



# RISK MANAGEMENT PROCEDURE

## CONTENTS

1	PURPOSE .....	1
2	SCOPE .....	1
3	PROCEDURE.....	1
4	RESPONSIBILITIES.....	2
	<b>Compliance, monitoring and review</b> .....	2
	<b>Reporting</b> .....	2
	<b>Records management</b> .....	2
5	DEFINITIONS.....	2
6	RELATED LEGISLATION AND DOCUMENTS .....	2
7	FEEDBACK .....	2
8	APPROVAL AND REVIEW DETAILS .....	2
9	APPENDICES .....	3
1.	Risk Management Framework Part 2.....	3
	Risk Management Procedures .....	4
	<b>Risk Management Process</b> .....	4
	<b>Communication &amp; Consultation</b> .....	6
	Reporting Requirements.....	7
	<b>Coverage &amp; Frequency</b> .....	7
	Key Indicators .....	7
	• Identification .....	7
	<b>Validity of Source</b> .....	7
	<b>Tolerances</b> .....	7
	<b>Monitor &amp; Review</b> .....	7
	Appendix A – Risk Assessment and Acceptance Criteria .....	8
	EXISTING CONTROLS RATING .....	8
	Appendix B – Risk Theme Definitions .....	10
	<b>RISK ACTION PLAN</b> .....	16
	A Risk Action Plan describes how you will implement your organisation’s preferred treatment options for managing the risks that have been identified. ....	16
	After completing the Risk Register, it is helpful to determine where your workshop risk can be reduced and minimized through additional risk management strategies. This IS known as a Risk Action Plan. ....	16
	<i>(Example Risk Action Plan on following page)</i> .....	16

## 1 PURPOSE

- 1.1 To assist in the implementation of the Risk Management Policy of the Diocese of North West Australia (“the Diocese”).

## 2 SCOPE

- 2.1 This Procedure applies to all church workers (clerical, lay, paid & volunteer) within the Diocese and all Diocesan and parish property.

## 3 PROCEDURE

- 3.1 The Diocese aims to achieve best practice, aligned with AS/NZS ISO 31000:2009 Risk Management, in the management of all risks that may affect the Diocese and its workers, church members, assets, functions, objectives and operations; or members of the public.
- 3.2 The provisions of this Procedure can be found in Part 2 of the Diocesan Risk Management Framework (the Framework) located at Appendix 1.

## 4 RESPONSIBILITIES

### Compliance, monitoring and review

- 4.1 The Registrar will monitor and review the achievement of the Risk Management objectives, the management of individual risks and the ongoing identification of issues and trends.

### Reporting

- 4.2 All Diocesan risks to be reported to Trustees and Diocesan Council.
- 4.3 The levels of risk are to be assessed according to the Diocesan Risk Assessment and Acceptance Criteria, to allow consistency and informed decision making.
- 4.4 The Trustees will make recommendations to Diocesan Council for the mitigation of risk.

### Records management

- 4.5 The Registry maintains all records relevant to administering this policy using its recordkeeping system.

## 5 DEFINITIONS

- 5.1 Terms not defined in this document may be found in the Diocesan Glossary.

## 6 RELATED LEGISLATION AND DOCUMENTS

- 6.1 Risk Management Policy

## 7 QUESTIONS & FEEDBACK

- 7.1 Church members may provide feedback about this document by emailing [registrar@anglicandnwa.org](mailto:registrar@anglicandnwa.org).

## 8 APPROVAL AND REVIEW DETAILS

Certifications and Assent	Details	Signature	Date
Chair of Committees	Certified as printed in accordance with the regulation as reported		
Registrar	Certified as passed by the Synod or Diocesan Council or Diocesan Council Executive		
Bishop	Assented		
Approval and Amendment History	Details		
Original Approval Authority and Date	Diocesan Council 24/06/2020		
Next Review Date	24/06/2023		

## 9 APPENDICES

1. Risk Management Framework Part 2
2. Diocesan Strategic Risk Register TEMPLATE
3. Ministry Centre Risk Management Pack
  - A. Risk Management Overview
  - B. Risk Register TEMPLATE (including one example of a potential risk)
  - C. Risk Action Plan TEMPLATE
  - D. Risk Action Plan EXAMPLE

## RISK MANAGEMENT FRAMEWORK – PART 2

### Introduction

This Risk Management Framework (“framework”) sets out the approach by the Diocese of North West Australia (“the Diocese”) to the identification, assessment, management, reporting and monitoring of risks.

