# PRO-QR 02/02 RISK MANAGEMENT PROCEDURE

## Related Policies

Policy 12: Risk Management Policy

## Scope

This document outlines the Risk Management process for Wesley. This process encompasses all aspects of Risk Management including strategic, business, operational, project and emerging risks of Wesley. This process is consistent with the International Risk Management Standard ISO31000 and is supported by Wesley's risk management Policy, Framework, Plans, Software System and Training.

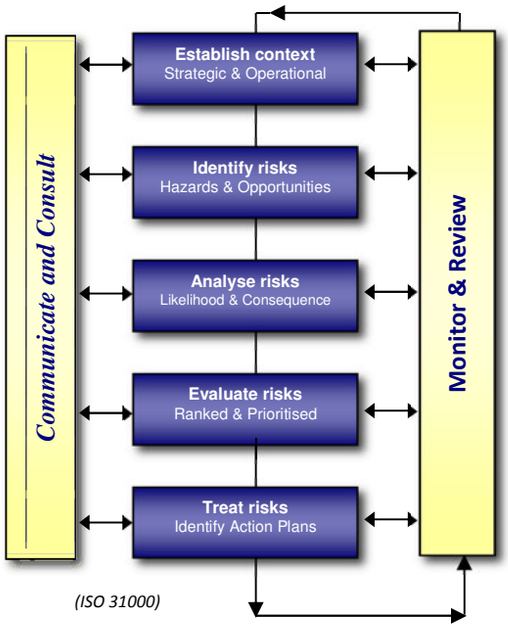
## Definitions and Abbreviation

| | |
|---|---|
| **Risk** | Effect of uncertainty on objectives. |
| **Risk Management** | Co-ordinated activities to direct and control an organisation with regard to risk. |
| **Enterprise-wide Risk Management or ERM** | Also known as organisation-wide or integrated risk management. An integrated approach to assessing and addressing all risks that threaten achievement of the organisation's strategic objectives. The purpose of ERM is to understand, prioritise, and develop action plans to maximise benefits and mitigate top risks. |
| **Risk Management Framework** | Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout Wesley. |
| **Risk Management Policy** | Overall intentions and direction of an organisation related to risk management. |
| **Risk Management Plan** | Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. |
| **Risk Management Process** | Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk. |
| **Inherent Risk** (also known as Absolute) | Risk with no controls in place. That is, the controls are absent or have failed. |

| | |
|---|---|
| **Managed Risk** | Risk as it is currently managed with Existing Controls in place. |
| **Acceptable Risk** (also known as Residual) | Perceived risk remaining after Proposed Controls or risk treatment controls have been implemented. |
| **Risk Register Owner** | Although the central repository for risks (Risk Register) is owned by the Risk Officer, there are several smaller sub-risk registers such as Safety Register (owned by the Occupational Health and Wellbeing Manager) and the Facilities Register (owned by the Facilities Manager) for that function. |
| **Risk Owner** | A position or entity with the accountability and authority to manage a control or associated risk treatments. |
| **Risk Champion** | This person will co-ordinate and facilitate the management of risk with their Manager for their department or program. |
| **Consequence (Most Reasonable)** | Outcome or impact of an event and may be expressed qualitatively or quantitatively. There can be more than one consequence from one event. Consequences can be positive and negative. Consequences are considered in relation to the achievement of objectives.<br>All consequences for the risk should be recorded. However when rating the risk the most reasonable consequence to occur should be used. |
| **Controls** | |
| **Existing Control** | An existing process, policy, device, practice or other action that acts to minimise negative outcomes and/or enhance positive opportunities. |
| **Key Control** | Control(s) that are essential to the effective management of the risk. Controls include any policy, process, device, practice or other actions designed to modify risk. |
| **Supplementary Control** | Control(s) that when added to key controls strengthen the overall management of the risk. |
| **Fully Applied Control** | The control or treatment is in place and applied at all times, and all requirements are being met. |
| **Partially Applied Control** | The control is in place however is not applied at all times, and not all of the control requirements are being met or effective. |
| **Overall Control Effectiveness** | The term effective, when applied to all controls, addresses the question of whether or not the controls are operating as intended. A system of controls cannot be effective unless it is adequate. |
| **Probability** | The extent to which an event is likely to occur. |

**The Risk Management Process Overview**

The process for managing Wesley business risk is consistent with the International Risk Management Standard ISO31000. It involves five key steps and also includes feedback through a monitoring and review process and appropriate communication and consultation throughout the whole process at all steps.



*(ISO 31000)*

**Procedural Steps**

**Step 1: Establish the Context**

The first step in a risk management process is to establish the context of the environment within which your service areas operate. The environment we operate is an extremely complex one and a number of factors will need to be considered when determining the parameters within which risks must be managed.

Therefore to manage risk effectively, consideration will be given to:

(1) Wesley's Strategic Plan 2012-2015.

(2) Financial, operational, competitive, political, social, client, cultural and legal environment within which the services operate.

(3) Objectives of your service areas' business plans.

(4) Balance between potential benefits, opportunities and cost.

(5) Relationship between risk management activities and other projects.

(6) Measures and targets.

Wesley has identified five contextual elements in relation to risk management:
1. Strategic Risk,
2. Business Risk,
3. Operational Risk ,
4. Project Risk and
5. Emerging Risk

Emerging Risks will be considered by Executive Management Team as appropriate.

