab through a formal notification process from employees, management and directors to the PA CEO;
 - c) a “top ten” list of major risks (as agreed by the A&RC) to be discussed at management meetings (fixed agenda item), together with any new or emerging risks; and
 - d) the Board will be updated at each meeting through the CEO Board report.
- 5.6 This policy is subject to formal review every four (4) years.

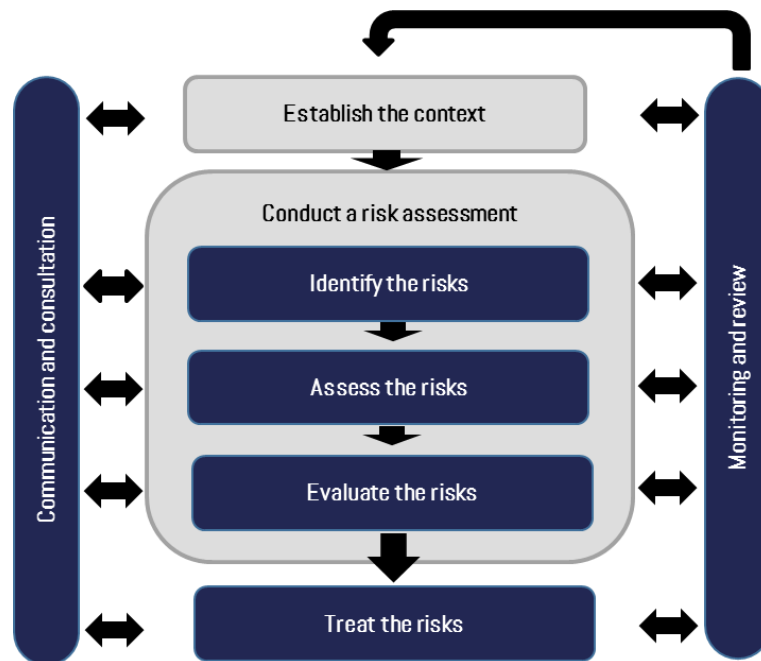
6 RISK MANAGEMENT PRINCIPLES

- 6.1 PA has adopted the principles detailed in AS ISO 31000:2009, to ensure risk management is effective within the organisation, namely:
- a) Risk management creates and protects value;
 - b) Risk management is part of decision making;
 - c) Risk management explicitly addresses uncertainty;
 - d) Risk management is systematic, structured and timely;
 - e) Risk management is based on the best available information;
 - f) Risk management is tailored;
 - g) Risk management takes human and cultural factors into account;
 - h) Risk management is transparent and inclusive;
 - i) Risk management is dynamic, iterative and responsive to change; and

- j) Risk management facilitates continual improvement of the organisation.

7 RISK MANAGEMENT PROCESS

- 7.1 The PA risk management process is based upon the AS ISO 31000:2009 Risk Management Process, as shown in the following flowchart. Organisational risks identified will be managed by PA in accordance with this process:



AS ISO 31000:2009 Risk Management Process

8 RISK MANAGEMENT COMPLIANCE AND CONTROL

- 8.1 In developing a culture of risk management, PA senior management is responsible for appropriate responses to manage risk, aided by the risk action plans and the creation of a risk register within RiskLab.
- 8.2 To enable this, PA:
- a) Has implemented a systematic process to assist in the identification, assessment, treatment and monitoring of risks;
 - b) provides the necessary tools and resources to senior management and employees to support the effective management of risks; and
 - c) reviews and communicates risk management best practice on a regular basis.

