



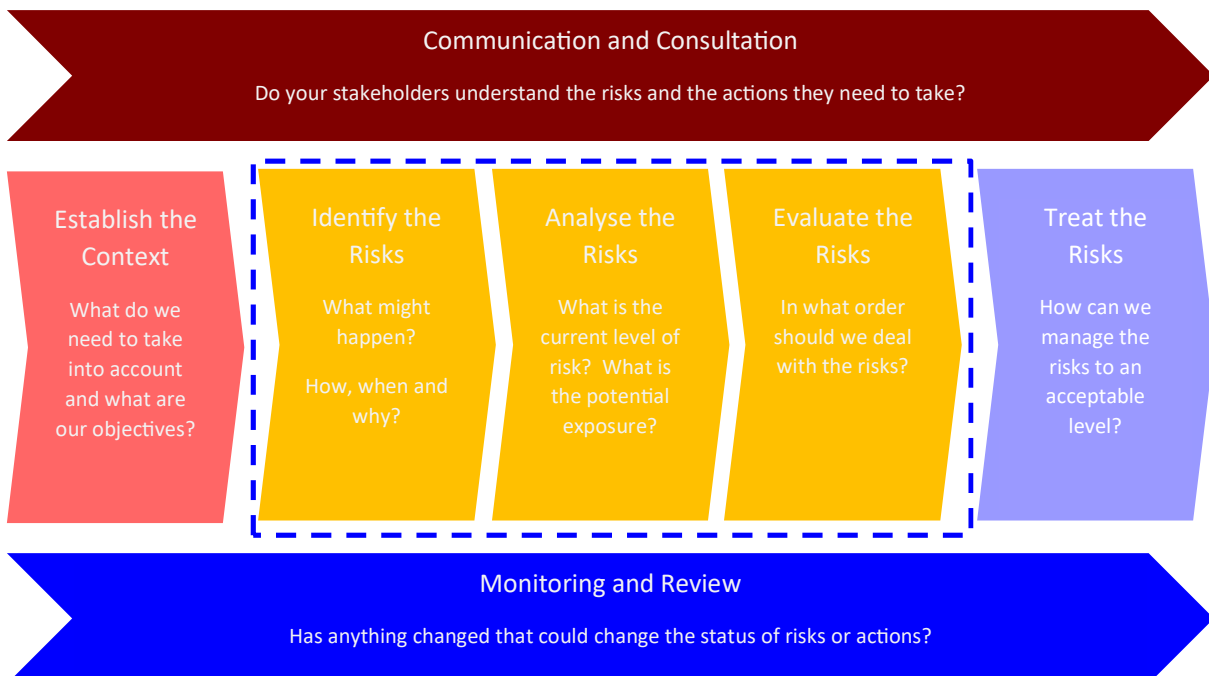
## Risk Management Plan

### Introduction

The steps in managing risk are as follows:

- » **Establish the Context** – identify the objectives of the church and the key stakeholders in relation to these objectives
- » **Risk Assessment**
  - » **Identify Risks** – identify where, when, why and how events could prevent, degrade, delay, or enhance the achievement of organizational goals
  - » **Analyse Risks** – determine the consequences of the risk being realised and likelihood of the risk being realised to calculate the level or rating of the risk
  - » **Evaluate Risks** – apply acceptance criteria to determine the action that needs to be taken for a risk
- » **Treat Risks** – develop and implement cost-effective action plans for increasing potential benefits and reducing potential costs
- » **Monitor Risks** – monitor the effectiveness of the controls that have been employed to treat risks

These steps, along with communication and consultation work together as shown in the following diagram:





---

## Communication and Consultation

Communication and consultation are key to Risk Management achieving its purpose of ensuring a consistent approach to the management of all risk for BNJCA.

This policy and process for managing risks must continue to be reviewed, maintained and remain appropriate for BNJCA. This continuous review and improvement process must involve consultation across all ministry areas.

Continuous communication and consultation with internal and external key stakeholders are required at all stages of the Risk Management Process as their involvement and input is an essential factor of effective risk management.

You need to identify and collaborate with key stakeholders to best manage a risk. This means:

- » you understand the key stakeholder's expectations
- » they are aware of their roles and responsibilities
- » they are aware of the risks and controls that impact BNJCA objectives
- » they are kept informed about the progress and key outcomes

### When to Communicate

There should be communication and consultation at every step of the Risk Management Process. Triggers for further communication include:

- » new risks identified due to a change in internal or external operating environment (or both)
- » there are significant failures in the effectiveness of controls
- » there are areas of uncertainty and insufficient information is available to analyse and evaluate the risk
- » treatment actions are behind schedule or overdue

### How to Communicate

There are many ways that you can communicate and consult with your stakeholders. These include:

- » meetings (e.g., regularly discussing risk management at meetings with staff who can assist in identifying, assessing, and managing risks)
- » workshops (e.g., a risk assessment workshop with staff to analyse the impact of risks and evaluate different Risk Treatment actions)
- » email
- » reports and memos to the management (e.g., monthly reporting for management to monitor and review the status of risks and treatment plans)
- » informal conversations

Factors to consider when communicating and consulting with stakeholders:

- » Determine 'who is the audience' when you communicate with broad stakeholders (consider staff, volunteers, visitors, public, Risk Owners and Church Council).