Overall responsibilities are noted in the diagram below:

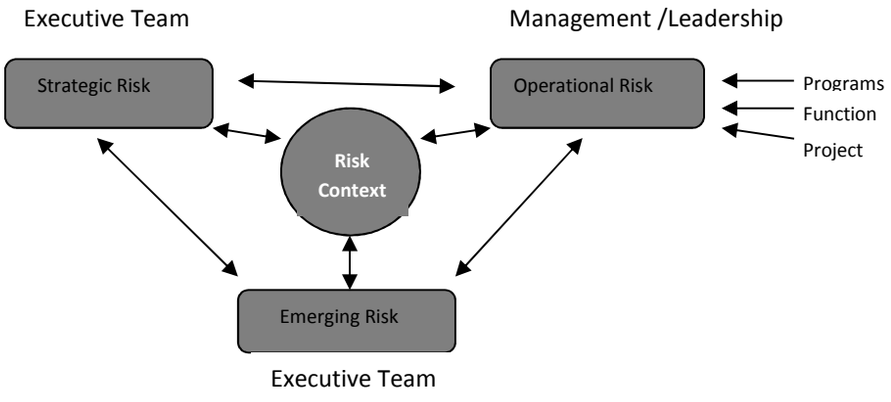



Diagram 2: Overall Responsibilities

**Step 2: Identify Risks**

The next step in the process is to carry out a risk identification review and document the risk to be managed. Where risks have previously been identified, this step will serve to confirm the completeness of these risks: having regard to changes in the business or operating environment. Identification will include all risks that impact the achievement of Wesley objectives, whether or not they are under the control of Wesley.

### Risk Identification Methods

There are many methods of identifying risk, including Safe Work Method Statements, Incident and Hazard Reporting, root cause analysis, facilitated brainstorming, interviews, checklists, questionnaires, workshops, historical loss, scenario and system analysis.

It is important to identify and generate a comprehensive list of events that might affect the achievement of Wesley objectives and services. Comprehensive identification of risks is important because a potential risk not identified at this stage will not be included in further analysis and potentially miss a significant opportunity or exposure. At this stage it is important we identify whether the risk is service and or program specific. Where a risk has implications for another service area, or Wesley as a whole, the risk should be noted to the Risk Officer and or General Manager of your service area for review.

Each business service area will be required to assess itself, at least quarterly, against the relevant risk context areas to ensure that risks are being identified at all times.

In line with ISO 31000 and industry practice, nine generic types of risk have been determined by the Executive Team, namely:

1. Financial
2. Market and Political, Reputation and Image
3. Governance, Compliance and Legal Relationships
4. Service and Clinical Care
5. People and Culture
6. OH&S
7. Infrastructure and Assets
8. Technology and Information Systems
9. Business Interruption

*See Appendix 4 - Risk Management Consequence Criteria for further explanation.

**Step 3: Analyse or Assess Risk**

Once all risks have been identified they will be analysed in terms of the possible magnitude (*consequence*) of the risk event and how likely the risk event is to occur (*likelihood*). Risks will be measured against an established criteria for most reasonable consequence and likelihood by referring to the Wesley Risk Matrix.

See Appendix 4 - for Risk Assessment Tools (Consequence Table, Likelihood Table, Risk Matrix).

**Risk Analysis Process**

(1) First, on a scale of 1 (insignificant) to 5 (catastrophic), rate the consequence of the risk - What will be the result if the risk eventuates?

(2) Then, also on a scale of 1 (rare) to 5 (extremely likely) assess the likelihood rating - How likely is it that the event will occur or with what frequency?

(3) Lastly, the overall level of risk is determined by combining the consequence rating and the likelihood rating to providing a rating for the Risk.

(4) All risks analysed as a 'High' or an 'Extreme' risk must be discussed with the relevant General Manager.

(5) Confirmed 'Extreme' risks will be added to the risk registers by the relevant General Manager.

When determining the "Absolute or Inherent Risk Rating", the maximum foreseeable consequence or potential exposure may be the base for determining the consequence component.

But when determining the "Managed Risk Rating" or "Residual Risk Rating" the most reasonable consequence to occur is used to determine the consequence component.

Analysis may be qualitative or quantitative or even a combination of both depending on circumstances. This part of the process assists to rate the risk from highest to lowest perceived exposure to services and operations of Wesley.

**Assessment of Mitigating Practices/Controls**

In assessing the consequence and likelihood of risks it is also necessary to consider mitigating activities or management processes that reduce the level of risk. These mitigating effects, processes or key controls are identified, documented and assessed based on Wesley's established criteria below.

The aim of the risk evaluation process is to arrive at a prioritised list of residual risks that can be flagged for treatment

The types of control activities within Wesley will normally include:

- High level review (by the Risk and Control Owners);
- Activity controls (including OHS hierarchy of controls);
- Physical controls;
- Various regulatory / compliance controls;
- Systems of approvals and authorisations;
- Verifications and reconciliations; and
- Segregation of duties.

