Badminton Australia

Risk Management Framework

Title:	Badminton Australia Risk Management Framework
Type of Policy	Governance
Last Review Date:	N/A
Version:	Badminton Australia Risk Management Framework June 2026
Next Review Date:	June 2027
Responsible Person:	FAR / Board
Authority	Approved by the Board

Enterprise Risk Management Framework

Badminton Australia

Contents

Contents 2

1. Purpose and Scope 3

2. Governance and Process 4

2.1 Roles and Responsibilities 4

2.1.1 The BA Board of Directors and the ARC 4

2.1.2 Chief Executive Officer 5

2.1.4 Management Team 5

2.1.4 BA staff and consultants 5

2.1.5 BA Volunteers and Officials 5

2.2 Risk Reporting 6

2.3 Culture – 'Risk management is everyone's responsibility' 6

2.4 Risk Management 'Activity' Template 6

3. Accountabilities 6

3.1 Risk calendar 6

3.2 Training 7

4. Enterprise Risk Management Procedure 7

5. Control Effectiveness Criteria 14

1. PURPOSE AND SCOPE

The Board of directors recognises that to achieve the organisation's strategic priorities, Badminton Australia must pursue opportunities that carry risk, while protecting safety, integrity and sustainability. This statement defines the Board's appetite and tolerance for risk across each strategic priority.
Overall Position

- The Board has a higher appetite for risks that expand participation, partnerships and performance opportunities
- The Board has a lower appetite for risks that threaten safety, reputation, financial sustainability, or compliance.
- There is zero tolerance for unethical conduct, fraud, safeguarding breaches, and deliberate non-compliance with laws or regulations.

To meet BA's strategic objectives BA management must work collaboratively with key stakeholders to provide quality participation opportunities and pathways within Badminton.

BA's ongoing success is considered to be a product of delivering upon the key strategic objectives:

1. **Play – Facilitate more opportunities for people to participate**
    - **Appetite:** High. The Board supports innovative programs and initiatives that broaden grassroots and community engagement, even where outcomes are uncertain.
    - **Tolerance:** Tolerance for short-term financial or operational setbacks is acceptable if lessons are learned and adjustments are made. However, there is zero tolerance for risks that compromise participant safety or inclusion.

2. **Perform – Develop a High-Performance system that strives for excellence and international success**
    - **Appetite:** Moderate to high. The Board is willing to invest in ambitious athlete pathways, coaching innovation, and international competition exposure.
    - **Tolerance:** Performance variability is tolerated; however, there is zero tolerance for risks that compromise athlete's health, wellbeing, anti-doping compliance, or integrity in sport.

3. **Partner – Work together to enhance the experience and outcomes for everyone involved**
    - **Appetite:** Moderate. The Board supports partnerships with external organisations, funders, and communities, even where some reputational or delivery risks may exist.
    - **Tolerance:** Limited tolerance for short-term partnership challenges, provided alignment with organisational values is maintained. Zero tolerance for partnerships that present conflicts of interest or undermine integrity.

4. **Promote – Recognise, celebrate, and promote all aspects of badminton; operate with integrity and good reputation; ensure a high level of safety and wellbeing**
    - **Appetite:** Low. The Board prioritises brand integrity, safety, and wellbeing over high-risk promotional or reputational strategies.
    - **Tolerance:** Minimal tolerance for reputational risk; limited criticism is acceptable where aligned to long-term strategy. There is zero tolerance for risks that compromise safety, wellbeing, or ethical standards.

5. **Finance, Compliance and Legal – Operate in a financially and operationally sustainable manner, with strong governance**
    - **Appetite:** Low to moderate. The Board supports measured investment in growth initiatives while ensuring sustainability.
    - **Tolerance:**
        - **Finance:** Limited tolerance for short-term deficits, provided they are linked to Board-approved strategic investments. Adequate reserves must always be maintained.
        - **Compliance & Legal:** Zero tolerance for deliberate breaches of law, regulation, or policy. All obligations must be met fully and transparently.

To facilitate achieving on the strategic objectives, the Board of Directors and the Finance Audit and Risk Committee (FARC) support the development of practical risk management business rules to manage risk and identifying opportunities in a measured way.
BA considers that risk management is an important aspect of corporate governance and therefore a significant contributor to embedding our culture and values.

The purpose of this ***Enterprise Risk Management Framework*** and embedded procedure is to outline the principles and processes by which the Board of BA and management team will react to the risks facing the organisation.