- » Also consider external stakeholders and interdependencies to ensure all relevant and appropriate information is shared with key stakeholders.
- » Ensure that Church Council receives appropriate and regular assurance about the management of risk.

---

## **Establish the Context**

This is not only part of the setup of the management system, but also part of the on-going maintenance.

The context is derived from ministry requirements and involves setting the basic criteria necessary for risk management and defining the scope and boundaries for the activities of BNJCA.

### **Identify the objectives**

As risks have the potential to adversely impact the achievement of BNJCA objectives, it is important that the first step in the risk management process is to confirm the priorities and objectives of BNJCA.

The aim is to provide adequate controls/actions to protect BNJCA, while avoiding hindering the work of BNJCA or its processes, as is feasibly possible.

### **Identify the key stakeholders**

It is important at this stage to identify key stakeholders:

- » Who should be consulted during the risk management process? Who makes the decision on acceptable risk for this particular part of the business operations? Once you've identified the stakeholders, work closely with them to understand:
  - » What are their perceptions (e.g., objectives for the risk management activity), criteria and specific needs (e.g., expectations for any outputs)?
  - » What is their appetite for accepting certain risks (e.g., which risks are they willing to accept, and which risks will they not tolerate)?
- » Who is knowledgeable about the risk and the available controls?
- » Who is the customer and what are their needs? What is the impact to customers?
- » Does this have flow-on effects to other parts of the business?

It is essential for the stakeholders to understand their business objectives, as it provides focus when undertaking risk management activities, such as facilitating risk workshops and developing risk profiles.

### **Environment & stakeholder analysis**

An understanding of the business context is necessary to understand how potential external and internal events may impact the business.

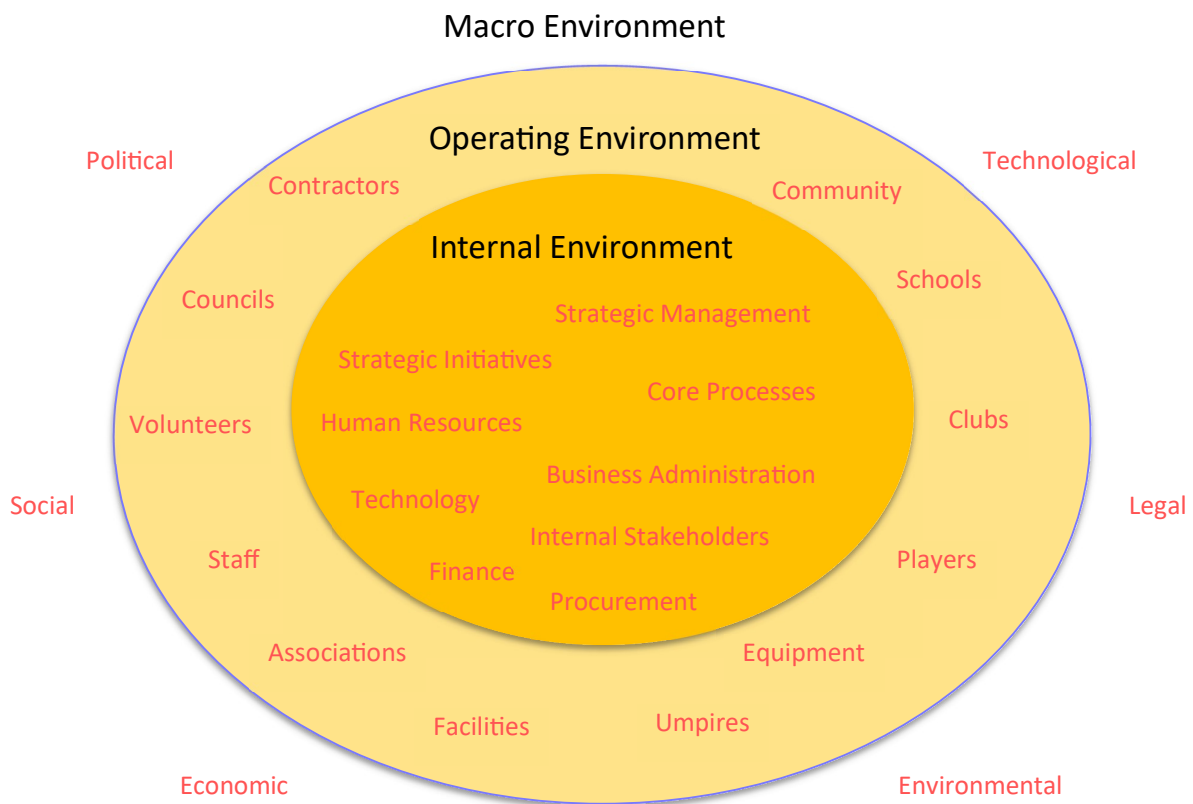
The following 'Environment & Stakeholder Analysis Model' has been used to assist with identifying internal and external environmental factors that may influence the business as well as identify various sources of potential operational risks.

This involves:



- » Considering the internal environment – including relevant objectives and related policies, processes, technologies, and internal key stakeholders that can influence the achievement of objectives.
- » Considering the external environment – including the regulatory environment, macro-economic factors, drivers and trends, and the perceptions and expectations of key external stakeholders

The purpose of performing the environmental and stakeholder analysis is to identify the sources of risk which align to relevant objectives/priorities by considering external and internal factors that influence the operation of BNJCA.



### Macro environment

The following table provides examples of the sources of macro i.e., large-scale factors which may potentially contribute to an event which impacts BNJCA.