Mitigating practices / control elements for consideration in assessing controls include (amongst other things) those in the diagram below:

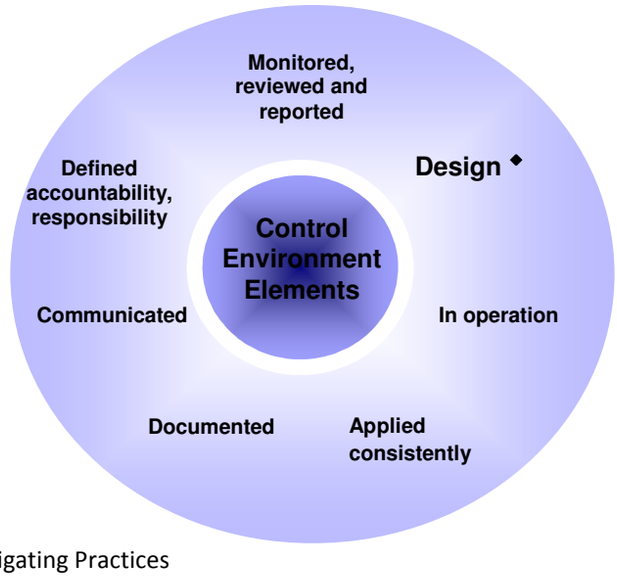



Diagram 3: Mitigating Practices

Note: If the design of existing controls is not effective in mitigating the risk, other elements (documentation of the control, monitoring and review etc) will also be ineffective in mitigating the risk.

After evaluating the risk and control measures in place, the risk is rated using Wesley's Risk Matrix (see Appendix 4) and is referred to as the **Managed Risk Rating**.

| Risk Rating | Management Level |
|---|---|
| Extreme | General Manager (executive) decision required.<br>Risk Owner responsibility to determine treatment actions for presentation to General Manager |
| High | General Manager (executive) decision required<br>Risk Owner responsibility to determine treatment actions for presentation to General Manager |
| Medium | MLT decision required<br>Risk Owner responsibility to determine treatment actions for presentation to General Manager |
| Low | Program Co-ordinator decision required.<br>Risk Owner responsibility to determine treatment actions for presentation to MLT Manager |

**Step 4: Evaluate Risk**

The risk owner will need to decide whether the Managed Risk Rating is tolerable or not.

Risk may be tolerated if:

(1) The level of risk is so low that specific treatment is not appropriate within available resources.

(2) The risk is such that there is no treatment available. For example, the risk that a project might be terminated following a change of government is not within the control of an organisation.

(3) The cost of treatment, including insurance costs, is so manifestly excessive compared to the benefit, that acceptance is the only option. This applies particularly to lower ranked risks.

(4) The opportunities presented outweigh the threats to such a degree that the risk is justified.

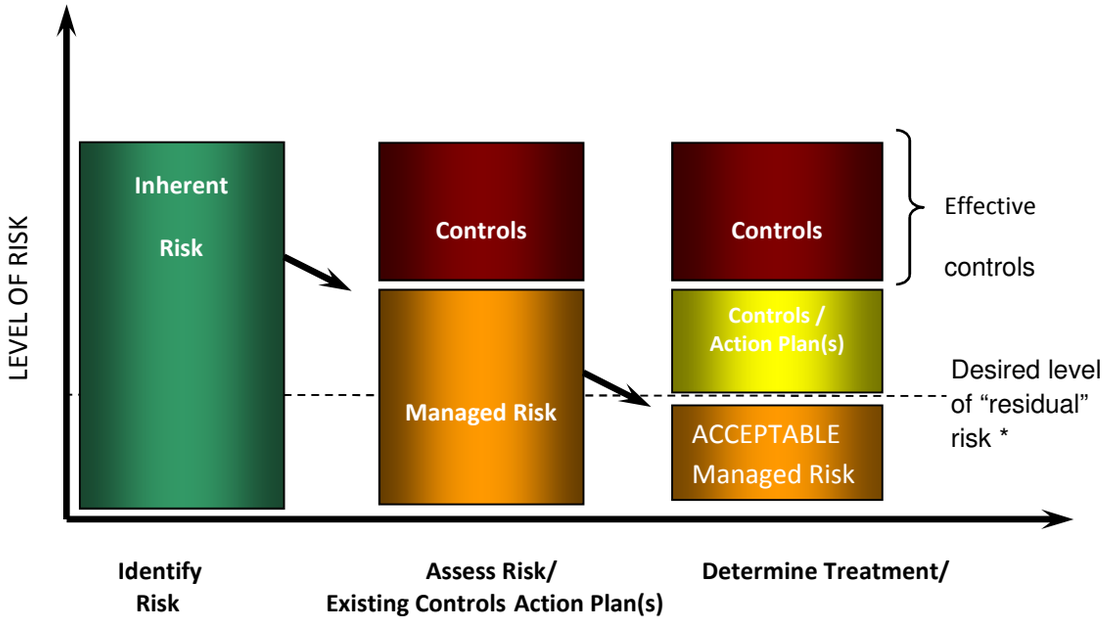
**Step 5: Treat Risk**

**Risk, Mitigating Practices / Control and Treatment Process Summary – "Bridging The Gap"**

As shown in the diagram below, evaluation of the effectiveness of existing mitigating practices / controls / processes reduces the level of risk, but may not be

sufficient to achieve an acceptable level of risk. This is where action plans to improve controls are required.

Diagram 4: Risk being managed by existing and proposed controls




* Acceptable or at a level which cannot be removed / cost effectively controlled

### *Risk Tolerance*

For **Extreme and High managed risk levels**, General Manager (Executive) decision is required to determine if the risk is acceptable within the current business practices and consider significant additional controls. Therefore it is necessary for the Risk Owner to identify options to treat these risks, evaluated options, develop and document a treatment plan for approval by the Responsible General Manager for immediate implementation.

