



## Risk Management Policy

Manual: Organisational Management

Document ID: C.06

### Contents

|   |           |
|---|-----------|
| <b>POLICY REVIEW &amp; VERSION CONTROL .....</b>              | <b>1</b>  |
| <b>BACKGROUND .....</b>                                       | <b>2</b>  |
| PURPOSE .....   | 2         |
| SCOPE.....  | 2         |
| <b>RISK APPETITE STATEMENT .....</b>                          | <b>2</b>  |
| <b>ROLES &amp; RESPONSIBILITIES .....</b>                     | <b>3</b>  |
| <b>RISK APPETITE.....</b>                                     | <b>4</b>  |
| <b>RISK MANAGEMENT FRAMEWORK .....</b>                        | <b>4</b>  |
| <b>RISK GOVERNANCE.....</b>                                   | <b>7</b>  |
| <b>RISK MANAGEMENT STRATEGY .....</b>                         | <b>8</b>  |
| Risk Definitions & Concepts.....                              | 8         |
| Risk Methodology .....  | 9         |
| Communication and Consultation.....                           | 9         |
| Establishing the Context .....                                | 10        |
| Risk Identification .....                                     | 10        |
| Risk Analysis.....  | 11        |
| Risk Evaluation.....  | 12        |
| Risk Treatment.....   | 13        |
| Monitoring and Review .....                                   | 14        |
| <b>RISK MANAGEMENT REPORTING &amp; OVERSIGHT PROCESS.....</b> | <b>15</b> |
| Risk Register & Review Process .....                          | 15        |
| Risk Reporting & Oversight.....                               | 15        |

### POLICY REVIEW & VERSION CONTROL

The risk management policy will be reviewed every three years or when there has been a significant change to the strategic plan or business activity. Any changes to the policy will need to be endorsed at the Risk & Continuous Improvement Committee and approved by the Board.

| Version | Date Reviewed                                | Amendments   |
|---------|--|--|
| 1.0     | 16/12/2015                                   | Initial risk management policy   |
| 2.0     | 23/03/2021<br>Board Approved<br>(31/05/2021) | Revised risk management policy in line with new risk management framework and risk appetite positions. |

|     |            |   |
|-----|------------|---|
| 2.1 | 28/03/2022 | Minor amendments to risk appetite framework following Board Risk Workshop and review of corporate risk register |
|-----|------------|---|

## BACKGROUND

### PURPOSE

To outline Mercy Services (Mercy) approach in identifying, assessing, monitoring and mitigating risks across the organisation. This policy outlines the organisation's approach to risk management and the operational areas under its remit.

### SCOPE

This policy is set by the Board in driving its expected approach to risk management across the organisation, with management to then implement the policy across the business areas.

## RISK APPETITE STATEMENT

The risk appetite statement communicates the Board's expectations of how much risk the organisation is willing to accept. The Board has set risk tolerances for each of Mercy's key risk areas as identified under the Risk Management Framework. These positions are established in line with the risk appetite criteria defined within this policy.

### **Detailed Risk Appetite Statements for areas under the Risk Management Framework**

**Strategic** – A *moderate* risk appetite position is adopted as Mercy's strategic plan has outlined several projects to be completed which seek to innovate and invest in new infrastructure to assist in growth and delivery of improved and more efficient services to clients and residents.

**Governance** – A *low* risk appetite position is adopted as Mercy has implemented a narrow delegations framework amongst its senior management and its governance framework encompasses several committees and groups, which review the structures and processes in place across the organisation within a defined process for decision making.

**Clinical, Quality & Safety** – A *low* risk appetite position is adopted in line with Mercy caring for vulnerable aged people and its position to provide high quality care, with a focus on the wellbeing of clients and residents, under a strong clinical review process which examines incidents, quality issues or complaints to continuously improve towards best practice care.

**Operational** – A *moderate* risk appetite position is adopted as Mercy is in the process of upgrading its infrastructure, platforms and policies to assist the organisation's growth and focus on improving efficiency along with the experience of clients, residents and their families.

**Financial** – A *moderate* risk appetite position is adopted given the current government funding uncertainty around services and as Mercy is in the process of reassessing these funding arrangements in line with its strategic plan.

**Regulatory & Legal Compliance** – A *low* risk appetite position is adopted in line with Mercy ensuring it maintains compliance with its regulatory requirements and practice standards in delivering effective care and governance of its operations.

**Safeguarding** – A *minimal* risk appetite position is adopted as Mercy has zero tolerance for abuse or neglect, which has been communicated across the organisation. As Mercy engages with vulnerable people throughout its services it has strict on-boarding and safeguarding processes in place to ensure appropriate background checks are undertaken, with a strong focus on incident management for oversight and escalation of concerns or allegations around safeguarding.

## ROLES & RESPONSIBILITIES

### Board

The Board acknowledges that it sets the tone and expectations with regards to the organisation's approach to risk management. For this it has set an overall risk appetite (or statement) in line with the position adopted. The Board has the following responsibilities in terms of the risk management:

- Ensure an effective risk management framework (including risk appetite and risk tolerance) is established and embedded into the clinical and corporate governance processes of the organisation;
- Provide strategic oversight and monitoring of organisation's risk management activities and performance; and
- Seek information from the Chief Executive as necessary to satisfy itself that risks are being identified and mitigation strategies are in place and effective.

### CEO

The CEO is responsible for instilling a strong risk culture across the organisation as set by the Board. This is to ensure appropriate focus and resourcing is in place to deliver the organisation's risk management strategy across teams. In addition the CEO will:

- Champion risk management culture within their organisation that includes a focus on continuous improvement and identifying opportunities as well as risks;
- Ensure the Risk Management Plan is implemented and the Risk Register is current;
- Ensure appropriate resources are allocated to managing and monitoring risk and to implementing risk mitigation strategies identified through risk planning activities;
- Allocate accountability for managing individual risks at an appropriately senior level to ensure risk mitigation strategies are implemented;
- Communicate risk management requirements to management and staff; and
- Take appropriate action on risks reported or escalated.