Macro Area	Definition and Examples of Risk Sources
Political	<p><b>Definition:</b> The political environment considers how and to what degree a government intervenes in society.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Government legislation – (impacting social and ethical issues)</li> <li>Government stability – (change of focus)</li> </ul>
Economic	<p><b>Definition:</b> Economic events which may affect how BNJCA operates and makes decisions.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Issues that change tithing patterns</li> <li>Employment market and staff turn over</li> <li>Budget constraints</li> </ul>
Social	<p><b>Definition:</b> The social environment considers cultural aspects in society which may affect how BNJCA operates or the programs and services that need to be provided.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Public safety</li> <li>Environmental impact</li> <li>Marriage and family breakdown</li> <li>Adverse publicity about an incident</li> </ul>
Technological	<p><b>Definition:</b> The technological environment considers ecological and environmental aspects which may cause technological changes.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Automation Systems</li> <li>Rate of technological change</li> <li>Technical resource availability</li> </ul>
Legal	<p><b>Definition:</b> The legal environment (and related regulatory expectations) may affect BNJCA costs and/or how it operates.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Changes to relevant local regulations</li> <li>Litigation or class action</li> </ul>
Environmental	<p><b>Definition:</b> Considers those sources of risk occurring from the natural environment.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Fire – system/plant fire or bushfire</li> <li>Flood – natural or man-made</li> <li>Extreme weather conditions (e.g., heat, lightning, severe storms)</li> <li>Pandemic</li> <li>Environmental spills</li> <li>Climate change</li> <li>As well as stakeholder expectations of how BNJCA manages all these</li> </ul>

## Operating Environment

The following table provides examples of the sources of operating environment factors which may potentially contribute to an event which impacts BNJCA.



Industry	Definition and Examples of Risk Sources
Community	<p><b>Definition:</b> The general public in and around the Brisbane North area who may have an impact on or use services from BNJCA.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Unmet expectation</li> <li>Adverse publicity in regard an incident</li> </ul>
Schools	<p><b>Definition:</b> Schools where BNJCA has a direct association through the delivery of Religious Education or Chaplaincy programs.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Unmet expectation</li> <li>Misalignment of ethos</li> <li>Breaching limitations of activity or influence</li> </ul>
Contractors	<p><b>Definition:</b> The term ‘contractors’ refer to the third-party organisations with whom BNJCA contracts with, to source solution components and/or deliver aspects of a solution.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Provision of poor service</li> <li>Maintenance practices could cause impact to service</li> <li>Delays in the delivery of equipment or ability to deliver as per specifications</li> <li>Impact of parts availability for repair or replacement</li> <li>Auditing and compliance practices</li> <li>Staffing changes</li> <li>Contractor relationship</li> <li>Contractual and financial disputes</li> <li>Supply chain – importation of goods</li> </ul>
Clubs	<p><b>Definition:</b> Any club that is affiliated to BNJCA. Actions of any staff member or volunteer from an affiliated club are deemed to be actions of that club</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Delay in registration payments</li> <li>Delay in providing player information</li> <li>Delay in providing nomination for representative cricket activities</li> <li>Noncompliance with BNJCA policies</li> <li>Misalignment of strategies</li> <li>Unmet expectations</li> <li>Decisions that bind or limit the actions of BNJCA</li> <li>Any action by a staff member or volunteer in violation of the officials code of conduct</li> <li>Messaging on social and broadcast media that adversely impacts BNJCA objectives</li> </ul>
Facilities	<p><b>Definition:</b> Buildings, structures, and property under the management of BNJCA</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Unsafe fittings and fixtures</li> <li>Damage to facilities</li> <li>Poor construction</li> <li>Unsafe design and/or construction</li> </ul>



Industry	Definition and Examples of Risk Sources
Equipment	<p><b>Definition:</b> Any machinery, tools, playing equipment or training items that are owned by BNJCA.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Damage</li> <li>Inappropriate use</li> <li>Projected at speed (balls)</li> </ul>
Volunteers	<p><b>Definition:</b> The term ‘volunteer’ refers to any individual who occupies a role in an un-paid capacity for BNJCA</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Provision of poor service</li> <li>Unauthorised or unethical behaviour</li> <li>Committing BNJCA beyond delegated authority</li> <li>Making decisions beyond delegated authority</li> </ul>
Staff	<p><b>Definition:</b> Anyone who is paid a casual or permanent wage by BNJCA.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Provision of poor service</li> <li>Unauthorised or unethical behaviour</li> <li>Committing BNJCA beyond delegated authority</li> <li>Making decisions beyond delegated authority</li> </ul>
Councils	<p><b>Definition:</b> The local councils where BNJCA maintain facilities or operate services</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Decisions against BNJCA requests or applications</li> <li>Planning/zoning changes</li> <li>Change of Councillor for wards/divisions with BNJCA facilities</li> </ul>
Associations	<p><b>Definition:</b> Other cricket associations with whom BNJCA coordinates or collaborates including:</p> <ul style="list-style-type: none"> <li>Cricket Australia</li> <li>Queensland Cricket</li> <li>Warehouse Cricket</li> <li>Subdistricts Cricket</li> <li>Queensland Junior Cricket and</li> <li>Junior cricket associations that are affiliated with Queensland Junior Cricket</li> <li>Far North Coast (NSW) Cricket</li> <li>Actions of any staff member or volunteer of another association are deemed to be actions of that association</li> </ul> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Provision of poor service</li> <li>Decisions that are prejudiced against BNJCA</li> <li>Changes that impact BNJCA</li> <li>Representative and development competitions</li> <li>Activities that impinge on the BNJCA player base</li> </ul>