It is unlikely that risks will ever be entirely eliminated, but by demonstrating that actions are being implemented, the risks may be reduced to a more acceptable level.

For "**medium**" managed risks, decisions will be required by the Leadership Group to determine if the risk is acceptable and will consider significant additional controls. It will be necessary for the Risk Owner to identify options to treat these risks, evaluate options, develop and document a treatment action plan for approval by the responsible General Manager for immediate implementation.

For "**low**" managed risks, Program Co-ordinator decision will be required to determine if the risk is acceptable and will consider significant additional controls. It will be necessary for the Risk Owner to identify options to treat these risks, evaluate options, develop and document a treatment action plan for approval by the responsible Leadership Group manager for immediate implementation.

A number of risk management treatment strategies have been noted in Appendix 7 of this Procedure.

If a proposed control is not implemented, it should be documented why the Proposed Control was rejected.

**Risk management treatment strategies include:**

***Avoiding the risk*** – by deciding where practicable, not to proceed with the activity likely to generate risk.

***Mitigating and/or reducing the risk***

- Take action to reduce the likelihood of the event by:

  Audit programs; inspection processes and controls; preventative maintenance; implementing policies and procedures; structured training; technical/engineering controls; design features; quality improvement; management and standards; contract conditions; project management; supervision; testing.

- Take action to reduce the consequences by:

  Contingency planning; design features; engineering and structural barriers; contractual arrangements; disaster recovery plans; public relations.

***Sharing the risk*** – involve another party bearing or sharing some part of the risk. Mechanisms include the use of contracts, insurance arrangements and organisational structures, such as partnerships and joint ventures.

***Accepting the risk*** – after risks have been reduced or transferred, there may be residual risks, which are retained. Plans should be put in place to manage the consequences of these risks if they should occur.

Selecting the most appropriate risk treatment option should be made by considering the following issues:

- The cost of managing risks must be balanced against the benefits obtained;

- The extent of risk reduction gained;
- The extent to which there is an ethical or legal duty to implement a risk treatment option which may override any cost/benefit analysis; and
- How sensitive is the risk to Wesley's image and reputation and its perception by stakeholders and external parties. This may warrant implementing costly actions.

### Risk Treatment Strategies

Potential risk treatment strategies include avoidance, retention, reduction and transfer. Appendix 2 outlines each strategy with examples:

Multiple treatment options can be used to manage a critical risk. For example, fire in a client service premises is managed through the following risk treatment strategies:

- Reduction (fire alarms, automatic sprinklers, fire extinguishers, evacuation plan and drill)
- Transfer (insurance); and
- Retain (business continuity and emergency planning).

*See Appendix 7 for Risk Management Treatment Strategies

**Step 6: Monitor and Review Risk**

Risk Management is a dynamic process and it will be necessary to incorporate monitoring and review of processes and activities into day to day operational management activities in order to capture any new or emerging risk or opportunities arising from changing business circumstances. Additionally a review of the risk treatment options chosen will be necessary to ensure the options are achieving the desired outcomes. Likelihood or consequences may change, service advancements or legislation/policy changing the exposure. The questions that will be asked are:

(1) Has the risk been reduced? If not, why not?

(2) Are there other measures that could be implemented?

(3) Some risks, depending on the level of overall risk, may require very regular review. This will be determined in the development of the quality improvement plan.

As a general guide:

- A low or moderate risks and their associated controls will require six monthly review to ensure the likelihood or consequences has not altered;
- High risks and associated controls will be reviewed quarterly depending on the likelihood rating;

- An extreme risk may and associated controls will be reviewed monthly or more often, if the likelihood of occurrence is very high; and
- All existing and emerging risks will be reviewed at least annually.

The review of controls is more aligned to the control that is in place and active, that no one has changed or removed a control as this would have an impact on the overall control effectiveness and the risk rating. For example, administrative controls such as policies and procedures have their own timeframe for review, the control review might be the procedure is still in place and active and is there anything that may impact on the Procedure requiring review of the Procedure in more detail.

**Communicate and Consult**

Communication and consultation are important elements during each step of the risk management process. Effective communication is essential to ensure that those responsible for implementing risk management and those with a vested interest, understand the basis on which risk management decisions are made and why particular actions are required.

When appropriate, external and internal stakeholders should be engaged throughout the risk management process, which supports buy-in and identification of issues that may not have been raised.

It is important that a communication approach recognises the need to promote risk management concepts across all elements of the business including Management to staff, volunteers and clients.

Consultation includes characteristics such as:

- Being a process not an outcome;
- The impact on a decision through influence rather than power; and
- Not necessarily joint decision making, but inputs into the decision making.

**Risk Documentation**

Risk documentation involves a structured process to record information such as risks that have been identified, assessment of these risk and related controls, selection of treatment options and plans to manage the risks. Appropriate documentation needs to occur throughout the risk management cycle. Wesley utilises RiskMan software as a central repository of information relating to identified risks.

