

POLICY	Governance
TITLE:	Risk Management Policy
AREA:	Governance
RESPONSIBILITY:	Business Operations Manager
RELATED POLICIES:	
DRAFTED BY:	Business Operations Manager
DATE APPROVED:	17 th June 2018
APPROVED BY:	Paddle Australia
NEXT REVIEW:	June 2020

CONTENTS

1. CONTEXT	3
1.1 Purpose	3
1.2 Scope	3
2. KEY OBJECTIVES	3
3. REVIEW OF POLICY	4
4. ACCESS TO THE POLICY	4
5. RISK MANAGEMENT REQUIREMENTS	4
6. RISK MANAGEMENT PRINCIPLES	4
7. RISK MANAGEMENT PROCESS	5
8. RISK MANAGEMENT COMPLIANCE AND CONTROL	5
9. ASSESSMENT OF EFFECTIVENESS	6
10. REPORTING REQUIREMENTS	6
11. RISK MANAGEMENT RESPONSIBILITIES	6
11.1 Paddle Australia Board	6
11.2 Audit & Risk Committee (A&RC)	7
11.3 Paddle Australia Chief Executive Officer	8
11.4 Paddle Australia Managers/Senior Staff	8
11.5 Risk Owners	8
12. RISK FRAMEWORK	9
12.1 Risk Matrix	9
12.2 Risk Grading Criteria – Impact Ratings	9
12.3 Risk Grading Criteria – Likelihood Ratings	11
12.4 Risk Tolerance Levels	12

1. CONTEXT

1.1 PURPOSE

The purpose of this Risk Management Policy is to communicate Paddle Australia's (PA) commitment to managing organisation-wide risks and to establish clear responsibilities for itself in order to maximise strategic and operational achievement.

1.2 SCOPE

This policy applies to directors, management, staff, officials, volunteers, and members of PA.

PA is committed to the formal, systematic and structured proactive management of risks across the organisation.

Risk is inherent in all aspects of PA's activities and whilst many of these risks cannot be eliminated they can, however, be identified, quantified and controlled. Risks that impact on the objectives of PA can offer both opportunity and threat. This Policy is designed to provide PA personnel with a systematic framework in order to minimise threats and maximise opportunities to PA.

2. KEY OBJECTIVES

- a) The Australian Risk Management Standard (AS ISO 31000:2009) defines risk management as "coordinated activities to direct and control an organisation with regard to risk".
- b) This Policy confirms that PA is committed to implementing a strategic, consistent and structured enterprise-wide approach to risk management in order to effectively manage opportunities for gain and minimise the impact of threats causing losses.
- c) This Policy is aligned to reflect AS ISO 31000:2009 Risk Management – Principles and Guidelines which provides the framework used to develop the PA enterprise-wide risk management framework.
- d) Risk will 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.
- e) By understanding and managing risk, PA will provide greater certainty and confidence for our stakeholders, PA directors and employees, participants, and for the communities in which we operate.
- f) 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.
- g) Risk management will be embedded into business activities, functions and processes. Risk understanding and tolerance for risk will be key considerations in decision making.
- h) Risk issues will be identified, analysed and ranked in a consistent manner. Common systems and methodologies will be used.

- i) 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.
- j) 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.
- k) The effective management of risk is vital to the continued growth and success of PA.

3. REVIEW OF POLICY

This Policy is subject to formal review every four years.

4. ACCESS TO THE POLICY

This Policy will be communicated to directors, management, staff, officials, volunteers, and members of PA. The policy will be available through the PA website.

5. RISK MANAGEMENT REQUIREMENTS

- a) Risk management will be incorporated into the strategic and operational planning processes of PA;
- b) Risk and the management of risk will be identified and monitored according to the PA enterprise-wide risk management policy;
- c) 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;
- d) Risks will be identified, reviewed and monitored on an ongoing basis;
- e) Risks will be assessed and evaluated against the PA Risk Management Framework (outlined in Section 12 of this policy);
- f) Relevant risks that are identified will be recorded within PA's risk management register;
- g) All risks will be assigned an owner whose responsibilities are specified in this policy under Section 11.5 of this policy.

6. RISK MANAGEMENT PRINCIPLES

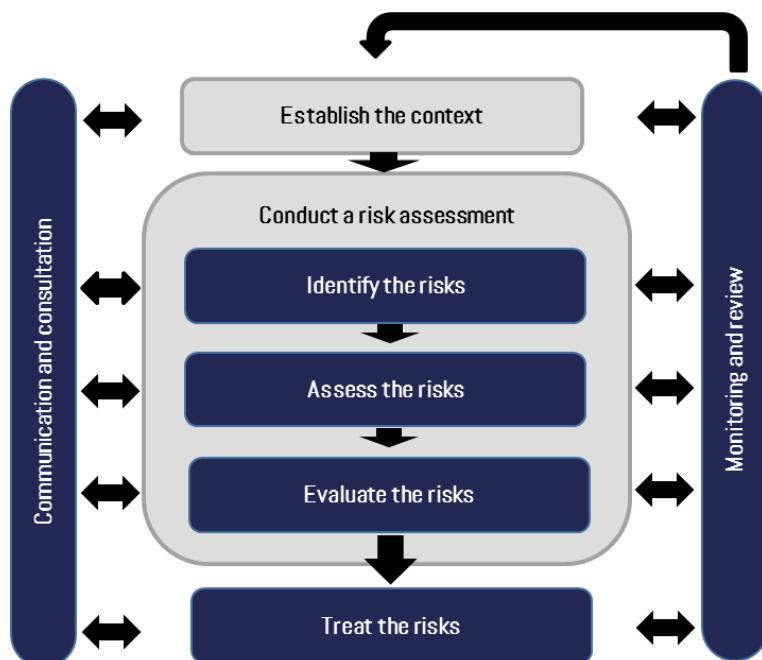
PA has adopted the principles detailed in AS ISO 31000:2009, to ensure risk management is effective within the organisation. These principles are:

- 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

The PA risk management process is based upon the AS ISO 31000:2009 Risk Management Process as shown in Figure 1 (below). Risks identified will be managed according to this process.