The framework is aligned with AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines.

It is essential that all areas of the Diocese adopts this framework to ensure:

- Good governance;
- Compliance with relevant legislation, regulations and internal policies;
- Planning and reporting requirements are met; and
- Uncertainty and its effects on objectives is understood.

The framework, comprising policies in Part 1 and procedures in Part 2, aims to balance a documented, structured and systematic process with the geographical size and complexity of the Diocese, along with existing time, resource and workload pressures.

### Risk Management Procedures

All Ministers-in-Charge of Ministry Centres and the Registrar are required to assess and manage their risk profiles on an ongoing basis.

Each Minister-in-Charge and the Registrar is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the ministry centre or project.
- Reviewed on at least an annual basis, unless there has been a material restructure or change in the risk and control environment.
- Maintained in the standard format.

This process is supported by compliance with this procedure, training workshops and ongoing engagement.

### Risk Management Process

To ensure alignment with ISO 31000:2009 Risk Management, the following approach is to be adopted for all risk assessments.

#### 1. Establishing the Context

The first step in the risk management process is to understand the context within which the risks are to be assessed and what is being assessed. This forms two elements:

##### *Organisational Context*

The Risk Management Procedure provides the basic information and guidance regarding the organisational context to conduct a risk assessment; this includes Risk Assessment and Acceptance Criteria (Appendix A). In addition, existing Risk Themes are to be utilised (Appendix B) where possible to assist in the categorisation of related risks.

Any changes or additions to the Risk Themes must be approved by the Registrar.

All risk assessments are to utilise these documents and templates to allow consistent and comparable risk information to be developed and considered within planning and decision-making processes.

##### *Specific Risk Assessment Context*

To direct the identification of risks, the specific risk assessment context is to be determined prior to and used within the risk assessment process. For risk assessment purposes, the Diocese has been divided into four levels of risk assessment context:

#### Level 1: Strategic Context

Refers to the organisation's external environment and high-level direction. Inputs to establishing the strategic risk assessment context may include:

- The Diocesan Vision and Mission
- Stakeholder Analysis
- Environment Scan / SWOT Analysis
- Existing Strategies / Objectives / Goals

#### Level 2: Operational Context

Refers to the day to day activities, functions, infrastructure and services of the Diocese. Prior to identifying operational risks, the operational area should identify its Key Activities in delivering its Mission, i.e. what is trying to be achieved.

#### Level 3: Project Context

Project Risk has two main components:

- **Risk in Projects** refers to the risks that may arise because of project activity (i.e. impacting on process, resources or IT systems) which may prevent the Diocese from delivering its Mission.
- **Project Risk** refers to the risks which threaten the delivery of project outcomes.

#### Level 4: Hazard Context

This refers to direct physical threats, hazards or vulnerabilities that may harm persons and/or cause loss and damage.

In addition to understanding what is to be assessed, it is also important to understand who are the key stakeholders or areas of expertise that may need to be included within the risk assessment.