## Variations to Procedure

### Service Specific Variations

## Related Documents

| Related Forms, Guidelines, other documentation |
|---|
| Risk Management Framework PR-QR-02/01<br>Risk Management Policy Policy No 12<br>Health and Safety Policy Policy No 1<br>Health and Safety Action Plan<br>Quality Framework CG DOC 01 |
| **Related Local Procedures** |
| OHS Management in the Workplace PR DC22/03<br><br>OHS Risk Assessments |

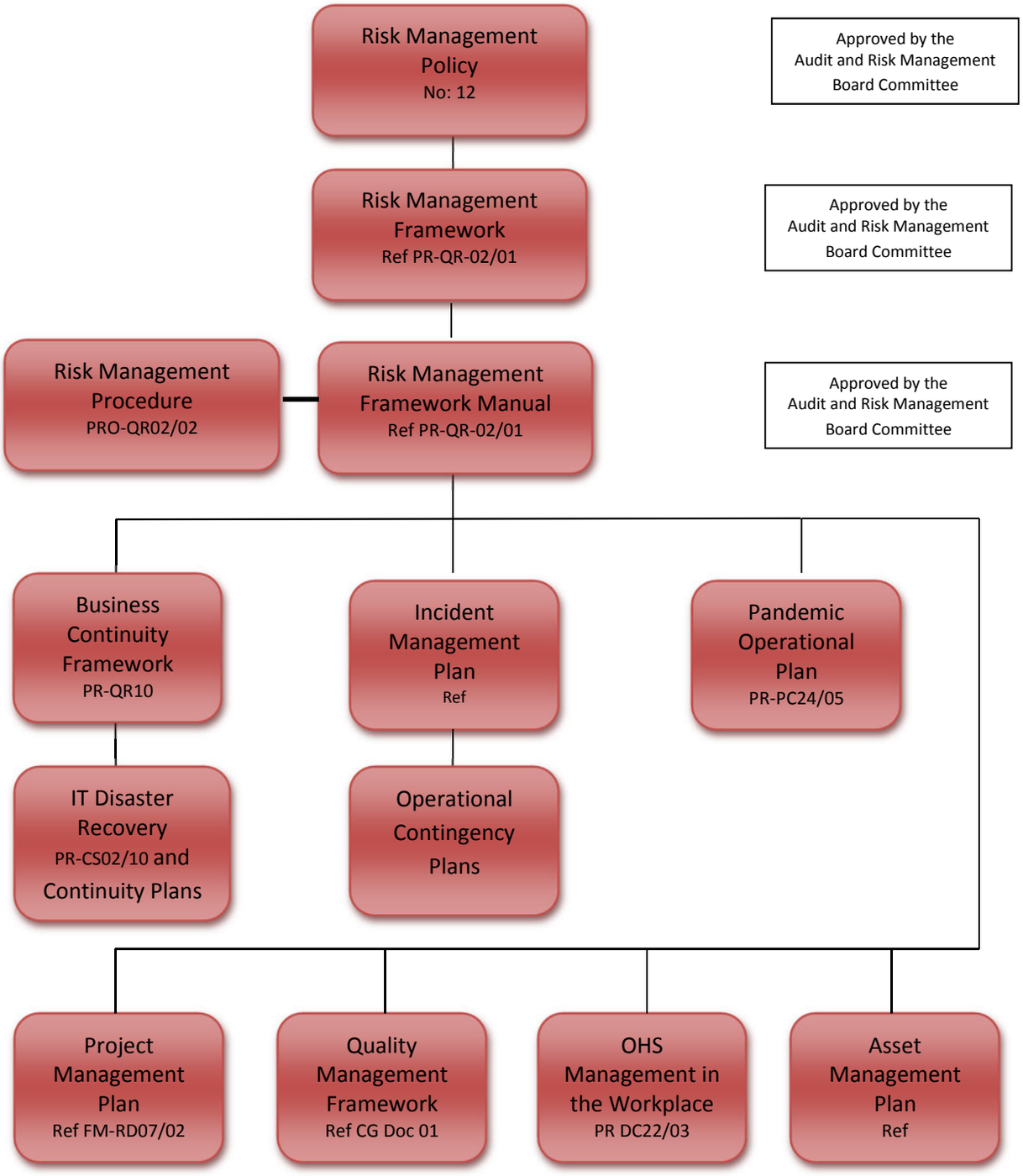
## External Context

| Relevant Standards |
|---|
| ISO 31000 International Risk Management Standard<br>HB266 Guide for managing risk in not-for-profit organisations |
| **Relevant Legislation / Regulations** |
| |