This Framework encompasses the following elements:

- provides the context for organisational risk management at BA;
- outlines the overarching documentation structure and risk review requirements;
- describes the governance structure and accountabilities that are in place; and
- provides the procedure for identifying and assessing risks, and the response required in order to mitigate risks that may impact BA.

Review & Oversight

The Enterprise Risk Management Framework is a document mandated by the Board of Directors, but delegated to the FA, who will ensure:

- The overall position will be reviewed annually by the FARC and endorsed by the Board
- Any risk assessed as exceeding tolerance levels must be immediately escalated to the CEO and FARC for Board consideration
- Appetite settings will be revisited considering emerging risks, stakeholder expectations, and the organisation's strategic direction.

2. GOVERNANCE AND PROCESS

2.1 Roles and Responsibilities

It is necessary to articulate the responsibilities of the organisation in relation to risk management processes and behaviours. These responsibilities are defined as follows;

2.1.1 The BA Board of Directors and the FARC

The maintenance of a sustainable risk management function that supports the organisation remains the ultimate responsibility of the Board with oversight from the FARC. The Board and FARC, with the assistance of the CEO is responsible for ensuring that sufficient resources, knowledge and reporting structures are in place to ensure that all of the risk identification, assessment and treatment processes can be carried out efficiently across the organisation.

Responsibilities of the FARC include:

- Consider the organisation's risk profile;
- Monitor risk management maturity and capability;
- Review and assess the effectiveness of BA's risk management processes; and
- Report to the Board on the above matters.

Key artefacts required by the Board and FARC to ensure that risk management is embedded in the organisation includes the following:

- Risk Management Policy
- Enterprise Risk Management Framework (this document);
- Strategic Risk Register; and
- Communications that encourage all staff, contractors, committees, working groups, officials and volunteers to embrace risk management as part of their day to day roles.

2.1.2 Chief Executive Officer

BA's Chief Executive Officer (CEO) is responsible for day to day oversight of risk management, including the assessment of principal risks and ensuring that these risks are being monitored and managed by the BA Staff and consultants. The CEO has the responsibility to ensure the:

- **Identification** of risk – identify the reputational, regulatory, operational, financial and strategic risks that are prevalent in fulfilling the BA's Vision.
- **Analysis** of risk – analyse the reputational, regulatory, operational, financial and strategic risks in accordance with the agreed likelihood and consequence scales.
- **Evaluation** of risk – evaluate risks to ensure appropriate action is taken on prioritised risks.
- **Treatment** (mitigation) of risk – develop mitigation strategies and action plans to reduce unacceptable levels of risk that would impact the success of BA.
- **Monitor and Review** – monitor all risks and opportunities impacting BA

2.2.1.4 BA staff and consultants

All BA staff and consultants are responsible for incorporating risk management practices into business-as-usual activities.

BA staff and consultants must actively manage risks that are part of their day-to-day work in accordance with this Framework and by identifying and responding to risks with the support of the CEO and/or Board.

2.1.5 BA Volunteers and Officials

Our volunteers are integral to our success. BA will support all volunteers by providing specific safety management training to reduce safety risks that may be prevalent in the execution of their volunteering role.

All BA volunteers are encouraged to advise BA management of risks that may impact coach or player safety.

2.1.6 Stakeholders

BA will ensure a systematic process for identifying and engaging relevant stakeholders such as members and funding partners throughout any risk management process. This includes the gathering of stakeholder input on risk identification and tolerance levels, clearly communicating risk assessments and mitigations strategies and support feedback from stakeholders to raise any emerging concerns and verifying any risk related interests are being adequately addressed within this framework.

2.1.7 Technology and Data Risk Management:

It is important for BA to implement comprehensive controls to identify, assess, and mitigate risks arising from:
digital infrastructure,
cybersecurity threats,
data privacy breaches,
system failures, and technological obsolescence.

BA is to undertake regular assessments on incident response protocols, and data governance policies (or data governance included in existing policies to ensure privacy regulations, business continuity and disaster recovery plans.
There is also a need to ongoing evaluation of emerging technology risks such as AI ethics, cloud dependency and third party vendor security to protect organisational assets and maintain stakeholder trust.

2.2 Risk Reporting

The CEO is responsible for the reporting of risks and incidents in line with this Framework.

Section 3.1 identifies the timing of risk reviews and assessments.