Industry	Definition and Examples of Risk Sources
Umpires	<p><b>Definition:</b> The game officials provided by umpiring associations for stage 2 and stage 3 representative games</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Unavailability</li> <li>Umpires with inadequate experience/skill</li> </ul>
Players	<p><b>Definition:</b> Any player that qualifies as a junior player from any affiliated club. Parents of players are also included in this category.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Unmet expectation</li> <li>Unauthorised or unethical behaviour</li> <li>Any action in violation of the players code of conduct</li> <li>Any action in violation of the parents /spectators code of conduct</li> <li>Messaging on social and broadcast media that adversely impacts BNJCA objectives</li> </ul>

## Internal Environment

The following table provides examples of the sources of internal environment factors which may potentially contribute to an event which impacts BNJCA.

Area	Definition and Examples of Risk Sources
Core Processes	<p><b>Definition:</b> These are processes which define BNJCA's existence as a faith organisation and what BNJCA is providing to their community. These core processes comprise:</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Failure of employees to follow business processes</li> <li>Processes are not correctly documented</li> <li>Inadequate Service and service level management</li> <li>Equipment failures</li> <li>External or internal malicious attacks</li> </ul>
Strategic Management	<p><b>Definition:</b> These are the processes for strategy setting, business planning and performance management against strategic and operational objectives. This includes, but is not limited to policies, objectives, communication, and alignment across BNJCA initiatives.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Service portfolio management</li> <li>Demand management</li> <li>Change management</li> <li>Risk management</li> <li>Capacity management</li> <li>Availability management</li> <li>Compliance management</li> <li>People</li> </ul>





Area	Definition and Examples of Risk Sources
Human Resource Management	<p><b>Definition:</b> Human Resource Management consists of the processes for employing, training, inducting, developing, disciplining, and terminating staff.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Training strategy and plans are not sufficient for supporting the business</li> <li>Gaps in employee or Council level skills and/or capability</li> <li>Employment of resources with inadequate experience/skill</li> <li>Resignation of key employees or Council members</li> <li>Unclear roles &amp; responsibilities for individuals</li> </ul>
Technology Management	<p><b>Definition:</b> Changes, failures or deficiencies in technology such as audio-visual infrastructure, systems and hardware and network transmission services.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Maintenance of systems and hardware not carried out</li> <li>Cyber security threats/attacks</li> <li>Execution of Performance or Capacity Management</li> <li>Critical applications and/or systems failures</li> <li>Facility outages or failures</li> <li>Configuration errors</li> <li>Identity and access management shortcomings</li> </ul>
Accounting and Finance Management	<p><b>Definition:</b> Processes for management and financial accounting.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Poor execution of finance management processes e.g., delegations and reconciliations</li> <li>Ability to fund growth – budget limitations</li> <li>Adverse financial audit findings</li> <li>Breach of banking covenants</li> <li>Workers' compensation risk</li> </ul>
Procurement Management	<p><b>Definition:</b> Processes for managing the sourcing, contracting, measuring, and transitioning third parties who provide products and/or services.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Supplier relationships</li> <li>Contract management</li> <li>Invoice management</li> <li>Staffing changes</li> <li>Supply levels</li> <li>Contractual and financial disputes</li> </ul>
Business Administration	<p><b>Definition:</b> Processes for overall administrative management of the business.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"> <li>Accuracy of service, financial and performance reporting</li> <li>Receivables and payables accuracy</li> <li>Breakdown in communication and/or decision-making processes</li> <li>Auditing and compliance</li> </ul>



Area	Definition and Examples of Risk Sources
Internal Stakeholders	<p><b>Definition:</b> Internal stakeholders include staff and volunteers.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"><li>Unauthorised or unethical behaviour</li><li>Fraudulent or illegal activities</li><li>Industrial action</li><li>Decisions made by management which could impact service delivery</li></ul>
Strategic Initiatives	<p><b>Definition:</b> Delivery and implementation of strategic initiatives, organisational restructure, and stakeholder relations.</p> <p><b>Sources of risk include:</b></p> <ul style="list-style-type: none"><li>Misalignment of organisational structure and/or the allocation of resources to deliver services</li><li>Program challenges to meet budget, timeframes and expected benefits</li><li>Ineffective deployment of new initiatives</li><li>Internal support structure and practices could change and impact delivery of service during implementation</li></ul>

## Identify Risks

The purpose of this step is to identify sources of risk and define their related risk event, cause(s), consequence(s) and an owner.

Risk identification is about understanding what might happen and who is accountable.

At the end of this step, you will have a comprehensive list of risks based on events which may occur, and which might have an impact on the achievement of the objective (in terms of enhancing, preventing, degrading, or delaying achieving the objectives).

The risk identification process should answer these questions:

- » What could occur?
- » Who could it impact?
- » Where could it occur?
- » Why could it occur?
- » How could it arise?

## Consider potential sources of risk

You can conduct an environmental and stakeholder analysis to identify potential sources of risk.

Information gathered during the first step, 'Establishing the Context', can also be used during this stage to assist with identifying potential sources of risk. Risk sources arise from the internal and external environment in which BNJCA operates and may or may not be under the control of BNJCA.