## 2. Risk Identification

Using the specific risk assessment context as the foundation and in conjunction with relevant stakeholders, answer the following questions, capture and review the information within each Risk Profile:

- What can go wrong? / What are areas of uncertainty and how does this impact? (Risk Description)
- How may this risk eventuate? (Causal Factors)
- What are the potential consequential outcomes of the risk eventuating? (Resulting In)
- What Risk Theme best applies to the Risk Description? (Risk Theme)
- What are the current measurable activities that mitigate this risk from eventuating? (Existing Controls)

## 3. Risk Analysis

To analyse the risks the Diocese Risk Assessment and Acceptance Criteria (Appendix A) is applied:

#### *Inherent Risk Rating*

- Determine relevant consequence categories and rate how bad it could be if the risk eventuated without existing controls in place (Consequence)
- Determine how likely it is that the risk will eventuate to the determined level of consequence without existing controls in place (Likelihood)
- By combining the measures of consequence and likelihood, determine the inherent risk rating (Level of Risk)

#### *Assessed Risk Rating*

- Based on the documented existing controls, analyse the risk in terms of Existing Control Ratings (Overall Control Rating)
- Determine relevant consequence categories and rate how bad it could be if the risk eventuated with existing controls in place (Consequence)
- Determine how likely it is that the risk will eventuate to the determined level of consequence with existing controls in place (Likelihood)
- By combining the measures of consequence and likelihood, determine the assessed risk rating (Level of Risk)

Risks are not analysed until the existing controls have been taken into account. Accordingly, the first step is to identify existing controls and understand their role in influencing the likelihood and consequence measures. Controls are those things that limit likelihood and consequence, and include such things as

training, management overview, succession planning, passwords, disaster recovery planning, business planning, safety management, etc. The Risk key controls are defined as being:

- Preventative – all about preventing the risk from occurring and limit likelihood
- Detective and Responsive – about identifying the risk as it occurs and rectifying or limiting the consequences

#### 4. Risk Evaluation

The Risk Owner is to verify the risk analysis and make a risk acceptance decision based on:

- Controls Assurance (i.e. are the existing controls in use, effective, documented, up to date and relevant)
- Existing Control Rating
- Level of Risk
- Risk Acceptance Criteria (Appendix A)
- Risk versus Reward / Opportunity

The risk acceptance decision needs to be captured within the risk register and those risks that are acceptable are then subject to the monitor and review process.

Note: A Risk Owner at this point may need to escalate a risk to the Registrar due to its urgency, level of risk or systemic nature.

#### 5. Risk Treatment

For risks deemed unacceptable, determine risk treatment options that may improve existing controls and/or reduce consequence / likelihood to an acceptable level.

Risk treatments may involve actions such as avoid, share, transfer or reduce the risk with the treatment selection and implementation to be based on;

- Cost versus benefit
- Ease of implementation
- Alignment to the Diocesan Mission

For risk treatments that fall outside risk owners delegated level of authority, a formal risk treatment plan is to be developed for endorsement.

Once a treatment has been fully implemented, the Risk Owner is to review the risk information and acceptance decision with the treatment now noted as a control and those risks that are acceptable then become subject to the monitor and review process.

#### 6. Monitoring & Review

Risk Owners to review their acceptable risks at least on an annual basis or if triggered by one of the following; changes to context, new information is available, a treatment is implemented, an incident occurs or due to audit/regulator findings.

Risk Owners are to monitor the status of risk treatment implementation and report on, if required.

The Registrar will monitor and report on significant risks and treatment implementation as part of a Trustees standing agenda item, with specific attention given to risks that meet any of the following criteria:

- Risks with a Level of Risk of High or Extreme
- Risks with Inadequate Existing Control Rating
- Risks with Consequence Rating of Catastrophic
- Risks with Likelihood Rating of Almost Certain

The design and focus of Risk Summary reports will be determined from time to time on the direction of the Audit and Risk Committee of the Trustees who will also monitor the effectiveness of the Risk Management Framework, to ensure it is practical and relevant to the organisation.

## Communication & Consultation

Throughout the risk management process, stakeholders will be identified, and where relevant, be involved in or informed of outputs from the risk management process.

Risk management awareness and training will be provided to all paid workers and key volunteers.

Risk management will be included within the worker induction process to ensure new workers are introduced to the Diocesan risk management culture.

# Reporting Requirements

## Coverage & Frequency

Each ministry centre or business unit is responsible for ensuring:

- That their Risk Profiles are formally reviewed and updated, at least on an annual basis or when there has been a material restructure, change in risk ownership or change in the external environment.
- Risks reported to the Diocesan Office are reflective of the current risk and control environment.