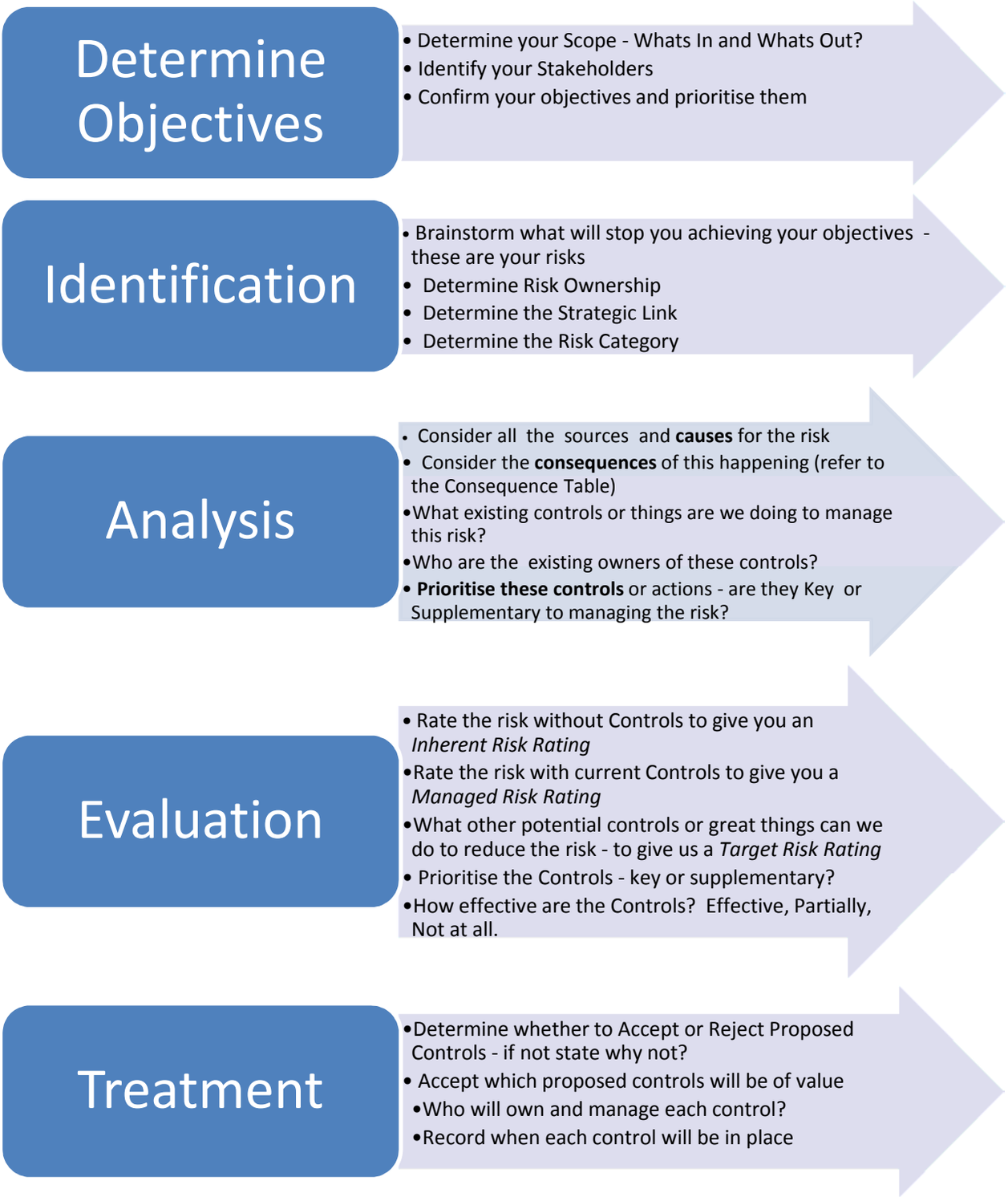
***Revision Record***

| *Version* | *Date* | *Document Writer* | *Revision Description* |
|---|---|---|---|
| *1* | *19/8/2014* | *Sue Templeman* | *Document written* |
| | | | |
| | | | |

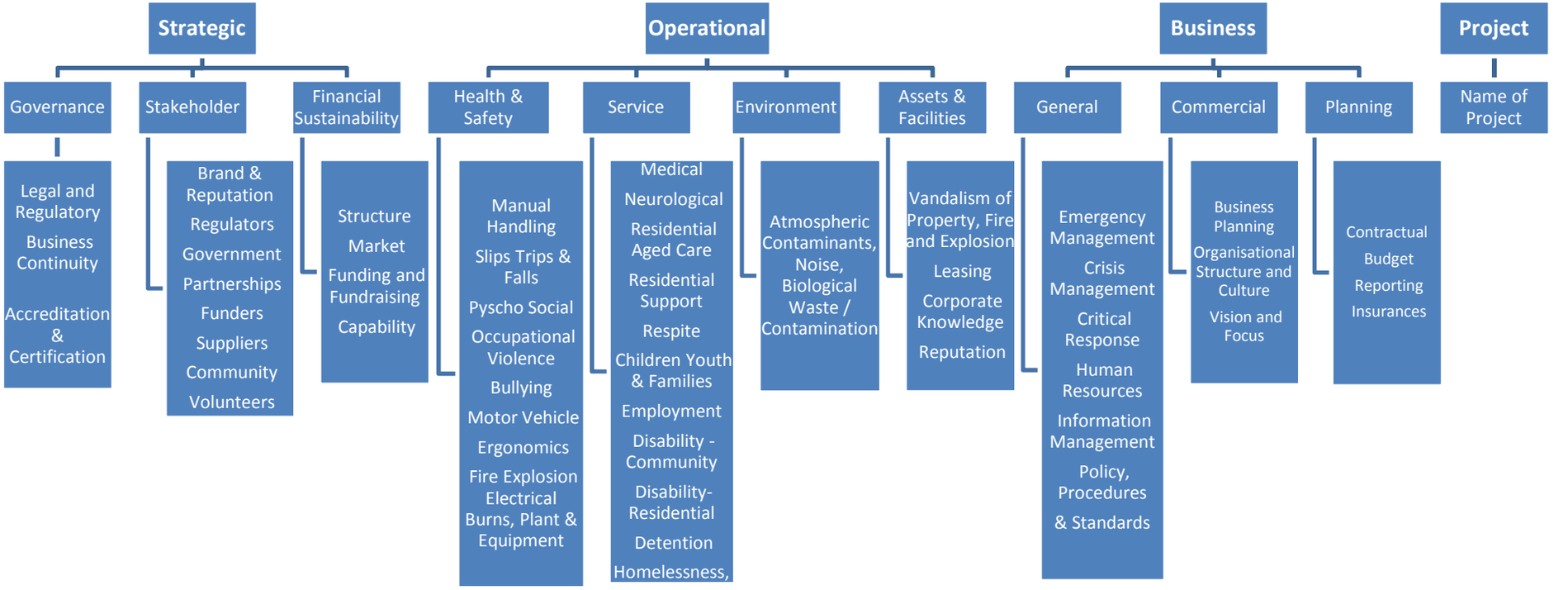
## *Appendix 1: Risk Management Process*