9 RESPONSIBILITIES

9.1 PA Board

- 9.1.1 PA Board is responsible for overseeing the establishment (and implementation via management) of risk management systems and reviewing the effectiveness of these systems, including:
- a) overseeing the creation, implementation and maintenance of the risk management system of PA and its internal control framework, including information systems;

- b) establishing a risk profile for PA setting out both financial and non-financial material and/or strategic risks facing PA;
- c) reviewing the effectiveness of PA implementation of its risk management systems and internal controls on an on-going basis and reviewing the outcome of any non-financial audits;
- d) seeking to reach a common understanding with management and auditors about the risk management process, key financial and regulatory risks and related controls including focusing on the “key” risks which are considered to be currently, or may in the future be, more significant or more likely to occur;
- e) analysing the effectiveness of PA risk management and internal compliance systems and the effectiveness of their implementation;
- f) developing an understanding of the overall business environment, relevant laws and codes of importance to PA and the programs/projects that PA have in place to provide reasonable assurance of compliance;
- g) reviewing PA health and safety policy and ensuring regular reporting to the Board on issues related to workplace health and safety;
- h) ensuring that the Chief Executive Officer states in writing to the Board annually that the statement given to the Board that PA financial reports present a true and fair view, in all material respects, of PA financial condition and operational results and are in accordance with the relevant accounting standards, are founded on a sound system of risk management and internal compliance and control which implements the policies adopted by the Board;
- i) ensuring that the Chief Executive Officer states in writing to the Board annually that PA risk management and internal compliance and control system is operating efficiently and effectively in all material respects; and
- j) reviewing insurance coverage and claims trends.

9.2 **Audit & Risk Committee (“A&RC”)**

9.2.1 The A&RC is appointed by the Board and comprised of two (2) Directors and up to three (3) independent members with a standing invitation to the Chief Executive Officer, Chief Operating Officer and Finance Manager. Legal, risk and insurance expertise are co-opted as required. A&RC is responsible for:

- a) implementing the principles, actions and requirements of the risk management framework and monitoring its implementation within PA;
- b) providing the necessary tools and resources to identify and manage risks;
- c) reviewing risks on a quarterly basis, including identifying new risks, changes to existing risks and retirement of previously identified risks (through a formal decision-making process);
- d) the way in which ownership of risks is taken by senior management or others in accordance with function or expertise;
- e) regular reporting of the status or risk items to the Board;
- f) appraising risk owners’ actions taken to manage risk and correcting inappropriate performance;

- g) internal compliance and control systems for the implementation of the risk management plan;
- h) the consideration of non-financial audits; and
- i) the compliance with regulatory requirements and best practice.

9.3 Paddle Australia CEO

9.3.1 The CEO is responsible for:

- a) identifying legislation, policy and guidelines affecting risk management practices at PA;
- b) maintaining PA Risk Register;
- c) providing assistance and support throughout PA for risk management;
- d) organising appropriate risk management education and training for PA employees; and
- e) Monitoring the implementation of the PA Risk Management Framework across the organisation.

9.4 Senior Management

9.4.1 Senior management will be responsible for:

- a) championing the roll out of the PA Risk Management framework into PA;
- b) ensuring employees understand their responsibilities with respect to operational risk management;
- c) developing a risk aware culture within their area of responsibility;
- d) advising the CEO of needs for any training, development and facilitation; and
- e) maintenance of risk registers within their areas.

9.5 Risk Owners

9.5.1 Risk owners are responsible for:

- a) identifying existing controls to help manage the risk;
- b) developing treatment plans to reduce the likelihood and/or impact of the risk;
- c) monitoring the implementation of the treatment plans and reporting on their effectiveness and outcomes; and
- d) monitoring and alerting senior management of significant changes in risk status.