The CEO is required to provide a ***risk reporting and updates*** to support the identification and management of risks and incidents to the FARC for presentation as follows:

i. Updates to risk register (at least every 2 months)
ii. Selected 'Deep Dive' on a selected risk item
iii. Risk treatment plan update (as required under Section 4, Step 4) if required

The aim of the risk *reporting and updates* is to ensure that risk related matters are discussed in an appropriate forum and to ensure that the FARC can react to risks in a timely manner.

2.3 Culture – 'Risk management is everyone's responsibility'

To achieve a culture of 'risk management is everyone's responsibility', the Board, CEO, and staff, must be consistent in all levels of communication to stakeholders, volunteers, public and others on matters that may impact BA.

Risk mitigation is not isolated to Board, CEO and staff, but a key part of the role of volunteers, consultants, stakeholders and supporters who contribute to the success of BA.

2.4 Risk Management 'Activity' Template

In addition to the orgnisational risk management processes, BA will establish a Risk Management 'Activity' Template. This template will be used at the discretion of the CEO for use on activities that have high risk outside of regular organisational business. These types of risks may include but are not limited to:

- Team overseas travel
- Team camps within Australia involving underage players
- International events held in Australia
- Implementation of a new program
- Any other activity as deemed by the CEO

3. ACCOUNTABILITIES

3.1 Risk calendar

The following calendar presents the range and cycle of annual activities required to effectively and efficiently manage risk in accordance with the Framework.

	Review Enterprise Risk Management Framework	FARC	Annually (February)
	Endorse the Enterprise Risk Management Framework	Board and FARC	Annually (February)
2			
	Identify, assess and review strategic and operational risks as part of formal workshop	Management Team	Bi-annually
	Review risk strategies and process as part of formal workshop process	Board and FARC	Annually at Face-to-Face meeting
	Review and update risk register, and identify any new risks	Management Team	When risks is identified or at least every 2 months
	Compile risk reporting package for the CEO to distribute to FARC and Board	CEO	For each FARC and Board meeting
	Risk discussed as an agenda item at team meetings, reviewing new risk items	Management Team and staff	Standing agenda item for monthly Operational meetings
	Review treatment plans for High and Extreme risks	FARC	At each FARC meetings
	Review treatment actions	Management Team	Monthly
	External audits	Appointed auditor	Annually
	Technology and Data Risk management	CEO	Annually to FARC or upon major incident.

3.2 Training

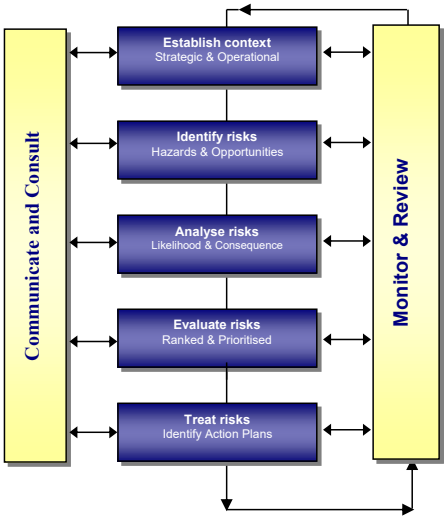
To build organisational capability and common understanding, training that supports risk leadership and accountability for risk owners and staff is undertaken. Yearly and to be included in all staff workshops. Structure of risk training will be in line with strategic objectives agenda of staff workshops.

4. Enterprise Risk Management Procedure

The risk management process overview

The process for managing risks involves **five key steps** (consistent with ISO 31000), together with a monitoring and review process based on communication and consultation.

Key aspects of the risk management cycle should be documented, including the identified risks, risk assessments, control assessments, treatment options and action plans.



Communicate and Consult

Effective communication and consultation are essential to ensure that all stakeholders understand the basis on which risk management decisions are made and why particular actions are required.

Risk management needs to be promoted across all the organisation.

Monitor and Review

Monitoring and review procedures need to be incorporated into both strategic and day-to-day operational activities to capture any new risks arising from changing business circumstances and to review implementation of risk reduction strategies.

A Risk Reporting Package is in place to provide information to the Board the Audit and Risk Committee.

Step 1: Establish the Context

The context needs to be established prior to starting the risk assessment. It involves an examination of the external, organisational and risk management environment in which the risk identification, analysis and treatment options are considered.