### Management & Staff

It is the **responsibility of all staff and management to manage risk** as it arises during the course of their role. Management are responsible for monitoring and managing risks within their area and ensuring staff are aware of their responsibilities in identifying and escalating any risks to their manager.

Management in addition will:

- Promote risk management within their areas of responsibility, including communication of requirements to relevant staff;
- Be accountable for risks and mitigating controls within their area of responsibility and take appropriate action on risks reported or escalated; and
- Assist in reporting on updates to the organisation Risk Register, including changes to risk management strategies, current risk ratings and emerging risks.

## RISK APPETITE

Risk Appetite is the degree of risk an organisation is prepared to accept in the pursuit of its strategic objectives and operational activities. As outlined in the Risk Appetite Statement, Mercy’s Board has set risk appetite positions for each of the key risk areas under its Risk Management Framework, which are defined further in the next section.

Mercy has set criteria for determining its risk appetite levels, with the relevant risk position and approach outlined in the table below:

| <b>RATING</b>                     | <b>Minimal</b>                            | <b>Low</b>   | <b>Moderate</b>  | <b>High</b>   |
|-----------------------------------|---|--|--|---|
| <i>Risk Position</i>              | Limited to no tolerance for risk          | Cautious or conservative tolerance of risk             | Stable or balanced tolerance of risk                   | Open to risk in maximising outcomes                 |
| <i>Approach to managing risks</i> | Mitigate or avoid all risk where possible | Small acceptance of risk to deliver effective services | Cede to a degree of risk to provide effective services | Accept risk levels due to greater reward / benefits |

The Board reviews the risk appetite statement and the positions adopted for each of the various risk areas annually. This policy’s risk appetite ratings are reviewed as part of the overall policy revision process.

### *Summary of Current Risk Appetite Positions*

| <u>Risk Area</u>                         | <u>Risk Appetite Position</u> |
|--|-------------------------------|
| <b>Strategic</b>                         | Moderate                      |
| <b>Governance</b>                        | Low                           |
| <b>Clinical, Quality &amp; Safety</b>    | Low                           |
| <b>Operational</b>                       | Moderate                      |
| <b>Financial</b>                         | Moderate                      |
| <b>Regulatory &amp; Legal Compliance</b> | Low                           |
| <b>Safeguarding</b>                      | Minimal                       |

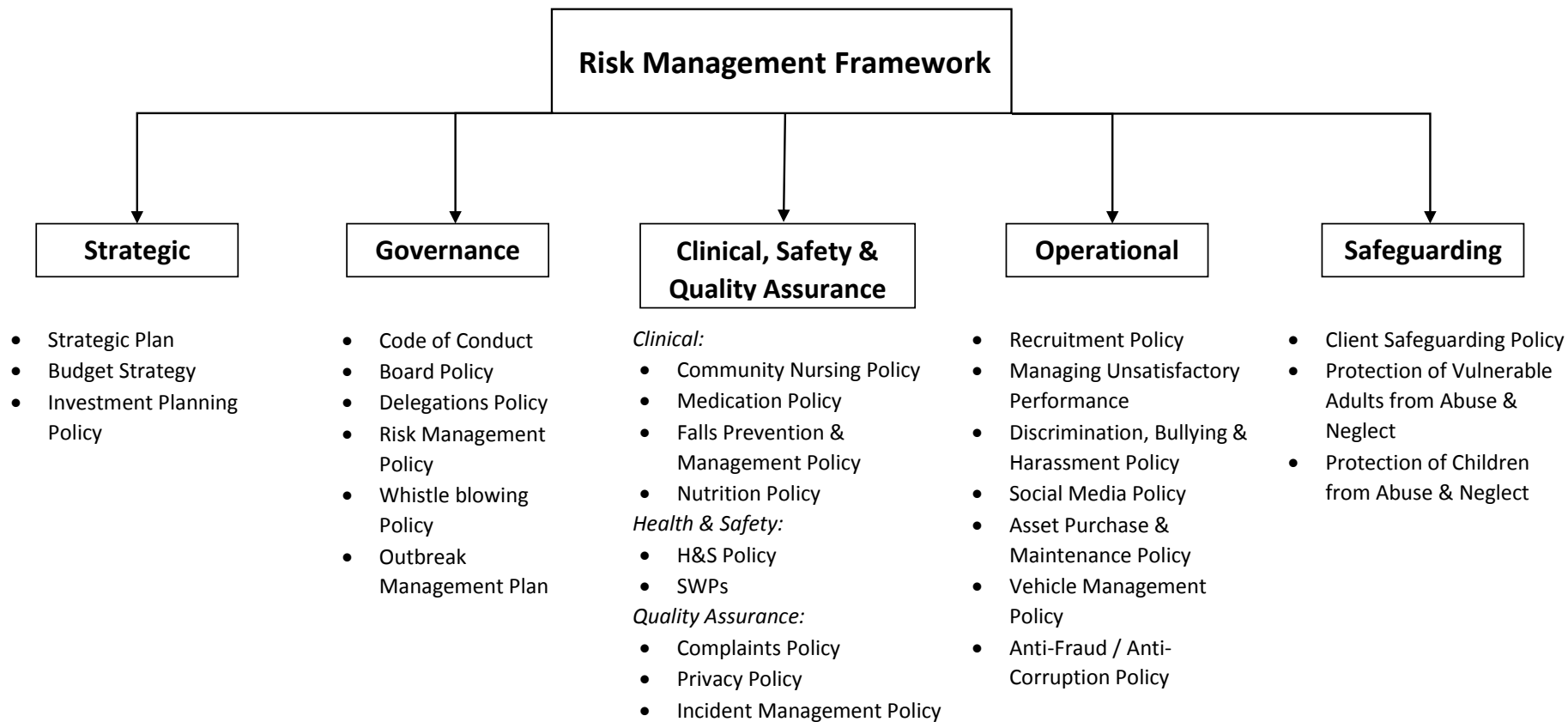
## RISK MANAGEMENT FRAMEWORK

A risk management framework (RMF) is the structured process used to identify potential threats to an organisation and to define the strategy for eliminating or minimising the impact of these risks, as well as the mechanisms to effectively monitor and evaluate the risk management strategy.