Above: AS ISO 31000:2009 Risk Management Process

8. RISK MANAGEMENT COMPLIANCE AND CONTROL

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.

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. ASSESSMENT OF EFFECTIVENESS

PA assesses 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.

10. REPORTING REQUIREMENTS

PA senior management, via the PA Chief Executive Officer, ensures that the Board is adequately informed of significant risk management issues and the actions undertaken to manage risks on a regular basis. The following reporting process is in place:

- a) Management will regularly review the risk register with their teams and update the mitigation strategies and perceived level of risk as appropriate.
- b) New risks will be added to the register through a formal notification process from staff, management and directors to the PA Chief Executive Officer.
- c) A "top ten" list of major risks (as agreed by the Audit and Risk Committee) to be discussed at monthly management meetings (fixed agenda item), together with any new or emerging risks.
- d) The Board will be updated at each meeting through the Chief Executive Officer Board report.

11. RISK MANAGEMENT RESPONSIBILITIES

11.1 PADDLE AUSTRALIA BOARD

The Board of PA is responsible for overseeing the establishment (and implementation via management) of risk management systems and reviewing the effectiveness of these systems.

The Board's role in relation to risk includes:

- 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's 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’s 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’s health and safety at work 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’s financial reports present a true and fair view, in all material respects, of PA’s 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 Paddle Australia’s 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.

11.2 AUDIT & RISK COMMITTEE (A&RC)

The A&RC is appointed by the Board and comprised of two Directors and up to three independent members with a standing invitation to the Chief Executive Officer, Business Operations Manager and Finance Manager. Legal, risk and insurance expertise are co-opted as required.

It is responsible for:

- a) Implementing the principles, actions and requirements of the risk management plan 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 manner 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.

11.3 PADDLE AUSTRALIA CHIEF EXECUTIVE OFFICER

The Chief Executive Officer is responsible for:

- a) Identifying legislation, policy and guidelines affecting risk management practices at PA;
- b) Maintaining PA's Risk Register;
- c) Providing assistance and support throughout PA for risk management;
- d) Organising appropriate risk management education and training for PA staff; and
- e) Monitoring the implementation of the PA Risk Management Framework across the organisation.

11.4 PADDLE AUSTRALIA MANAGERS/SENIOR STAFF

Senior management will be responsible for:

- a) Championing the roll out of the PA Risk Management Framework into PA;
- b) Ensuring staff understand their responsibilities with respect to operational risk management;
- c) Developing a risk aware culture within their area of responsibility;
- d) Advising the Chief Executive Officer of needs for any training, development and facilitation; and
- e) Maintenance of risk registers within their areas.

11.5 RISK OWNERS

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.

12. RISK FRAMEWORK

12.1 RISK MATRIX

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

12.2 RISK GRADING CRITERIA – IMPACT RATINGS

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

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

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.

12.3 RISK GRADING CRITERIA – LIKELIHOOD RATINGS

The following probability thresholds and ratings in relation to assessing risks be used.

LIKELIHOOD	5	Almost Certain	Will probably occur more than once within 12 months
	4	Likely	High probability that will occur at least once within next 24 months
	3	Possible	Reasonable likelihood that could occur more than once in 24 months
	2	Unlikely	Not likely to occur within next 24 months
	1	Rare	Not impossible but highly unlikely

12.4 RISK TOLERANCE LEVELS

The following risk tolerance thresholds be used in relation to the actions PA personnel shall take in relation to managing risks.

RISK LEVEL	REQUIRED ACTIONS
EXTREME	<p>Intolerable</p> <ul style="list-style-type: none"> Operations / activity should be <u>discontinued</u> until level of risk is able to be reduced (or written authorisation to continue is provided by the PA CEO and Chair). Consider options for reducing the impact or probability of the risk. CEO to be informed ASAP and provide urgent attention, guidance and approval of mitigation strategy. Consider external advice (legal, insurance or risk advisor).
HIGH	<p>Tolerable level of risk – significant management & monitoring required</p> <ul style="list-style-type: none"> Action should be taken to ensure risk level is As Low As Reasonable Practicable (ALARP). Consider options for reducing the impact or probability of the risk. If level of risk is ALARP, continue to manage using documented operating procedures. Increase monitoring of controls to ensure effectiveness in managing the risk.
MODERATE	<p>Tolerable level of risk – follow operating procedures</p> <ul style="list-style-type: none"> Ensure risk level is ALARP. If level of risk is ALARP, continue to manage using standard operating procedures with normal monitoring protocols.
LOW	<p>Tolerable level of risk.</p> <ul style="list-style-type: none"> Maintain existing controls. No additional controls required.