The sources of risk you identify are not in themselves potential risks. Instead, the sources will help you identify the potential causes for risk events. Each source may provide multiple causes for a risk event. To help enumerate the causes that may contribute to a risk event, the following lists provide parameters to be considered:



Threat Type		
» Access Control Failure	» Incorrect Processing	» Regulatory
» Governance/Monitoring	» Operations Continuity	» Third Parties
» Physical and Environment	» Equipment failure	» Human Resources
» Unethical/Illegal activity	» Data Compromise	» Hazard
Origin	Impact Group	
» Accidental	» Individual	
» Deliberate	» Financial	
» Environmental	» Compliance	
	» Community	
Actor		
» Negligent worker	» General public	» Criminal activity
» Rogue worker	» Contractor	
» Visitor	» Natural event	

Other methods used to identify sources of risk include:

- » interviews (1:1 or group) with relevant key stakeholders
- » facilitated workshop discussions with key stakeholders
- » incident analysis
- » external and internal reviews
- » information searches on risks facing churches
- » process mapping / scenario simulation
- » audit / monitoring
- » judgement from Subject Matter Experts
- » Post-Implementation-Reviews of past projects
- » SWOT (strength, weakness, opportunity, threats) analysis
- » checklists
- » event / loss data

## Define the Risk

Once a risk event has been identified, it needs to be defined.

A risk is an event that could occur in the future, which could affect the achievement of objectives.

However, defining a risk is not as easy as it seems, common mistakes are often:

- » Stating a missing or failing risk treatment (e.g., lack of suitable door locks), rather than the actual risk event (e.g., unauthorised entry to property); or
- » Stating an already existing issue, rather than a risk event (that has the potential to occur).

Define the risk statement in the form:

*“There is a risk of <a threat event>, due to <causes/weaknesses>, resulting in <consequences>”.*



## Identify a Risk Owner

A Risk Owner should be allocated. This is the person with the responsibility and authority to manage the risk, and is usually directly responsible for the strategy, activity or function that relates to the risk.

---

## Risk Analysis

The purpose of this step is to develop a more detailed understanding of the risks in order to prioritise them based on their Risk Exposure Level.

Risk analysis is about considering current controls and their effectiveness; analysing the likelihood of the risk occurring, analysing the consequences of the risk; and determining the current risk exposure.

Analysis can be qualitative (such as expert opinion), quantitative (such as assessing an event/issues history or modelling), or a combination of these.

The Risk Exposure Level is determined by combining the consequences of a risk event with the likelihood of the risk event occurring.

The knowledge gained during this phase enables you to understand the effectiveness of current controls and the current risk exposure; which will help in the decision-making process of risk prioritisation - in terms of determining whether risks need to be treated. It will also help to ensure that we don't get distracted by minor risks while ignoring more serious risks that are less understood.

The type of information used to support analysis of risks can include:

- » business history and experiences
- » industry information and experience (local and international)
- » relevant incident data (internal and/or external)
- » market insights and competitor analysis
- » subject matter expertise and insights

## Consider current risk treatments

Before analysing each risk, the Risk Owner and relevant key stakeholders should firstly identify the current treatments already in place and examine their effectiveness to modify the likelihood and potential consequences of the risk to an acceptable level. Usually, it requires more than one person to identify current controls and assess their effectiveness.

## Identify risk treatment actions

A control is a measure (or combination of) that aims to manage or modify (i.e., reduce, increase, prevent, or eliminate) the risk; usually by reducing the likelihood and /or impact or consequence of the risk.

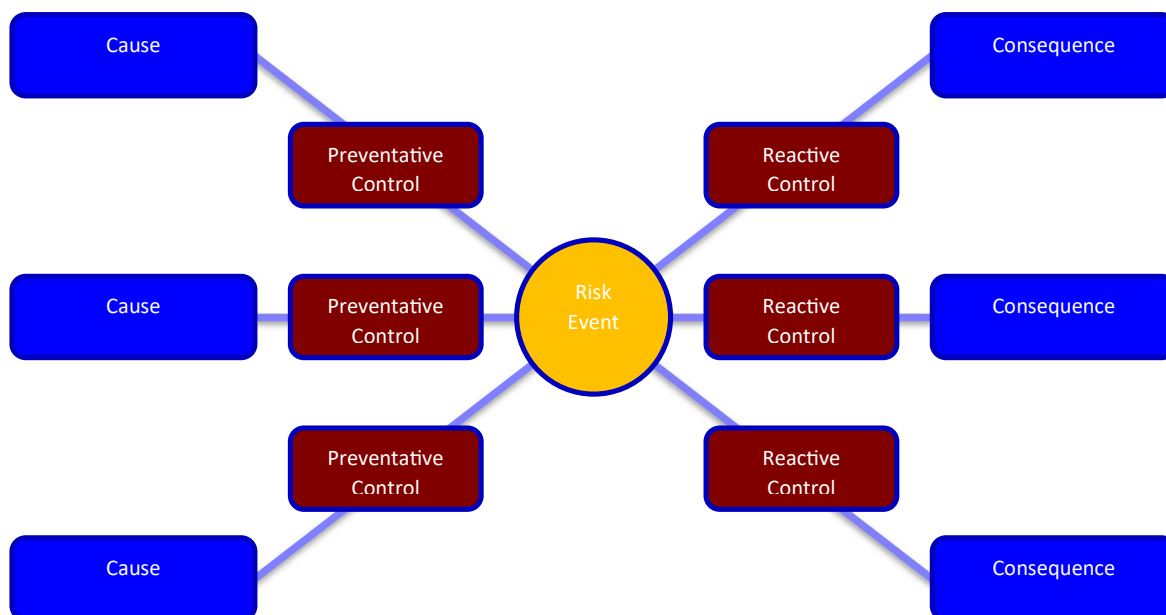
This activity may not always require producing an exhaustive inventory of all individual risk controls and treatment actions in place; in some instances, a more high-level consideration of the effectiveness of the key controls that are currently in place to manage the risk may be sufficient.