Mercy has identified the following key risk areas which form the basis for its risk management framework:

- **Strategic** – covering the failure to achieve the organisation’s overall objectives, including the risks associated with planning and the decisions made or modified over time as well as the effective use of financial resources;
- **Governance** – refers to the actions, structures, traditions and policies by which authority is exercised and decisions are taken and implemented;
- **Clinical, Safety & Quality Assurance** – relates to the quality and safety of health care services through identifying circumstances or opportunities that put clients or staff at risk of harm and reviewing practices for continuous improvement (includes Regulatory & Legal Compliance risks);
- **Operational** – incurred from inadequate or failed internal processes, people and systems or external events (includes Financial risks); and
- **Safeguarding** – being to protect the welfare and human rights of people that are connected with the organisation, particular those at risk of abuse, neglect or exploitation.

Mercy has developed a suite of policies and procedures to manage risks under each of these key risk areas. Policies that underpin the risk areas are outlined as per image 1 below.



**Image 1:** Mercy's Risk Management Framework

## RISK GOVERNANCE

To ensure effective oversight of Mercy’s risk management framework and implementation of this risk management policy, an organisational governance framework has been established as per image 2 below. The key governance bodies related to implementing the risk management framework are:

- **Mercy Services Board** – is engaged annually on Mercy’s risk appetite to ensure it remains within set tolerances and as per the strategic plan. The Board also reviews the corporate risk register annually to ensure key corporate risks are monitored and managed appropriately.
- **Risk & Continuous Improvement Committee (RCI)** – is responsible for addressing risk issues that arises from within Mercy’s operations. The committee comprises of management across Mercy’s service areas and includes clinical, operational, financial, HR, learning & development as well as quality staff expertise to assess the risks the organisation is exposed to. Risk registers of each functional area are reviewed quarterly, which the RCI reviews for any impact to the corporate risk register.
- **Finance & Investment Committee** – reviews financial investments, liquidity management and the financial budgeting process for the organisation.
- **Clinical Advisory Council** – the council is responsible for reviewing clinical risks and providing advice on clinical matters to continuously improve practices and maintain quality of care across services.
- **Health & Safety Committees (Residential & Other Services)** – Monitors potential risks regarding work, health and safety practices including SWPs.
- **Client Advisory Council** – comprises of clients across Mercy’s services who provide feedback and advice on any issues faced with their services, which can identify operational risks or provide avenues for continuous improvement.
- **Community Housing Advisory Committee** – oversees the health & safety, wellbeing, operational and code of behaviour aspects for those residents living within Mercy’s social housing facilities.

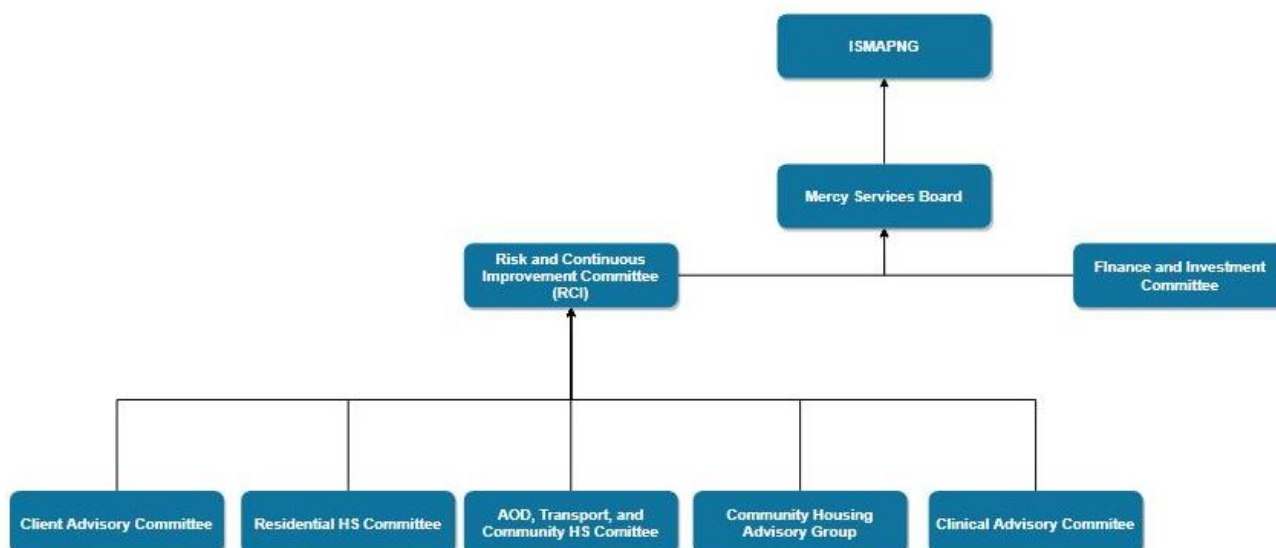


Image 2 – Mercy’s Organisational Governance Framework

## RISK MANAGEMENT STRATEGY

### Risk Definitions & Concepts

**Risk Appetite** – is the degree of risk an organisation is prepared to accept in the pursuit of its strategic objectives and operational activities. Risk appetite is expressed in the form of a high level qualitative statements that clearly capture the organisation's attitude to and level of acceptance of different risks. Where appropriate, the risk appetite statement may include quantitative measures.

**Risk Management Framework** – is the structured process used to identify potential threats to an organisation and to define the strategy for eliminating or minimising the impact of these risks, as well as the mechanisms to effectively monitor and evaluate the strategy.

**Risk Matrix** – used during risk assessment to define the level of risk by considering the category of likelihood against the category of consequence. Provides a simple mechanism to increase visibility of risks and assist management decision making.

**Risk Tolerance** – support the translation of the risk appetite by management into operational limits for the day-to-day management of material risks.

Concepts related to the risk register template:

**Risk Cause** – is an internal / external circumstance or event that results in that risk.

**Risk Controls** – a measure (including a process, policy, practice or other action) that modifies the risk in acting to minimise negative risks or enhance positive opportunities.

**Risk Description** – a structured statement of the risk identifying the key elements including the source, events and causes.