## Key Indicators

Key Indicators (KIs) are required to be used for monitoring and validating key risks and controls. The following describes the process for the creation and reporting of KIs:

- Identification
- Validity of Source
- Tolerances
- Monitor & Review

## Identification

The following represent the minimum standards when identifying appropriate KIs for key risks and controls:

- The risk description and casual factors are fully understood
- The KI is fully relevant to the risk or control
- Predictive KIs are adopted wherever possible
- KIs provide adequate coverage over monitoring key risks and controls

## Validity of Source

In all cases an assessment of the data quality, integrity and frequency must be completed to ensure that the KI data is relevant to the risk or Control.

Where possible the source of the data (data owner) should be independent to the risk owner. Overlapping KI's can be used to provide a level of assurance on data integrity.

If the data or source changes during the life of the KI, the data is required to be revalidated to ensure reporting of the KI against a consistent baseline.

## Tolerances

Tolerances are set based on the Diocese's Risk Appetite. They are set and agreed over four levels:

- Green – within appetite; no action required.
- Yellow – The KI must be monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Amber – the KI must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Red – outside risk appetite; the KI must be escalated to the Bishop or Registrar where appropriate management actions are to be set and implemented to bring the measure back within appetite.

## Monitor & Review

All active KIs are updated as per their stated frequency of the data source.

When monitoring and reviewing KIs, the overall trend must be considered over a longer timeframe instead of individual data movements. The trend of the KI is specifically used as an input to the risk and control assessment.

# Appendix A – Risk Assessment and Acceptance Criteria

## EXISTING CONTROLS RATING

LEVEL	RATING	FORESEEABLE	DESCRIPTION
E	Excellent	Doing more than what is reasonable under the circumstances	Existing controls exceed current legislated, regulatory and compliance requirements, and surpass relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation
A	Adequate	Doing what is reasonable under the circumstances	Existing controls are in accordance with current legislated, regulatory and compliance requirements, and are aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation
I	Inadequate	Not doing some or all things reasonable under the circumstances	Existing controls do not provide confidence that they meet current legislated, regulatory and compliance requirements, and may not be aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation

## MEASURES OF CONSEQUENCE

LEVEL	1	2	3	4	5
RATING	Insignificant	Minor	Moderate	Major	Catastrophic
PEOPLE	Negligible injuries	First aid injuries	Medical type injuries or Lost time injury < 5 days	Lost time injury > 5 days	Fatality, permanent disability
FINANCIAL	Less than \$5,000	\$5,000 - \$50,000	\$50,000 - \$2M	\$2M - \$20M	More than \$20M
OPERATIONS	No material service interruption	Temporary interruption to an activity – backlog cleared with existing resources	Interruption to Service Unit/(s) deliverables – backlog cleared by additional resources	Prolonged interruption of critical core service deliverables – additional resources; performance affected	Indeterminate prolonged interruption of critical core service deliverables – non-performance
REPUTATION	Unsubstantiated, localised low impact on key stakeholder trust, low profile or no media item	Substantiated, localised impact on key stakeholder trust or low media item	Substantiated, public embarrassment, moderate impact on key stakeholder trust or moderate media profile	Substantiated, public embarrassment, widespread high impact on key stakeholder trust, high media profile, third party actions	Substantiated, public embarrassment, widespread loss of key stakeholder trust, high widespread multiple media profile, third party actions
LEGAL / COMPLIANCE	Occasional noticeable temporary non-compliances	Regular noticeable temporary non-compliances	Non-compliance with significant regulatory requirements imposed	Non-compliance results in termination of services or imposed penalties	Non-compliance results in criminal charges or significant damages or penalties