10 PA RISK FRAMEWORK

10.1 Risk Matrix

| | |
|--|---------------|
| | IMPACT |
|--|---------------|

| Risk Matrix | | Insignificant | Minor | Medium | High | Extreme | |
|-------------|----------------|---------------|----------|----------|----------|----------|----------|
| | | 1 | 2 | 3 | 4 | 5 | |
| PROBABILITY | Rare | 1 | Low | Low | Low | Moderate | Moderate |
| | Unlikely | 2 | Low | Low | Moderate | High | High |
| | Possible | 3 | Low | Moderate | High | High | Extreme |
| | Likely | 4 | Low | Moderate | High | Extreme | Extreme |
| | Almost Certain | 5 | Moderate | High | High | Extreme | Extreme |

10.2 Risk Grading Criteria – Impact Ratings

10.2.1 The risk is to be assessed over the following categories in relation to impact (consequence):

- a) **Financial** – impact on Paddle Australia finances;
- b) **Operational** – impact on provision of Paddle Australia products, projects and services;
- c) **Brand / Reputational** – impact on Paddle Australia brand and general credibility;
- d) **Physical / Safety** – impact on the safety and well-being of people;
- e) **Regulatory / Legal** – impact on Paddle Australia regulatory exposure; and
- f) **People / Participation** – impact on corporate knowledge / continuity.

10.2.2 Impact levels and criteria are shown in the following table:

| Financial | Operational | Brand/ Reputational | Physical/ Safety | Regulatory/ Legal | People/ Participation |
|-----------|-------------|------------------------|---------------------|----------------------|--------------------------|
|-----------|-------------|------------------------|---------------------|----------------------|--------------------------|

| | | | | | | | | | |
|--------|---|---------------|---|--|---|--|---|---|---|
| IMPACT | 5 | Extreme | A risk that can prove catastrophic or terminal for the whole organisation. | More than \$100,000 | Unable to deliver product/services in a region. Widespread migration of members to competitor organisation. Prohibited from delivering competition at any level. | Collapse of organisation. Major inquiry into systemic misconduct. Wholesale resignation of Board Members or Senior Management. | Death or total permanent disability of player/participant due to compromised safety standards. Preventable death of a member of the public. | Criminal prosecution of organisation and/or Board due to failure to comply with the law. | Active participation declines by more than 25%. |
| | 4 | High | Risks which can significantly jeopardise some aspects of the organisation, but which will not result in organisational failure. | More than \$25,000 but less than \$100,000 | Widespread failure or loss of product/service standards. Increasing migration of members to competitor organisations. Unable to deliver the National Championships. | Loss of affiliated clubs/providers. Investigation of serious individual misconduct. Loss of significant skills from Board or Senior Management. | Serious injury of player/participant due to compromised safety standards. Preventable serious injury of member or public. | Civil action against organisation and/or Board due to negligence. New regulations that impede operations. | Active participation declines by more than 15%, but less than 25%. |
| | 3 | Medium | Risks which will cause some problems, but nothing too significant. | More than \$10,000 but less than \$25,000 | Moderate impact on product/service standards. Unable to deliver local sports competitions. Widespread discontent by members/participants. | Threats of withdrawal from affiliated clubs/providers. Failure of prominent branded project or product. Failure of a club or provider. Individual or group misconduct. Sustained public criticism of the organisation. | Systemic injuries of players/participants and/or public. Increased frequency of near misses. | Regulatory/police investigation with adverse findings against organisation and/or Board. | Net active participation declines by more than 5%, but less than 15%. |
| | 2 | Minor | Any risks which will have just a mild impact but should be addressed. | More than \$1,000 but less than \$10,000 | Minor impact on product/service delivery. Competitive threats to membership. Constrained capacity to meet the demands of existing or new members/participants. | Localised negative media coverage. | Minor injuries of players/participants and/or public. | Regulatory/police investigation of organisation and/or Board without adverse findings. | Net active participation declines by more than 0%, but less than 5%. |
| | 1 | Insignificant | Risks which do not pose any significant threat, and which can be left unmitigated without special action. | Less than \$1,000 | Very minor, temporary product/service disruption. | Media interest in local issue. | Insignificant injuries of players/participants and/or public. | Persistent complaints against organisation and/or Board. | Stable net active membership. |

11 BREACH OF POLICY

11.1 Any Worker who is found to have breached this policy may be subject to disciplinary action, up to and including termination of employment or engagement with the Organisation.