**Risk Impact** – potential effect of the risk occurring (amount of loss or gain sustained).

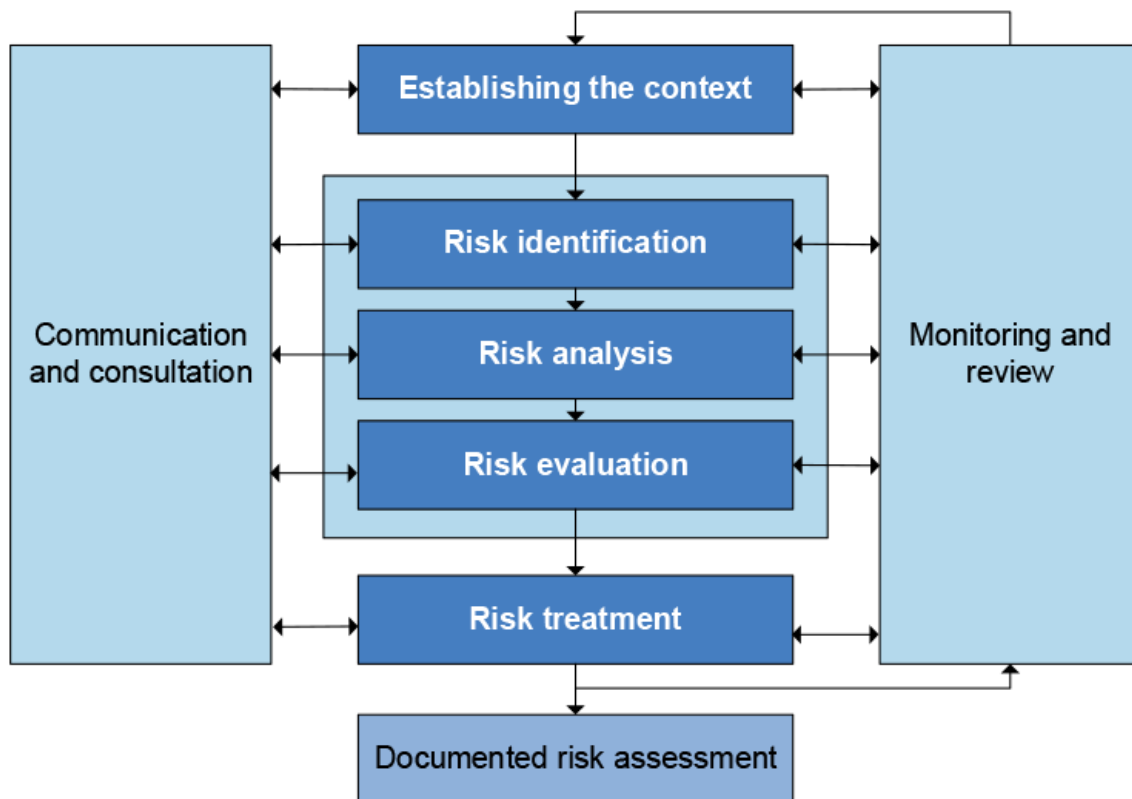
**Inherent Risk** – represent the amount of risk that exists in the absence of any controls or preventative measures.

**Residual Risk** – represents the amount of risk remaining following the implementation of the organisation's controls or preventative measures.



## Risk Methodology

Mercy adopts the international risk management standard ISO 31000:2017 in terms of its approach and methodology for managing risk. This is outlined in image 3 below.



**Image 3** – Extract from AS/NZS ISO 31000: Risk Management – Principles and guidelines

### Communication and Consultation

Ongoing communication throughout the risk process is critical to ensure an effective risk management framework. Staff need to be aware of the risks Mercy is exposed to, along with the process for managing risks and how to escalate risks that arise. Importantly, continual communication helps to reinforce the context in which risks are managed within Mercy and helps develop a strong risk culture.

Mercy implements its risk management framework through the Risk & Continuous Improvement Committee (RCI) which ensures a common understanding across management and service areas in applying its risk management strategies. The RCI also provides an avenue for consultation and discussion on risk registers and key risks that impact the organisation across services. This brings Mercy's expertise from each area together to assist in analysing and identifying risks.

Review of departmental risk registers are undertaken quarterly and reported to the RCI, providing an avenue to review risk reporting arrangements and processes across the organisation. Annually, the corporate risk register is presented to the Board for its oversight and review, which provides an opportunity to consult with the Board on risk ratings and management strategies. The development of risk profiles allows for the organisation to effectively assess its risk position to ensure it remains within Board target levels.

The following are key principles to be adopted in managing risk across the organisation:

- Involve relevant staff in decision making and assessment of risks;
- Ensure risk is considered and documented as part of decision making;
- Consult with those effected by the risk and ensure those affected are aware of why the decision was made; and
- Clearly communicating how risk is managed and controlled across the organisation.

## Establishing the Context

The context for Mercy’s risk management strategy incorporates the strategic, operational and regulatory setting in which it operates across its services. This considers both the internal and external environment contexts.

- *Strategic* – considers the organisational context operated in including reputational risk to develop a high level approach or strategy in supporting the organisation to manage its risks and achieve strategic goals;
- *Operational* – considers the types of services provided, how they are delivered and the capabilities to provide them. It includes the clinical management aspects in delivering safe services to clients and residents; and
- *Regulatory* – considers the regulatory compliance environment in which Mercy operates in, including the risk management practices to adopt in achieving quality assurance across operations.

In establishing the context, several questions may need to be considered including:

- The type of service provided
- The clinical need vs practical application
- What outcome is desired?
- Has there been previous issues in a similar context or experience?
- What are the societal (or client) expectations around delivery of the service?
- What are the financial implications vs dignity of risk?
- What external factors may impede achieving desired outcomes?
- Are there any consequences from a reputational aspect?