Within the overall risk context (including emerging risks) the Board and FARC have a focus on the following risk types:

Finance – risks and opportunities that may impact the financial performance are:

- fraud, theft,
- conflict of interest,
- loss of funding
- duplication of payments, expenditure and revenue budget of BA.
- level of reserves that need to be held, cash flow
- national membership model
- unbudgeted losses from programs and events

Safety – incidents that may cause injury or fatality to staff, contractors, competitors, visitor and volunteers.

Information Management – risks to information and data

- that may expose BA to business continuity risks.
- Privacy of data held
- Security of National Data Base
- Cybersecurity
- Breaches
- Other emerging risks

Legal and Compliance – regulatory and compliance issues with legislation or internal policies or procedures that may impact on BA's ability to continue operations.

Strategic – events and incidents that may generate adverse publicity impact on the reputation of BA, community relations and media.

Reputation – events and incidents that may impact on the reputation of BA.

Commented [JM1]: Tj. To review the context

Step 2: Identify risks

The next step is risk identification, review and documentation of the risks to be managed. Previously identified risks are reviewed with reference to any changes in the business or operating environment.

Step 3: Analyse risks

Risk analysis assists in deciding whether risks need to be treated and helps determine the most appropriate risk treatment strategies. Risk analysis involves consideration of the sources of risk, their positive or negative *consequence* and the *likelihood* that those consequences may occur. From this analysis the impact of risk can be determined.

Risk consequence rating table

Rating Descriptor & Score	Operational Performance Parameters					
	Finance	**Safety**	**Information Management**	**Legal & Compliance**	**Strategic**	**Reputation**
Extreme	Financial impact to revenue greater than or equal to $75,000	Fatality and/or severe irreversible disability	Loss or corruption of critical data/ knowledge of staff resulting in the loss of key project/program continuity for a period greater than or equal to 2 months.	Cessation of business and operating licenses due to non-compliance with regulations	Long lasting impact on strategic plan, stakeholders and key outputs	Total breakdown of public and stakeholder confidence in the integrity of a program or the organisation
Major	Financial impact to revenue greater than or equal to $25,000 but less than $75,000	Significant irreversible disability or impairment to one or more persons	Loss or corruption of critical data/ knowledge of staff resulting in the loss of key project/ program continuity for greater than or equal to 1 month but less than 2 months.	Fines, penalties and or restrictions on business by regulators that impact our license	Major impact on strategic plan, stakeholders and key outputs	Consistent media attention focusing on the integrity of a project, program or the organisation
Moderate	Financial impact to revenue greater than or equal to $15,000 but less than $25,000	Treatment by a medical practitioner required. Potential ongoing injury management	Temporary loss or corruption of data/ knowledge of staff resulting in lost continuity for greater than or equal to 1 week but less than 1 month.	Fines and penalties by regulators that impact the organisation for a short term	Moderate impact on strategic plan, stakeholders and key outputs	Short-term media attention focusing on the integrity of a project, program or the organisation
Minor	Financial impact to revenue greater than or equal to $5,000 but less than $15,000	Self-medication or local first aid administered	Isolated temporary loss or corruption of data/ knowledge of staff resulting in lost for a period less than 1 week.	Minor or short-term regulatory issue not impacting the organisation	Minor impact on strategic plan, stakeholders and key outputs	Isolated and localised media attention on the integrity of a project or initiative.
Insignificant	Financial impact to revenue less than $5,000	Very minor injury; no first aid required	Isolated temporary loss or corruption of data/ knowledge of staff resulting in no lost continuity	Isolated issue not impacting the organisation	Isolated short term impact on strategic plan, stakeholders and key outputs	One-off localised attention on the integrity of a project or initiative.

Commented [JM2]: Review amounts and parameters

Risk likelihood rating table

RATING	LIKELIHOOD OF OCCURENCE
Almost certain	The event is expected to occur in most circumstances Will occur within the next 6 months
Likely	The event will probably occur at some time Will probably occur within the next 12 months
Possible	The event could occur at some time Will probably occur within the next 18 months
Unlikely	The event is unlikely to occur May occur within the next 2 years
Rare	The event may only occur in exceptional circumstances Not likely to occur within the next 2 years

Overall risk rating:

- All inherent risks (risks rated before mitigations) ranked as 'Severe' or 'High' require analysis of existing risk controls in place to determine the net residual risk rating.
- Inherent 'Low' and 'Medium' risks may be excluded from further analysis, however the rationale for excluding these risks and management's on-going responsibilities should be documented.