Each key control should have a control owner; and risks typically have, or require, multiple risk controls and treatment actions.

You can define potential controls by identifying the causes and consequences of any risk event.

Causes are factors that trigger or lead to a risk event occurring. Consequences are the impacts on the objectives if the risk event occurs. It's critical we understand the 'cause' because it's the key factor we can control or treat. A risk event can have more than one cause or consequence (this includes financial, employee, reputation, etc.). The diagram below shows the connection between cause, risk event and consequence, and shows how preventative and reactive controls that can be employed to prevent the cause or mitigate the consequence.



### Analyse the likelihood of the risk

Every risk event has a likelihood of occurring.

The analysis of likelihood considers the current risk controls in place to modify the likelihood of the risk event occurring.

Determining likelihood is an art not a science. It requires professional judgment. This activity requires the Risk Owner to work closely with key stakeholders to analyse the likelihood of a risk event occurring, in order to evaluate the significance of the risk.

Significance of risk likelihood is determined by using the criteria in the Risk Likelihood Table.

Likelihood can be assessed on six levels based on frequency or via a qualitative description. You can use whichever measure best suits your needs, however the category that results in the highest likelihood rating prevails.



The likelihood rating should be selected with respect to severity of the consequence rating (discussed in the next section). For instance, it's common for risks with more severe consequence to occur with a low frequency. On the other hand, risks with smaller business impact may be more likely to occur.

Likelihood ratings are directly linked to risk causes because the causes explain what drives the risk.

Likelihood	Expectation	Experience	Probability
Almost certain	Expected to occur in most circumstances	Happens at least once at most events of this type	> 90%
Likely	Expected to occur occasionally	Happens at more than half the events of this type	65% - 90%
Possible	Expected sometimes	Happens once every three or four events of this type	20% - 65%
Unlikely	Occurs only in unusual circumstances	Has only happened once or twice before in the last 5 years for an event or facility of this type	5% - 20%
Rare	Not expected to occur but not impossible	Have not seen this happen at an event or facility of this type.	< 5%

## Analyse the consequences of the risk

Risk events can also be assessed in terms of consequence severity and impact if it occurred.

This degree of risk analysis requires the Risk Owner to work closely with key stakeholders in order to identify and analyse the potential consequences of a risk event.

A risk event may have multiple consequences. The analysis of consequence must consider the current risk controls in place that can modify the consequence of the risk event.

Significance of risk consequence is determined using the criteria in the Risk Consequence Table.

The Risk Consequence Table can be used to measure the consequence severity in terms of (quantitative and/or qualitative) impacts to one of the four impact areas; and assign a consequence rating to a risk event ranging from 'Minor' to 'Extreme'.

These four impact areas are:

Individuals	Community	Financial	Compliance
<b>Examples include:</b>	<b>Examples include:</b>	<b>Examples include:</b>	<b>Examples include:</b>
Health and Safety	Delivery of services	Income	Legal
Wellbeing	Reputation	Expenditure	Environmental
Injury	Supply chain	Budgets	Regulation
		Damages	Government

Risk Owners only need to assess the aspects of the Risk Consequence Table that are relevant to their potential risks.

A conservative approach should be undertaken when deciding on a rating. For example, if the key impacts for a risk fall into multiple columns, the column associated with the most severe rating should be the final rating (i.e., If you have Financial impact at 'Major', and Reputation impact at 'Extreme', then you should rate the consequence of the risk as 'Extreme').



Consequence	Wellbeing	Reputation	Financial	Disruption
Catastrophic	Death or disablement of a player, volunteer, employee, contractor, or member of the general public related to BNJCA facilities, BNJCA equipment or actions at a BNJCA event.	Negative media coverage outside Queensland. Several clubs leave the association.	More than \$100K	No fixtures can be played for the remainder of the season. No representative teams attend Championships or Development Carnivals this season.
Major Loss	Serious injury requiring emergency medical treatment of a player, volunteer, employee, contractor, or member of the general public related to BNJCA facilities, BNJCA equipment or actions at a BNJCA event.	Negative media coverage within Queensland. Ongoing negative commentary on social media. Prolonged stream of dissenting emails. One club leaves the association.	\$25K - \$100K	No fixtures can be played for two or more weekends. The association event has to be cancelled One or two representative teams do not attend Championships or Development Carnivals
Moderate Loss	Injury requiring medical treatment of a player, volunteer, employee, contractor, or member of the general public related to BNJCA facilities, BNJCA equipment or actions at a BNJCA event.	Negative media coverage within the North Brisbane region. Several negative comments on social media. A short period of receiving dissenting emails. Several players stop playing in BNJCA competitions	\$10K - \$25K	No fixtures can be played for one weekend. The association event has to stop immediately. Several players withdraw from representative teams
Minor Loss	Injury requiring first-aid or no medical treatment of a staff member, volunteer or member of the general public related to BNJCA facilities, BNJCA equipment or actions at a BNJCA event.	A few negative social media comments. A couple of dissenting emails. One or two players stop playing in BNJCA competitions.	\$2500 - \$10K	Some matches have to be abandoned for the day. The association event has to be postponed. One or two players withdraw from representative teams
Insignificant	Minor scrapes or bruises that occur commonly occur during the course of a cricket match.		Less than \$2500	Some matches have to stop for a period of time.