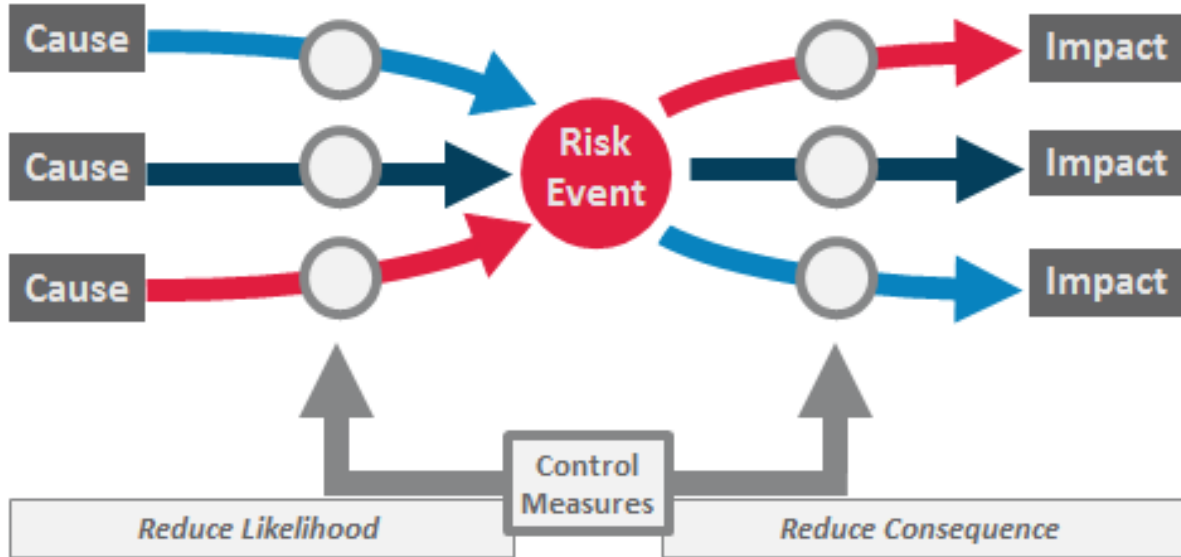
## Risk Identification

The process of identifying risks involves asking ‘what could happen?’ and ‘how could it happen?’ To assist in documenting this step, a risk register template (Appendix 1) has been created. This allows for risks to be identified and described, including the cause of the risk and the impact of the risk or areas affected. Avenues for identifying risks are summarised in the below table.

| <b><i>Risk identification source</i></b>                   | <b><i>Examples</i></b>  |
|--|---|
| <i>Structured or formal identification process</i>         | Department risk planning / register process<br>Risk workshops / risk profiling<br>Scenario or stress testing              |
| <i>Existing meeting structures</i>                         | Team meetings, Leadership meeting<br>Committees & councils (RCI, Clinical, Client or H&S)                                 |
| <i>Quality assurance review against standards or audit</i> | Self-assessments<br>Clinical quality reviews or audits<br>Accreditation reviews<br>Professional judgement and observation |
| <i>Incident or complaint</i>                               | Incident & complaint reporting process or review<br>Aged Care Quality & Safety Commission                                 |

|  |  |
|--|--|
|  | Feedback or independent investigation review   |
| <i>Industry body / Regulatory Bodies</i> | Case studies of current risks facing industry<br>Guidance or advice on key risks<br>Weekly newsletters on sector updates |

To identify a risk, potential causes of the risk need to be collated to define the risk event. Once a risk is identified the risk needs to be described concisely, setting out what the risk is, what it is affecting, and how it impacts on objectives. The description is important as it specifies the cause of the risk and enables the risk assessor to understand the impact the risk has on the organisation. A part of identifying the risk is determining the type of risk it falls under – as per the categories of risk outlined under the risk management framework. The process is represented by the image below.



**Image 4** – Risk identification process

### Risk Analysis

The process of analysing risks involves understanding the risks requiring action, and then ranking those risks through an assessment process, so that resources to treat risks can be allocated to those of greater priority. Risks are assessed by combining estimates of likelihood and consequences. The purpose of this process is to understand the nature of risk, and determine the level of risk prior to treatment (mitigation). The analysis can be qualitative, quantitative or a combination of both. This analysis allows for decisions to be made on risk based evidence, assigning resources to areas of greatest risk.

The likelihood of a risk occurring is measured in terms of its probability or frequency of occurrence over time. Whereas consequence is measured by the impact the risk results in. Both likelihood and consequence are assessed under a five level rating system. Mercy has categorised consequences by the severity types, with examples of how to assess the severity on a qualitative or quantitative basis dependent on the risk as outlined in the table below.

| Severity Risk Types                         | Severity Categories   |   |   |   |  |
|---|---|---|---|---|--|
|   | Insignificant   | Minor   | Moderate  | Major   | Significant  |
| Clinical Care & Client / Resident Wellbeing | No injury   | Superficial or minor injury where 1st aid is required   | Injury requiring hospitalisation  | Severe long term illness or injury suffered   | Permanent disability or death  |
| Safeguarding                                | No safeguarding issue present   | Breach of relationship boundary raised against a staff member                                     | Complaint or allegation of inappropriate behaviour made against a staff member                      | Concern raised of abuse made against a staff member   | Several allegations or cases of abuse raised against a staff member  |
| Financial                                   | Up to 1% of budget  | Up to 5% of budget  | Up to 15% of budget   | Up to 25% of budget   | Greater than 25% of budget   |
| Operational: Workforce                      | No workforce or staff shortage impacting service operations                               | Service disruption for a few hours up to a day due to workforce shortage or staff unavailability  | Service disruption or delay over a few days due workforce shortage or staff unavailability          | Ongoing disruption to a service for up to a week due workforce shortage or staff unavailability               | Inability to perform a service for a prolonged period (>week) due to workforce shortage or staff unavailability          |
| Operational: Facilities & Assets            | Minimal effect on services. No loss or damage to property, assets, records or information | Singular disruption to service. Minor loss or damage to property, assets, records and information | Temporary suspension of services due to loss or damage to property, assets, records and information | Prolonged service disruption or suspension due to loss or damage to property, assets, records and information | Cessation of services due to loss or damage to property, assets, records and information                                 |
| Regulatory & Legal                          | No regulatory or legal infringement   | Minor non-compliance with regulatory / legal requirement  | Breach of regulations or legal standards requiring notification and prompt rectification            | Multiple regulatory or legal breaches requiring mandatory reporting & potential regulatory action             | Systemic regulatory / legal breach requiring immediate reporting, resulting in possible fines or restriction on services |
| Governance                                  | No impact despite failure / lack of process & oversight                                   | Small impact to clients / business operations due to failure / lack of process & oversight        | Some ongoing impact to clients / business operations due to failure / lack of process & oversight   | Prolonged impact to clients / business operations due to failure / lack of process & oversight                | Systemic impact to clients / business operations due to failure / lack of process & oversight                            |
| Work Health & Safety                        | Injury, accident or illness not requiring medical treatment                               | Injury, accident or illness where 1st aid treatment is required                                   | Serious injury, accident or illness requiring hospitalisation                                       | Permanent disability or life threatening injury, accident or illness  | Death(s) or multiple life threatening injury, accident or illness  |
| Reputation & Image                          | No media attention or image impact  | Some complaints and minor damage to image. No media attention                                     | Some media exposure and complaints but not specifically focused on Mercy                            | Temporary media attention & damage to image. Complaints and potential loss of clients                         | Ongoing high level of media exposure & damage to image identifying Mercy. Loss of several clients.                       |