## MEASURES OF LIKELIHOOD

LEVEL	RATING	DESCRIPTION	FREQUENCY
5	<b>Almost Certain</b>	The event is expected to occur in most circumstances	More than once per year
4	<b>Likely</b>	The event will probably occur in most circumstances	At least once per year
3	<b>Possible</b>	The event should occur at some time	At least once in 3 years
2	<b>Unlikely</b>	The event could occur at some time	At least once in 10 years
1	<b>Rare</b>	The event may only occur in exceptional circumstances	Less than once in 15 years

## RISK MATRIX

CONSEQUENCE LIKELIHOOD		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost Certain	5	MEDIUM (5)	HIGH (10)	HIGH (15)	EXTREME (20)	EXTREME (25)
Likely	4	LOW (4)	MEDIUM (8)	HIGH (12)	HIGH (16)	EXTREME (20)
Possible	3	LOW (3)	MEDIUM (6)	MEDIUM (9)	HIGH (12)	HIGH (15)
Unlikely	2	LOW (2)	LOW (4)	MEDIUM (6)	MEDIUM (8)	HIGH (10)
Rare	1	LOW (1)	LOW (2)	LOW (3)	LOW (4)	MEDIUM (5)

## RISK ACCEPTANCE CRITERIA

RISK RANK	LEVEL OF RISK	DESCRIPTION	CRITERIA FOR RISK ACCEPTANCE	RESPONSIBILITY
EXTREME	17 – 25	Urgent Attention Required	Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	Registrar / Trustees
HIGH	10 – 16	Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Archdeacon / Registrar
MEDIUM	5 – 9	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Minister-in-Charge / Manager
LOW	1 – 4	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Churchwarden / Supervisor

NB To improve communication, the Diocese has chosen to use word descriptors to rate risk rather than numbers.

## Appendix B – Risk Theme Definitions

### 1) Key Stakeholder Relationships

Failure to provide or be provided with agreed and/or expected levels of service and engagement to/from key internal or external stakeholders impacting the deliverables of the Ministry Centre and/or Diocese

### 2) Unsustainable / Inefficient Practices & Operations

The difficulties of operating a commercial, sustainable business model within the Diocesan hierarchy, governance framework and historical legacy

### 3) Safety & Health

Inadequate safety and health policy, framework, systems and structures to prevent injury to church workers, contractors, church members and/or visitors in the provision of a working environment or church activities. Includes subsequent public liability and workers compensation claims due to personal harm

### 4) Statutory, Regulatory & Compliance

Failure to correctly identify, interpret, assess, respond, communicate and comply with legislation, statutes and policies

### 5) Fraud & Misconduct

Intentional activities in excess of authority granted to an office holder or employee, which circumvent endorsed statutes, policies, procedures or delegated authority

### 6) Service / Business Interruption

An event causing the inability to continue church activities and/or diocesan functions

### 7) Commercial Development

Failure to effectively manage costs, controls and critical dependencies associated with commercial property development

### 8) Commercial Asset Management

Failure to effectively manage the day to day operations of commercial properties including user/tenant agreements, maintenance and inspection programmes and procedures in place to manage quality, usage and availability

### 9) Parish Property Management

Failure to effectively manage the day to day operations of parish properties including user/tenant agreements, maintenance and inspection programmes and procedures in place to manage quality, usage and availability

### 10) Safe Ministry

Failure to implement, update, renew, communicate and monitor effectiveness of Safe Ministry measures to protect vulnerable members of the church community. Includes subsequent liability and compensation claims.

## STRATEGIC RISK REGISTER TEMPLATE

Diocese of North West Australia

### Strategic Risk Register

Step 1	Establish the Context - Organisational Mission and Key Strategic Objectives									<b>DEFINITIONS</b>	
Mission	<i>To facilitate by prayer, encouragement and resourcing, the work of parishes and diocesan organisations</i>										
Strategic Objectives	<i>Engage local communities</i>										
	<i>Evangelise our contacts</i>										
	<i>Establish people as Christians</i>										
	<i>Equip Christians for service</i>										
<i>Export for the kingdom of God</i>											
Risk Identification				Analyse the risk		Evaluate the Risk			Risk Treatment	Review	
Category	Event	Caused by	Resulting in	Likelihood	Impact	Rating	Rank in Order of Priority	Treatment Type	Treatment Plan (dot points)	Current Status	Review Date