## *Appendix 2: Risk Management Process*



## *Appendix 3: Categories of Risk*



## *Appendix 4: RISK ANALYSIS TOOLS*

### (A) Consequence Criteria

| Rating | Financial | Market & Political (Reputation & Image) | Governance/ Compliance | Service/Clinical Care Outputs | People and Culture | OH&S | Business Interruption | Infrastructure and Assets | Technology & Information Systems |
|---|---|---|---|---|---|---|---|---|---|
| **5. Catastrophic Outstanding (Positive)** | Single incident of >$2,000,000 loss or gain | Reputation of the Service severely affected<br>Organisation may close or be split up<br>Significant loss of funding for several years<br>Long term loss of clients<br>National media coverage, attracts substantial new funds | Major litigation costing >$3m<br>Investigation by regulatory body resulting in long term interruption of operations<br>Possibility of custodial sentence | Total Cessation of multiple services for many months<br>Loss of Funding in one or more areas creating a significant budget deficit.<br>Positive transformation of business | State wide reliance on contracted staff or over stretching existing resources – 20% of workforce. | Fatality, and/or severe irreversible disability to one or more people<br>Major failure of plant and or systems.<br>Significant fines resulting in adverse media coverage and damage to brand | Critical service loss for more than one month | Total loss of or inability to operate plant/equipment resulting in inability to deliver one or more services | Long-term outages for more than 1 week resulting in closure of several services |
| **4. Major** | Single incident $1,000,000 - $2,000,000 loss or gain | Substantial embarrassment for the service, including adverse loss of confidence in service<br>CEO departs<br>Funding affected and/or loss of clients for many months<br>Attracts a moderate level of new funds | Major breach of regulation with punitive fine<br>Significant litigation involving many weeks of senior management time and up to $3m legal costs | Disruption of multiple services for several months<br>Distinctive enhancement or change of organisation | Substantial services operating with contracted staff or over stretched resources | Extensive injuries requiring admittance to hospital or impairment to one or more persons<br>Inability to maintain safe systems of work | Critical service loss for up to one month | Loss of systems that provide the tracking and monitoring of plant and assets (needs to be implemented) resulting in exposure to fraud, mismanagement | Critical outage lasting 3 to 5 days, disaster recovery plan activated |
| **3. Moderate** | Single incident $200,000 - $999,999 loss or gain | Noticeable loss of clients and/or funding for several months<br>Stakeholders and/or community concern generates interest from potential funders, major local media coverage<br>Senior manager departs, vacancy for several months | Breach of regulation with investigation by authority and possible moderate fine<br>Litigation and legal costs up to $999k | Total cessation of one service for a few months/multiple services for several weeks and subsequent disruption<br>Major improvement in scope of organisation | Local service placing reliance on contracted staff or over stretching resources | Short term disability to one or more persons<br>Medical treatment required, to one or more persons<br>Breach of OHS Act resulting in exposure of risk. | Critical service loss not back in 2 weeks | Inability to service infrastructure and assets due to budgets constraints | Outage of 1 to 3 days with workarounds available |
| **2. Minor** | Single incident $20,000- $200,000 loss or gain | Local media coverage<br>Issue raised by stakeholders<br>Complaint to management | Breach of regulations<br>Minor fine or legal costs<br>Minor litigation | Some service disruption in one area<br>Sizeable improvement in services | Skill shortages in certain areas. Some difficulties in recruitment | Significant medical treatment, lost injury time <2 weeks<br>Workcover claim – minor | Local only, service loss for minimum period | Inability to operate from a location for a minimum period. Breakdown in procurement and supplier disruptions | Outage of less than a day with workarounds available |
| **1. Insignificant** | Single incident $0 - $20,000 loss or gain | No media coverage<br>Complaint to employee | Minor legal issues or<br>Breach of regulations | Minimal disruption or enhancement | Some vacancies – filled by agency | First Aid or minor medical treatment required<br>Risks and Incidents managed and resolved appropriately | Negligible impact, brief loss of service | Infrastructure restored in a timely manner, minimal loss of time and disruption to plant, equipment, service or goods | Outage to non-critical system of less than 2 hours |

**Table A: Consequences ratings used and associated attributes**

*The Shaded sections indicate the stated risk appetite of the Board of WMM, where risks exceed this level they will be immediately escalated to the Board, to make a decision on continuation of service or additional controls

## (B) Likelihood Criteria

| Rating | Expression | Frequency | Attribute |
|---|---|---|---|
| 5 | **Extremely Likely** | Regularly or daily | The incident or event will most probably occur under most circumstances |
| 4 | **Likely** | More than once per year | The incident or event will probably occur under most circumstances |
| 3 | **Possible** | Once every year | The incident or event may occur under certain circumstances |
| 2 | **Unlikely** | Once in every 3 years | The incident or event is unlikely to occur |
| 1 | **Rare** | Once in every 10 years | The incident or event will only occur under the most exceptional circumstances |