Likelihood is assessed by the following scale:

- 1 – **Rare:** Not occurred in last 5yrs, Not likely to occur
- 2 – **Unlikely:** Occurs more than once in 5yrs but < annually, May occur
- 3 – **Possible:** Occurs at least annually but not more than monthly, Likely to occur
- 4 – **Likely:** Occurs at least monthly but no more than weekly, Most likely to occur
- 5 – **Almost Certain:** Occurs at least weekly, Expected to occur

The combination of the 5x5 consequence and likelihood ratings formulate the **risk rating matrix** (Appendix 2).

When analysing risks, the following points should be considered:

- What are the potential adverse (threats) consequences of each risk if they occur?
- What is the potential likelihood (probability) or frequency of the risks happening?
- What current controls (mitigations) exist to prevent, detect or correct the consequences or likelihood of the risk?
- Potential indicators for measuring the risk in a qualitative or quantitative way
- What is the worst case scenario for that risk?

## Risk Evaluation

The risk evaluation process requires a prioritisation of risks based off their risk assessment, post implementation of any mitigation or risk management strategies to minimise the risk. This is assessing the residual risk, to determine risk tolerances and highlight key ongoing risks to manage. Reviewing the level of residual risk allows the organisation to determine whether the risk remains within acceptable tolerance levels or requires further management action or controls to reduce the risk.

An important part of the risk evaluation process is determining the effectiveness of controls in place. Controls to mitigate risk can either be to reduce the impact (consequence) or the likelihood of the risk occurring. Assessing the effectiveness of controls in how they either reduce the consequence or

likelihood help determine the residual risk and determine if further risk treatment is required or whether existing controls are functioning correctly.

Risk controls (or mitigations) can be either:

- i. Preventative – reduce the likelihood of the risk occurring (e.g. internal controls like segregation of duties to prevent the risk from occurring; and
- ii. Corrective – reduce the impact or consequence of the risk once it has occurred (e.g. insurance).

When assessing controls, special attention is to be paid to critical controls, which are those mitigation measures that significantly reduce high inherent risks. These must be monitored and reviewed frequently to ensure their effectiveness is made and they are implemented correctly to ensure the level of residual risk is accurately accounted for.

Mercy has established a risk matrix framework to aid the risk evaluation and prioritisation process. This assigns an overall risk level for a risk, based off the assigned likelihood and severity. Those risks resulting in a High or Extreme rating are to be more closely monitored and overseen by the Board.

| LIKELIHOOD ↓   | SEVERITY →         |                    |                      |                      |                      |
|--|--------------------|--------------------|----------------------|----------------------|----------------------|
|  | 1 - Insignificant  | 2 - Minor          | 3 - Moderate         | 4 - Major            | 5 - Significant      |
| <b>1 - Rare</b><br>Not occurred in last 5yrs<br>Not likely to occur                          | <b>LOW</b><br>1    | <b>LOW</b><br>2    | <b>LOW</b><br>3      | <b>MEDIUM</b><br>4   | <b>MEDIUM</b><br>5   |
| <b>2 - Unlikely</b><br>Occurs more than once in 5yrs but < annually<br>May occur             | <b>LOW</b><br>2    | <b>MEDIUM</b><br>4 | <b>MEDIUM</b><br>6   | <b>HIGH</b><br>8     | <b>HIGH</b><br>10    |
| <b>3 - Possible</b><br>Occurs at least annually but not more than monthly<br>Likely to occur | <b>LOW</b><br>3    | <b>MEDIUM</b><br>6 | <b>HIGH</b><br>9     | <b>HIGH</b><br>12    | <b>EXTREME</b><br>15 |
| <b>4 - Likely</b><br>Occurs at least monthly but no more than weekly<br>Most likely to occur | <b>MEDIUM</b><br>4 | <b>HIGH</b><br>8   | <b>HIGH</b><br>12    | <b>HIGH</b><br>16    | <b>EXTREME</b><br>20 |
| <b>5 - Almost Certain</b><br>Occurs at least weekly<br>Expected to occur                     | <b>MEDIUM</b><br>5 | <b>HIGH</b><br>10  | <b>EXTREME</b><br>15 | <b>EXTREME</b><br>20 | <b>EXTREME</b><br>25 |

**Image 4:** Mercy’s Risk Matrix Framework

The result of this process results in a prioritisation of risks for which management and the Board can review and determine whether the risk level is appropriate or requires additional risk treatment (accept vs reject risk).

## Risk Treatment

Following the risk evaluation process and assessment of the residual risk levels, a determination can be made as to whether these risks remain within acceptable risk tolerance levels. If the residual risk is at a level higher than acceptable by management and the Board, additional risk treatment (additional controls or more effective mitigations) needs to occur to bring the risk level within the targeted level.

The risk treatment process involves identifying the most appropriate actions or practices to modify risks that are at an unacceptable level. Developing a risk treatment plan involves addressing the underlying causes, and assesses how effective the proposed treatment is. Risk treatment is required to manage those risks which are assessed outside of the organisation’s risk tolerance and risk appetite as set by the Board.