## MINISTRY CENTRE RISK MANAGEMENT PACK

### What is risk?

Risk is the exposure to the possibility of such things as economic or financial loss or gain, physical damage, injury or delay, because of pursuing or not pursuing a particular course of action. The concept of risk includes:

- The perception that something could happen
- The likelihood of it occurring and
- The consequences if it does occur.<sup>1</sup>

As part of providing ministry programs, you are likely to encounter risks. These risks<sup>2</sup> might include:

- Occupational Health and Safety (*including hazards*)
- Financial and administrative
- Property
- Delivery of services
- Public liability
- Litigation
- Public relations

### Descriptions & Ratings

#### Determining the severity of risk

Likelihood – What are the chances the risk situation will occur during a ministry program?	
VERY LIKELY	Occurs routinely & can be expected to occur during the program
LIKELY	Occurs often & a good chance to happen
MODERATE	Should occur at some time
UNLIKELY	Could possibly occur at some time
VERY UNLIKELY	Could possibly occur but would be an exceptional circumstance

Consequence –What harm could result if the situation occurred?	
INSIGNIFICANT	No likely injuries to person, no property damage, no financial loss, no effect on reputation of church, no disruption to the program, aims of program still achieved
MINOR	First aid treatment for person, minor property damage, small financial loss, little impact on reputation of church, little program disruption, most aims of the program achieved
MODERATE	Medical treatment to self or others, significant property damage, some impact on reputation of church, intervention by outside agency needed, significant financial loss, moderate program disruption, some of the aims of program achieved
MAJOR	Extensive injuries or permanent impairment likely, major property damage, significant impact on reputation of church, significant outside intervention, major financial loss, major program disruption, most of the aims of the program not achieved
INTOLERABLE	Permanent impairment or death, property damage irretrievable, irretrievable impact on reputation of church, permanent intervention required (organisational leadership), financial cost lead to closing of program, program irretrievably damaged, none of the program aims achieved

## Level of risk

Consequence or impact	Likelihood				
	ALMOST CERTAIN	LIKELY	POSSIBLE	UNLIKELY	RARE
CATASTROPHIC	Extreme	Extreme	High	High	Medium
MAJOR	Extreme	High	High	Medium	Low
MODERATE	High	High	Medium	Medium	Low
MINOR	High	Medium	Medium	Low	Low
INSIGNIFICANT	Medium	Low	Low	Low	Low

## Level of risk key

Risk rating	Description
LOW	Regular monitoring – risk management strategies ( <i>Hierarchy of Control Measures</i> ) used are likely to be sufficient to manage the risk
MEDIUM	Adapt usual risk management strategies, and monitor progress
HIGH	Identify management plan for specific risks, continuous monitoring by senior church leadership
EXTREME	Considerable attention will need to manage unique needs of the risk situation. Question whether the program can sustain this level of risk

## Adequacy of control measures

Key	Rating	Description
MTA	More than adequate	Addresses all potential risks and includes extensive contingency measures
A	Adequate	Addresses most potential risks and includes some contingency measures
NCA	Not completely adequate	Addresses most potential risks but does not include any contingency measures
TI	Totally inadequate	Does not address all potential risks and does not include any contingency measures

## What is risk management?

Risk management is the process of managing your organisation's exposure to potential liabilities.

It does this by identifying risks in order to prevent them or reduce them, and by providing funds to meet any liability if it occurs.<sup>3</sup>

You should complete a risk assessment for your premises and ministry programs at least annually.

This does not replace a **Hazard Identification** for each ministry program.

The **Risk Assessment** looks at what might happen, whereas **Hazard Identification** looks at what is present at the venue at a specific time.

Note that **Incident Management** involves managing the outcome after there has been an incident or accident. Refer to the Safe Program Policy and Incident Response Procedure.