Risk ranking

Consequence and likelihood criteria are combined and result in the enterprise risk matrix (heat map) in the table below. This identifies a risk ranking.

		CONSEQUENCE				
		Insignificant	Minor	Moderate	Major	Extreme
LIKELIHOOD	Almost certain	**Medium**	**Medium**	**Severe**	**Severe**	**Severe**
	Likely	**Low**	**Medium**	**High**	**High**	**Severe**
	Possible	**Low**	**Low**	**Medium**	**High**	**High**
	Unlikely	**Low**	**Low**	**Medium**	**Medium**	**High**
	Rare	**Low**	**Low**	**Low**	**Medium**	**Medium**

Step 4: Evaluate risks

Risk acceptability is to be evaluated, dependent on the level of risk.

The risk response in the below table shows the rate of response, and authority level for each level of risk. An action plan may include:

- Further treatment required in order to bring the level of risk down to an acceptable 'residual level'.
- An acceptance that current controls are adequate but require a level of monitoring

Risk response table

Residual Risk Ranking	Risk mitigation strategy	Risk escalation level
Severe	Escalation and immediate course of action to be determined within 14 days and documented in treatment plan. To be monitored at each FARC and Board meeting.	Board FARC CEO
High	Escalation and immediate course of action to be determined within 30 days and documented in treatment plan. To be monitored at each FARC meeting. **OR** Risk deemed 'acceptable' pursuant to BA strategy by the Board and FARC	FARC CEO
Medium	Acceptable risk - may require further assessment and be monitored quarterly by FARC	Risk owners Management Team
Low	Acceptable risk – continue to manage as normal review bi-annually by FARC	Risk owners

Step 5: Treat risks

For 'Severe' risks the risk owner must develop a risk treatment plan.

High risks may or may not require a treatment plan based on CEO or FARC discretion.

For risks rated as Medium or Low, development of treatment plans will be at the discretion of the CEO but are not considered necessary.

Risk treatment involves developing a range of options for mitigating risk, assessing those options and then preparing and implementing action plans.

These will be documented on the *Risk Register Worksheet* and include responsibilities for actions and timeframes.

To do this it is necessary to:

1. Assess the effectiveness of the current controls using the *Control effectiveness rating table (Section 5).*

2. Identify, assess and select the treatment options which include to accept, reduce, transfer, avoid or increase the risk. The most appropriate treatment option/s involves balancing the costs and benefits of implementing the option considering the nature of the risk. A number of options can be considered and applied individually or collectively (See below).

3. Identify in priority order the individual risk treatment plan actions based on the treatment options selected. Where treatment actions impact elsewhere in the organisation or with stakeholders, they should be involved in developing the treatment plan.

4. Assess the future risk ranking, after considering successful implementation of the mitigation plans.

5. Document this on the *Risk Action Plan Template*.

Progress against treatment plan actions for High and Severe risks will be reported to both the Board and the FARC.

Note: The Board will receive the full risk register each quarter however discussion will only be had on changes and new risks.

Treatment options can include the following:

- Accept the level of risk and do nothing
- Reduce the likelihood of consequence (for example, insurance coverage)
- Shift responsibility to external party/expert
- Increase risk to pursue opportunity

5. Control Effectiveness Criteria

The effectiveness of the existing controls for each risk needs to be assessed against the criteria in the below table. This assessment must consider the current status of controls in place for the risk.

Control effectiveness rating table

Rating	Description
Fully effective	Controls and processes are well designed for the risk, are operating effectively and are well documented. Reliability and repeatability have been shown through monitoring processes. Controls are well understood. Continue to monitor and review existing controls.
Substantially effective	Most controls/processes are designed correctly and are in place and effective. Some more work to be done to ensure reliability and repeatability, or to improve operating effectiveness. Controls are largely understood.
Partially effective	While the design of the controls is largely correct, the controls are not currently in place or very effective. There is only limited understanding of the controls. **OR** The controls that are in place are operating effectively and repeatedly and well understood, however some of the control design does not effectively mitigate the root cause/s of the risk.
Substantially ineffective	Significant control gaps or process weakness. Either controls do not treat the root causes of the risk appropriately, or they do not operate at all effectively or reliably. Little knowledge or verification is available.
Totally ineffective	Virtually no credible controls in place. Poor control design and very limited/no effectiveness in mitigating the root cause/s of the risk.