Badminton Australia

Enterprise Risk Management Framework

Version 0.1 (October 2020)

Enterprise Risk Management Framework

Badminton Australia

Contents

1. Purpose and Scope

Consistent with ISO 31000, Badminton Australia Ltd (BA) adopts the definition of risk management as follows:

"The processes, systems and culture applied in order to manage both the upside and downside of uncertainty on the strategic objectives of the Badminton Australia Ltd Board."

BA's Vision is to 'Encourage widespread participation opportunities, increase the popularity and raise performance standards of Badminton in Australia'.

To meet our Vision we must work collaboratively with key stakeholders to provide quality participation opportunites and pathways within Badminton.

Our ongoing success is considered to be a product of delivering upon our key objectives:.

1. Grow the Membership Base
2. Grow Participation
3. Improve high performance results
4. Run quality world class events
5. Develop the culture of the sport
6. Create a strong brand

To facilitate the achievement of our Vision and underlying strategy, the Board of Directors and the Audit and Risk Committee (ARC) support the development of practical risk management business rules. We acknowledge the significance of managing risks and identifying opportunities in a measured way to ensure we deliver on our key objectives.

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 Management Team and the Board of BA 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.

The Enterprise Risk Management Framework is a document mandated by the Board of Directors, but owned by the ARC, as the ARC is responsible for overseeing the audit and risk assessment function for BA.

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 ARC

The maintenance of a sustainable risk management function that supports the organisation remains the ultimate responsibility of the Board with oversight from the ARC. The Board and ARC, 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 ARC 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 ARC to ensure that risk management is embedded in the organisation includes the following:

- 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 Management Team.

2.1.4 Management Team

While the Enterprise risk management function is enabled by the Board and supported by the CEO the risk management processes as outlined in Section 4 remains the day to day responsibility of the Management Team. The Management Team have the responsibility to complete the following roles.

- **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.

2.1.4 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 Leadership Team.

2.1.5 BA Volunteers and Officials

Our volunteers are integral to our success. We support our 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.

2.2 Risk Reporting

The CEO in conjunction with the Management Team 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 package* to support the identification and management of risks and incidents to the ARC, on behalf of the Board, for presentation as follows:

i. Updates to risk register (at least every 6 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 package is to ensure that risk related matters are discussed in an appropriate forum and to ensure that the ARC 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', we recognise that the Board, Management, staff, contractors and volunteers must be consistent in our communication and clear in our mission to mitigate risk that may impact BA.

We also believe that risk mitigation is not isolated to Board, Management, staff, contractors and volunteers but a key part of the role stakeholders and supporters who contribute to the success of BA.

2.4 Risk Management 'Activity' Template

In addition to the orgnisaitonal risk management processes, BA will establish a Risk Management 'Actiivty' Template. This template will be used at the discretion of the CEO for use on 'one off' 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 children
- 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.

	What	Who	When
1	***Risk framework and context***		
	Review Enterprise Risk Management Framework	ARC	Annually (February)
	Endorse the Enterprise Risk Management Framework	Board and ARC	Annually (February)
2	***Risk identification, risk assessment, risk evaluation, risk mitigation***		
	Identify, assesses and review strategic and operational risks as part of formal workshop	Management Team	Annually (July)
	Review risk register compiled as part of formal workshop process	Board and ARC	Annually (July)
	Review and update risk register, and identify any new risks	Management Team	At least every 6 months
	Compile risk reporting package for the CEO to distribute to ARC and Board	CEO	For each ARC 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
3	***Risk monitoring and reviewing***		
	Review treatment plans for High and Extreme risks	ARC	At Quarterly ARC meetings
	Review treatment actions	Management Team	Monthly
	External audits	Morton, Watson and Young or appointed auditor	Annually
4	***Risk reporting***		
	Compile *risk reporting package* for the CEO to distribute to ARC and Board	CEO	For each ARC and Board meeting

3.2 Training

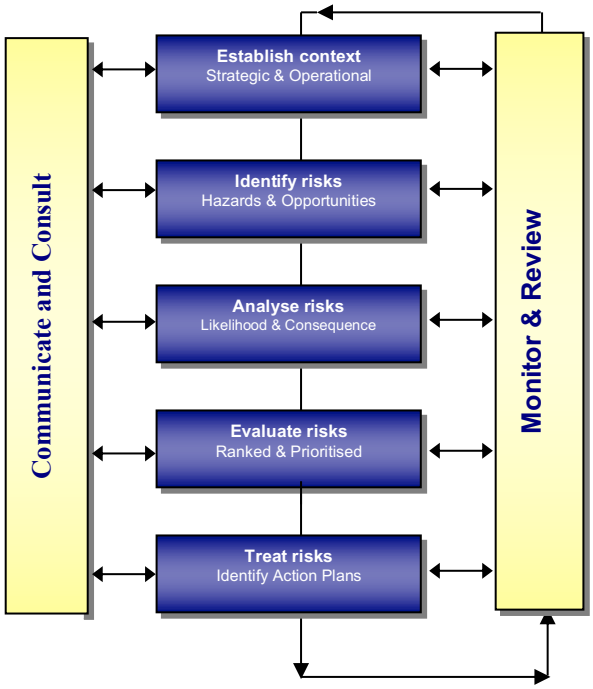
In order to build organisational capability and common understanding, training that supports risk leadership and accountability for risk owners and staff is undertaken as needed.

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 is 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 of the organisation.

Monitor and Review

Monitoring and review procedures need to be incorporated into both strategic and day-to-day operational activities in order 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 ARC has a focus on the following risk types:

Finance – risks and opportunities that may impact the financial performance, fraud, theft, conflict of interest, duplication of payments, expenditure and revenue budget of BA.

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.

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.

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 or not 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.

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 least monthly.	Board ARC CEO
High	Escalation and immediate course of action to be determined within 30 days and documented in treatment plan. To be monitored quarterly. **OR** Risk deemed 'acceptable' pursuant to BA strategy by the Board and ARC	ARC CEO
Medium	Acceptable risk - may require further assessment and be monitored quarterly.	Risk owners Management Team
Low	Acceptable risk – continue to manage as normal review annually.	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 ARC 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 ARC.

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 has 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 avalbale.
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.