**Table B: Likelihood ratings used and associated attributes**

**Risk Analysis Grid**

| Likelihood | Insignificant (1) | Minor (2) | Moderate (3) | Major (4) | Catastrophic (5) |
|---|---|---|---|---|---|
| Extremely Likely (5) | Medium (5) | Medium (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) | Medium (10) |
| Rare (1) | Low (1) | Low (2) | Low (3) | Low (4) | Medium (5) |

Consequence

**Extreme risk** – Must complete control evaluation. Executive & Board review.

**High risk** – Must complete control evaluation. Management & Executive review (Report to Audit & Risk Management Committee)

**Medium risk** – Management responsibility must be defined. Control evaluation where appropriate.

**Low risk** – Monitor. Examination of controls is not specifically required

**Table C: Overall Risk Rating**

## *Appendix 5: Risk Assessment Form*

A pro-forma of a Risk Assessment is provided below. The Risk Assessment should be tailored for specific operational use as appropriate.

**Risk Assessment Form**

**Name of Project:**
**Risk Assessor:**
**Attendees:**
**Date:**

| | |
|---|---|
| **Context:** | **Risk Name:** … |
| **Stakeholders:** | |
| **Focus Area Objective:** | |
| **Risk Category:** | |
| **Sub Risk Category:** | |
| **Risk Description:** | |
| **Risk Ownership:** | |
| **Contributing Factors (Causes):** | |
| **Consequences:** | |

| **Risk** | **Inherent Risk Rating (without mitigating controls or proposed controls)** | | | **Existing Controls** | **Managed risk rating** | | | **Control Effectiveness** |
|---|---|---|---|---|---|---|---|---|
| | Likelihood | Consequence | Risk Rating | | Likelihood | Consequence | Risk Rating | |
| **1.** | 3 | 3 | M | | 3 | 3 | M | Satisfactory |
| **2.** | 3 | 4 | L | | 3 | 4 | L | Unsatisfactory |
| **3.** | 3 | 3 | M | | 3 | 3 | M | Satisfactory |
| **4.** | 2 | 3 | H | | 3 | 4 | M | Highly Effective |
| | | | | | Overall Control Effectiveness | | | Satisfactory |

## *Appendix 6: Mitigating Plan*

A pro-forma of the mitigating plan is provided below. The mitigating plan should be tailored for specific operational use as appropriate

| **Proposed Controls**<br>**Name of Risk/Project:**<br>**Responsible Owner:**<br>**Group and Department/Program:**<br>**Completed By:**<br>**Date:**<br>**Approved by:** | |
|---|---|
| **Risk Category:** | |
| **Risk Description:** | |
| **Contributing Factors:** | |
| **Assessed Target (residual) risk rating:** | |

| **Proposed Control Options:**<br>**a.**<br>**b.**<br>**c.**<br>**d.** | **Accept or Reject**<br>**a.**<br>**b.**<br>**c.**<br>**d.** |
|---|---|
| **Selected Treatment Action(s)** [from those noted above]:<br>**1.**<br>**2.**<br>**3.**<br>**4.** | |
| **Rationale for recommended treatments:** | |
| **Resource Requirements:**<br>**1.**<br>**2.**<br>**3.** | **Estimated Costs $** |
| **Total Cost** | |
| **Pay-back period (or other appropriate measure)** | |

| **Responsibilities:** | **Timing:** |
|---|---|
| **Ongoing reporting and monitoring required:** | |

# *Appendix 7: Risk Treatment Strategies*

## *Avoid*

| Strategy | Example(s) |
|---|---|
| Divest | Sell, liquidate or spin off assets |
| Prohibit | Certain transactions, high risk activities, asset exposure etc |
| Stop | Specific activities and redirect resources |
| Screen | Alternative investments and low return / high risk capital projects |
| Eliminate | Through internal, pervasive and if necessary, organisational-wide controls |

## *Retain*

| Strategy | Example(s) |
|---|---|
| Accept | At current level with no further management action required |
| Reprice | By including a premium for the risk |
| Self-insure | Internal charges, participation in industry initiative etc |
| Offset | Against others in a “pool” |
| Plan | For contingencies (and perform testing), where there is a high consequence but low likelihood |

## *Reduce*

| Strategy | Example(s) |
|---|---|
| Disperse | Through financial and physical means to reduce the effect of catastrophic events |
| Control | Using internal management processes (policies, directives, training etc) to control activities |

## *Transfer*

| Strategy | Example(s) |
|---|---|
| Insure | Through independent third parties |
| Reinsure | Reduction of portfolio exposure through reinsurance |
| Hedge | New loans, borrowing etc |
| Secure | Pricing mechanisms |
| Outsource | To specialists, more efficient organisations, economies of scale |
| Indemnify | Risk sharing agreements with independent organisations |

*Exploit (in relation to opportunity risks)*

| Strategy | Example(s) |
|---|---|
| Allocate | Capital to take advantage of the opportunity |
| Diversify | Assets and portfolio |
| Expand | Through investment and development of new areas |
| Create | New products and services |
| Redesign | Business model to create greater value (or reduce risk) |
| Reorganise | Re-engineer |
| Price | To attract customer to new services and products |
| Influence | Regulators, customers, public opinion etc |

## *Appendix 8: Risk Management Documentation Process*