Risk is often perceived as a negative impact but there are occasions when accepting a risk may also have a positive consequence. This can be referred to as opportunity. The following table provides a list of positive consequences:



Consequence	Development	Enjoyment	Growth
Minor Gain	Individual players or coaches will notice some improvement in their skills	Individual players will get more enjoyment from their cricket.	A few additional players signed on for one or more clubs
Moderate Gain	Individual players or coaches will notice substantial improvement in their skills	Individual players will get a lot more enjoyment from their cricket	Two or more new teams entered into BNJCA competitions by more than one club.
Major Gain	Most players in a team, most coaches in BNJCA competitions or all Representative coaches will notice a substantial improvement in their skills and team performance reflect this.	Most players across the association in the age group affected will get a lot more enjoyment from their cricket.	Several teams entered into BNJCA competitions by most clubs affiliated with the association.

## Determine the current risk exposure level

Determine the current level of a risk by plotting the likelihood and consequence on the following Risk Matrix.

<<< Consequence >>>

	Insignificant (A)	Minor (B)	Moderate (C)	Major (D)	Catastrophic (E)
Rarely (1)	Low (1A)	Low (1B)	Low (1C)	Medium (1D)	Medium(1E)
Unlikely (2)	Low (2A)	Low (2B)	Medium (2C)	Medium (2D)	High (2E)
Possible (3)	Low (3A)	Medium (3B)	Medium (3C)	Medium (3D)	High (3E)
Likely (4)	Low (4A)	Medium (4B)	Medium (4C)	High (4D)	Extreme (4E)
Almost Certain (5)	Low (5A)	Medium (5B)	High (5C)	High (5D)	Extreme (5E)

<<< Likelihood >>>

## Determining the current opportunity exposure level

Determine the current level of an opportunity by plotting the likelihood and consequence on the following Opportunity Matrix.

<<< Consequence >>>

	Minor (F)	Moderate (G)	Major (H)
Rarely (1)	Low (1F)	Low (1G)	Low (1H)
Unlikely (2)	Low (2F)	Low (2G)	Medium (2H)
Possible (3)	Low (3F)	Medium (3G)	Medium (3H)
Likely (4)	Medium (4F)	Medium (4G)	High (4H)
Almost Certain (5)	Medium (5F)	High (5G)	High (5H)

<<< Likelihood >>>





---

## Risk Evaluation

The level of a risk should be compared against risk evaluation criteria, particularly risk acceptance criteria.

Once the risk has been identified and assigned likelihood and severity of consequence values, then apply the risk acceptance criteria to determine whether or not the risk can be accepted. If it cannot be accepted, then it should be prioritised for treatment.

### Comparing results of risk analysis with risk criteria

To evaluate risks, compare the assessed risks with the risk criteria defined during the context establishment.

Risk criteria used to make decisions should consider the objectives of BNJCA and the views of relevant interested parties. Risk evaluation decisions should be based on comparison of assessed risk with defined acceptance criteria, ideally taking into account the degree of confidence in the assessment.

In some cases, for example frequent occurrence of relatively low consequence events, it can be helpful to consider their cumulative effect over some time scale of interest rather than the risk of each event considered individually, as this can provide a more realistic representation of overall risks.

There may be uncertainties in defining the boundary between those risks that need treatment and those that do not. Under certain circumstances, using a single level as the acceptable level of risk that divides risks that need treatment from those which do not, may not be appropriate. In some cases, it can be more effective to include an element of flexibility into the criteria by incorporating additional parameters such as cost and effectiveness of possible controls.

The levels of risk can be validated based on consensus among risk owners. It is important that risk owners have a conception of the risks they are accountable for that accords with the results of objective assessment. Consequently, any disparity between assessed levels of risk and those perceived by risk owners should be investigated to determine which better approximates to reality.

### Prioritising risks for treatment

Risk evaluation uses the understanding of risk obtained by risk analysis to make proposals for deciding about the next step to take. Those should refer to:

- » whether a risk treatment is required; and
- » priorities for risk treatment considering assessed levels of risks.

Risk criteria used to prioritise risks should consider the objectives of BNJCA, contractual, legal and regulatory requirements and the views of relevant interested parties. Prioritisation as taken in the risk evaluation activity are mainly based on the acceptance criteria.

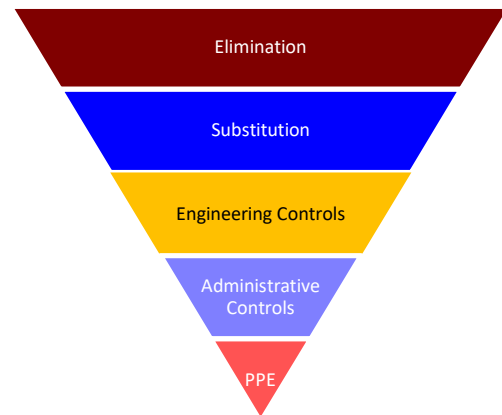


## Risk Treatment

The purpose of this step is to decide how to best treat the risks.