To treat risks outside of an acceptable risk level requires minimising either the likelihood of the risk occurring or its severity. The following risk treatment options are available for managing risks within tolerance levels:

- a) **Accept** – making an informed decision that the risk rating is at an acceptable level in line with strategic objectives or that the cost of the treatment outweighs the benefit. This option may also be relevant in situations where a residual risk remains after other treatment options have been put in place. No further action is taken to treat the risk, however, ongoing monitoring occurs.
- b) **Avoid** – deciding not to proceed with the activity that introduces an unacceptable risk, choosing an alternative more acceptable activity that meets business objectives, or choosing an alternative less risky approach or process.
- c) **Control or Reduce** – implementing a strategy that is designed to reduce the likelihood or severity of the risk to an acceptable level, where elimination is considered to be excessive in terms of time or expense.
- d) **Share or Transfer** – implementing a strategy that shares or transfers the risk to another party or parties, such as outsourcing the management of physical assets, developing contracts with service providers or insuring against the risk. The use of a third-party also needs to be considered as a risk and both parties should be aware of and agree to their obligations.

Once the decision has been made to treat a risk, it should be documented including the treatment option agreed, how it is to be implemented, monitored, who is responsible for the treatment (owner assigned) and a date for resolution assigned. A review of the risk analysis should be undertaken to determine the effectiveness of the risk treatment.

## Monitoring and Review

The monitoring and review process is a continual process throughout the whole risk assessment process. Risk analysis, risk registers and any risk treatments all require regular and consistent monitoring, with appropriate oversight. This enables to identify any changes to the organisational risk profile and adjust or respond appropriately in a timely manner. It also provides an avenue for management and the Board to review the effectiveness of the risk management strategies adopted.

Organisational areas of Mercy will monitor the risks they are exposed to and review their risks at a minimum quarterly, to ensure current risk ratings and exposures remain current. This process will be assisted by the designated risk and compliance lead at the organisation, who will provide effective challenge to the risk assessments taken by management. Other potential events that would trigger monitoring and review of risks include:

- if there has been a change to the strategic plan or business objectives;
- if a new business activity is engaged or a change to an existing business activity has occurred;
- following a serious incident or complaint;
- significant external event requiring a review of current exposure;
- changes to organisational structure;
- prior to introducing new technology or significant changes to existing technology;
- breakdown in a control in terms of its effectiveness or implementation; and
- change in legislative/regulatory or accreditation requirements.

The monitoring and review process will ensure that new or emerging risks are identified and included in assessments as they arise. A strong approach to risk management will assist in promoting options for better practices (and continuous improvement), while ensuring appropriate resources are assigned to address risk.

## RISK MANAGEMENT REPORTING & OVERSIGHT PROCESS

### Risk Register & Review Process

Mercy are to have a corporate and departmental risk register (template in Appendix 1) to address both the key risks at a strategic/Board level and operationally at a service level.

The corporate risk register will cover the organisation's top 20 risks (approximately), with the risk ratings and management strategies reviewed and approved by the Board annually. In determining the risks within the corporate register, it will consider the overall risk level and the risk's impact across the organisation – not just at a department level. The risk threshold is likely to be higher at a corporate level, as it includes an accumulation of the risk across all services. In line with the annual strategic plan update, the corporate risk register will be reviewed to ensure it considers any new risks arising from the strategic update and that risk assessments, risk levels remain appropriate.

The departmental risk register will document the key risks across Mercy's services and administration functions. A responsible manager will be designated ownership for each risk within the register. Departmental risk registers will be reviewed quarterly in discussion with each area's manager (or their delegate) and the Risk & Compliance Lead. A report of any proposed changes will be compiled based on the output of discussions to highlight any new risks or changes in risk rating. This will be presented to the RCI for approval and a copy provided to the Board. At the annual review, a more in depth review of risks will occur (including ratings) with a summary of changes presented to the Board for review and approval in line with the current risk appetite.

### Risk Reporting & Oversight

Risk reporting is an important part of the risk management strategy in ensuring risks are raised that are of concern to senior management for accountability and action. The quarterly departmental risk register review and presentation to the RCI provides the opportunity for risks of concern to be discussed and reviewed to ensure appropriate action is taken considering the overall impact to the organisation.

The Risk & Compliance Lead is responsible for monitoring and maintaining the corporate and departmental risk registers. This allows for a review from a quality assurance and continuous improvement perspective, to ensure consistency in application of the risk management framework.

Quarterly and annual risk register reviews will be first presented at the RCI for endorsement. The annual review will also be presented to the Board for its approval, along with review of risk tolerances and the risk appetite. The Clinical Advisory Council may also raise potential clinical risks that are to be included on the corporate or departmental risk register. Any risk identified via the Clinical Advisory Council would be included in the risk register review at the RCI. A table summarising risk reporting within Mercy is outlined in the table below.

| <b>Risk Reporting</b>                 | <b>Presented To / Discussed At</b>      | <b>Frequency</b> |
|---------------------------------------|---|------------------|
| Department Risk Registers             | Risk & Continuous Improvement Committee | Quarterly        |
| Department & Corporate Risk Registers | Board                                   | Annually         |
| Clinical Risks (as identified Ad Hoc) | Clinical Advisory Council               | Monthly          |