## MINISTRY CENTRE RISK REGISTER

IDENTIFICATION			ASSESSMENT			
Potential risks (situations/areas)	Results of risk (situation/areas)	Existing control measure	Adequacy of control measure/ justification for rating	Consequence rating	Likelihood rating	Risk rating
EXAMPLE: Too many young people for number of leaders	<ul style="list-style-type: none"> <li>Lack of supervision</li> <li>Inadequate numbers to deal effectively with critical incidents</li> </ul>	Additional leaders available on emergency call	Not completely adequate <ul style="list-style-type: none"> <li>May not be available at the time required</li> <li>Time taken to reach venue may mean they are not there when critical incidents occur</li> </ul>	rate	Likely	ificant

**MINISTRY CENTRE RISK REGISTER (cont)**

IDENTIFICATION			ASSESSMENT			
Potential risks (situations/areas)	Results of risk (situation/areas)	Existing control measure	Adequacy of control measure/ justification for rating	Consequence rating	Likelihood rating	Risk rating
	•		•			

## RISK ACTION PLAN

A Risk Action Plan describes how you will implement your organisation's preferred treatment options for managing the risks that have been identified.

After completing the Risk Register, it is helpful to determine where your workshop risk can be reduced and minimized through additional risk management strategies. This is known as a Risk Action Plan.

(Example Risk Action Plan on following page)

### Risk Action Plan Template

Risk Item			
Recommended Response			
Proposed actions			
Resource requirements			
Responsibilities throughout implementation of the plan			
Time frame for implementation of action			
Reporting & monitoring requirements			
Person responsible to overall implementation of the plan		Date	
Reviewer		Date	



**EXAMPLE RISK ACTION PLAN BASED ON EXAMPLE IN RISK REGISTER**

Risk Item	Too many young people attending for leader numbers		
Recommended Response	Control risk by developing & implementing program resourcing protocols		
Proposed actions	<ul style="list-style-type: none"> <li>• Determine ratios – minimum leader numbers &amp; maximum young</li> <li>• Draw up roster for all main leaders</li> <li>• Secure additional leaders committed to be available each week during hours of program &amp; draw up roster</li> <li>• If leaders not able to be present, they are to notify Youth Worker at least 3 hours prior to commencement of program</li> <li>• If minimum number of leaders not secured, cancel the program for the day</li> <li>• If program cancelled have at least 2 leaders at venue when program due to start to inform young people &amp; notify local school</li> <li>• Leaders to wear identifying clothing (shirts) to enable all young people &amp; parents to identify those in authority</li> </ul>		
Resource requirements	<p>Additional paid hours for Youth Worker to develop &amp; co-ordinate roster.</p> <p>Church leadership to provide material &amp; practical support to enable Youth Worker to complete task roles</p>		
Responsibilities	Youth Worker to liaise with Church leadership regarding Risk Schedule & Plan		
Timing	To be implemented immediately		
Reporting & monitoring required	<p>Monitored weekly by Youth Worker</p> <p>Youth Worker provide written report to Church leadership each month &amp; a verbal report quarterly</p>		
Person responsible	Youth Worker	Date	1/7/12
Reviewer	Minister-in-Charge	Date	1/12/12

**NOTES**

<sup>1</sup> Extract from BSBCMN416A – Identify risk and apply risk management processes, Business Services Training Package, IBSA, 2006, sourced from Australasian Risk Management Unit, Monash University, 2003, **How to slash your insurance claims: the essential steps to identifying and managing risk**, Our Community Pty Ltd. [www.ourcommunity.com.au](http://www.ourcommunity.com.au)

<sup>2</sup> Adapted from BSBCMN416A – **Identify risk and apply risk management processes**, Business Services Training Package, IBSA, 2006.

<sup>3</sup> Extract from BSBCMN416A – **Identify risk and apply risk management processes**, Business Services Training Package, IBSA, 2006, sources from Volunteering Australia, 2003, **Running the Risk?**, [http://www.volunteeringaustralia.org/publications/risk\\_man.html](http://www.volunteeringaustralia.org/publications/risk_man.html)