The process of 'risk treatment' is about identifying, selecting and implementing one or more treatment actions to modify risk exposure to an acceptable level.

The types of treatment actions to be implemented should be considered in the order shown in the diagram on the right.



### Develop risk treatment actions

Based on the decision to treat the risk (determined in Risk Evaluation), the risk owner will need to work with the relevant ministry team to develop and agree on the risk treatment actions to further control the risk.

The risk treatment actions will need to include realistic timeframes and identify the Risk Owner who will implement the actions.

### Treatment actions

The agreed upon treatment for some risks (e.g., a strategic-level risk) may consist of one or more major projects. For other risks (e.g., an operational-level risk), the treatment option may consist of a number of new repetitive controls embedded into business processes. Other forms of treatment include:

- » avoiding the risk (e.g., by deciding not to continue or start the activity which gives rise to the risk)
- » taking or increasing risk to pursue an opportunity
- » removing the source of risk
- » taking action (treat) to change the likelihood of this risk (e.g., replace standard door locks with bi-locks)
- » taking action (treat) to change the consequence of this risk (e.g., rapid response or recovery processes)
- » transferring or sharing the risk with another party or parties (e.g., acquire insurance)
- » accepting the current risk by the relevant ministry lead or the Church Council

### How to select the most appropriate treatment actions

The chosen treatment option needs to be checked against the risk appetite to ensure it's the appropriate option to manage the risk.

Treatment actions introduce change, which in itself can introduce new risks.

When selecting the most appropriate treatment option, you should consider:

- » If the likelihood of the risk is high: Reviewing the causes and take into account treatments that will reduce the likelihood (risk prevention).



- » If the consequence of the risk is high: Reactive responses that will address the consequences (i.e., reduce the negative impacts or enhance the positive impacts).
- » The costs and effort in implementing and managing the treatment, compared to the benefit or effectiveness in modifying the risk (e.g., reducing the likelihood or consequence of a risk event, or increased benefit from taking more risk).
- » The simplicity of implementing the treatment plan.
- » The interaction with existing risk treatment controls.

## Implement the risk treatment actions

The implementation of the risk treatment actions is critical to managing the risk, therefore it's important for the risk owner to monitor and communicate any concerns about the timely completion or effectiveness of the risk treatment actions to the Church Administrator for review.

The risk owner is responsible for:

- » developing and obtaining agreement on risk treatments (which need to be specific and relevant)
- » implementing the risk treatments
- » monitoring the progress of implementation
- » reviewing the risk treatments (after they are applied) and their effectiveness to modify the risk exposure

## Monitoring and Review

The monitoring of risk includes reporting, reviewing and assessing. Risks are rated prior to any treatment actions (inherent), with the current treatments in place (current) and also hypothetically when all treatments have been effectively applied (target).

Treatment actions in regard to any risk are always triggered against the current rating of the risk unless an exception is stated otherwise because that is the reality for that risk at the point in time when the trigger action needs to be taken.

## Reporting

The rating level of a risk dictates the timing for implementing treatments and the reporting requirements in relation to that risk. While the risk level is above the acceptable level, the following table indicates the timing for addressing the risk and reporting the risk.

Current Rating	Timing for treatment of the risk	Reporting on identification of the risk
Extreme:	Immediate action required	Notify Executive and Administrator immediately
High:	Plan completed for next Management Committee meeting	Update to be provided at the next Management Committee meeting
Medium:	Plan completed for next Management Committee meeting	Update to be provided at the next Management Committee meeting
Low:	No requirement for specific considerations.	No update required



## Reviewing risks

An internal audit of all risks on the Risk Register should be conducted each year to ensure that the register is up-to-date and that risks treatments are being actioned.

Where a risk has a current rating above the acceptable level, this risk should be reviewed on a weekly basis until the current rating meets the acceptable level.

Where a risk has an inherent rating of high, regardless of the current rating, this risk should be reviewed on a monthly basis to ensure that the risk treatments have remained effective.

## Assessing risk treatment effectiveness

Treatment effectiveness is the degree to which a treatment is successfully modifying the likelihood and/or consequence of a risk.

An effective treatment is a system which provides reasonable assurance about the modification of risk to an acceptable level and achievement of the business's objectives.

The measurement of effectiveness for each treatment is on a scale of 0 to 3 as defined in the following table:

Rating	Description
0	Treatment not implemented
1	Treatment implemented but not effective
2	Treatment implemented but only partially effective
3	Treatment implemented and fully effective

---

## Review

The Risk and Safety Sub-Committee will be the arbiter for interpretation and/or clarification of this plan.

Omissions or errors should be brought to the attention of the Risk and Safety Sub-Committee.

This plan is subject to regular review by the Risk and Safety Sub-Committee and will be amended (as appropriate). Acceptance of a new release of this plan will be supported by a motion from a Management Committee meeting.

---

## Inconsistency with the Association's Constitution

To the extent there is any inconsistency between this plan and the BNJCA Constitution, the Constitution will prevail.

---

## Currency

This plan is current from the published date at the beginning of this document.

This plan remains current until superseded by another Risk Management Plan with a later date of currency.