**Appendix 1 – Risk Register Template**

|                   |  |                            |  |
|-------------------|--|----------------------------|--|
| <b>DEPARTMENT</b> |  | <b>RESPONSIBLE MANAGER</b> |  |
|-------------------|--|----------------------------|--|

| ID | PRE - MITIGATION (Inherent Risk) |                     |  |  |  |           | POST - MITIGATION (Residual Risk) |  |  |  |
|----|----------------------------------|---------------------|--|--|--|-----------|-----------------------------------|--|--|--|
|    | RISK DESCRIPTION                 | RISK CAUSE / IMPACT | RISK SEVERITY  | RISK LIKELIHOOD  | RISK LEVEL   | RISK TYPE | MITIGATIONS, CONTROLS OR ACTIONS  | RISK SEVERITY  | RISK LIKELIHOOD  | RISK LEVEL   |
|    |                                  |                     | INSIGNIFICANT<br>MINOR<br>MODERATE<br>MAJOR<br>SIGNIFICANT | RARE<br>UNLIKELY<br>POSSIBLE<br>LIKELY<br>ALMOST CERTAIN | <b>LOW</b><br><b>MEDIUM</b><br><b>HIGH</b><br><b>EXTREME</b> |           |                                   | INSIGNIFICANT<br>MINOR<br>MODERATE<br>MAJOR<br>SIGNIFICANT | RARE<br>UNLIKELY<br>POSSIBLE<br>LIKELY<br>ALMOST CERTAIN | <b>LOW</b><br><b>MEDIUM</b><br><b>HIGH</b><br><b>EXTREME</b> |
|    |                                  |                     |  |  |  |           |                                   |  |  |  |
|    |                                  |                     |  |  |  |           |                                   |  |  |  |
|    |                                  |                     |  |  |  |           |                                   |  |  |  |
|    |                                  |                     |  |  |  |           |                                   |  |  |  |
|    |                                  |                     |  |  |  |           |                                   |  |  |  |
|    |                                  |                     |  |  |  |           |                                   |  |  |  |
|    |                                  |                     |  |  |  |           |                                   |  |  |  |



## Appendix 2 – Risk Rating Matrix

| Severity Risk Types                         | Severity Categories   |   |   |   |  |
|---|---|---|---|---|--|
|   | Insignificant   | Minor   | Moderate  | Major   | Significant  |
| Clinical Care & Client / Resident Wellbeing | No injury   | Superficial or minor injury where 1st aid is required   | Injury requiring hospitalisation  | Severe long term illness or injury suffered   | Permanent disability or death  |
| Safeguarding                                | No safeguarding issue present   | Breach of relationship boundary raised against a staff member                                     | Complaint or allegation of inappropriate behaviour made against a staff member                      | Concern raised of abuse made against a staff member   | Several allegations or cases of abuse raised against a staff member  |
| Financial                                   | Up to 1% of budget  | Up to 5% of budget  | Up to 15% of budget   | Up to 25% of budget   | Greater than 25% of budget   |
| Operational: Workforce                      | No workforce or staff shortage impacting service operations                               | Service disruption for a few hours up to a day due to workforce shortage or staff unavailability  | Service disruption or delay over a few days due workforce shortage or staff unavailability          | Ongoing disruption to a service for up to a week due workforce shortage or staff unavailability               | Inability to perform a service for a prolonged period (>week) due to workforce shortage or staff unavailability          |
| Operational: Facilities & Assets            | Minimal effect on services. No loss or damage to property, assets, records or information | Singular disruption to service. Minor loss or damage to property, assets, records and information | Temporary suspension of services due to loss or damage to property, assets, records and information | Prolonged service disruption or suspension due to loss or damage to property, assets, records and information | Cessation of services due to loss or damage to property, assets, records and information                                 |
| Regulatory & Legal                          | No regulatory or legal infringement   | Minor non-compliance with regulatory / legal requirement  | Breach of regulations or legal standards requiring notification and prompt rectification            | Multiple regulatory or legal breaches requiring mandatory reporting & potential regulatory action             | Systemic regulatory / legal breach requiring immediate reporting, resulting in possible fines or restriction on services |
| Governance                                  | No impact despite failure / lack of process & oversight                                   | Small impact to clients / business operations due to failure / lack of process & oversight        | Some ongoing impact to clients / business operations due to failure / lack of process & oversight   | Prolonged impact to clients / business operations due to failure / lack of process & oversight                | Systemic impact to clients / business operations due to failure / lack of process & oversight                            |
| Work Health & Safety                        | Injury, accident or illness not requiring medical treatment                               | Injury, accident or illness where 1st aid treatment is required                                   | Serious injury, accident or illness requiring hospitalisation                                       | Permanent disability or life threatening injury, accident or illness  | Death(s) or multiple life threatening injury, accident or illness  |
| Reputation & Image                          | No media attention or image impact  | Some complaints and minor damage to image. No media attention                                     | Some media exposure and complaints but not specifically focused on Mercy                            | Temporary media attention & damage to image. Complaints and potential loss of clients                         | Ongoing high level of media exposure & damage to image identifying Mercy. Loss of several clients.                       |

| LIKELIHOOD ↓   | SEVERITY →         |                    |                      |                      |                      |
|--|--------------------|--------------------|----------------------|----------------------|----------------------|
|  | 1 - Insignificant  | 2 - Minor          | 3 - Moderate         | 4 - Major            | 5 - Significant      |
| <b>1 - Rare</b><br>Not occurred in last 5yrs<br>Not likely to occur                          | <b>LOW</b><br>1    | <b>LOW</b><br>2    | <b>LOW</b><br>3      | <b>MEDIUM</b><br>4   | <b>MEDIUM</b><br>5   |
| <b>2 - Unlikely</b><br>Occurs more than once in 5yrs but < annually<br>May occur             | <b>LOW</b><br>2    | <b>MEDIUM</b><br>4 | <b>MEDIUM</b><br>6   | <b>HIGH</b><br>8     | <b>HIGH</b><br>10    |
| <b>3 - Possible</b><br>Occurs at least annually but not more than monthly<br>Likely to occur | <b>LOW</b><br>3    | <b>MEDIUM</b><br>6 | <b>HIGH</b><br>9     | <b>HIGH</b><br>12    | <b>EXTREME</b><br>15 |
| <b>4 - Likely</b><br>Occurs at least monthly but no more than weekly<br>Most likely to occur | <b>MEDIUM</b><br>4 | <b>HIGH</b><br>8   | <b>HIGH</b><br>12    | <b>HIGH</b><br>16    | <b>EXTREME</b><br>20 |
| <b>5 - Almost Certain</b><br>Occurs at least weekly<br>Expected to occur                     | <b>MEDIUM</b><br>5 | <b>HIGH</b><br>10  | <b>EXTREME</b><br>15 | <b>EXTREME</b><br>20 | <b>EXTREME</b><br>25 |