

Current version in effect from: 1 Apr 2024  
Approved by Council: 9 Nov 2022  
Revised by Council: 14 Jun 2023, 13 Dec 2023

## **CONTENTS**

Related Documents.....	2
1. Purpose.....	2
2. Approach.....	2
3. Scope.....	3
4. Definitions.....	3
5. Risk Management Policy.....	4
6. Risk Appetite.....	7
7. Risk Register.....	7
8. Procedures for Reporting and Management of Risks.....	7
9. Responsibility for Review and Updating.....	9
10. Acknowledgement.....	10
11. Date of Next Review.....	10

## **SCHEDULES**

Schedule A – Impact and Likelihood Matrix.....	11
Schedule B – Risk Appetite Statement.....	12
Schedule C – Risk Register Headings.....	14
Schedule D – General Management Controls.....	15
Schedule E – Risk Escalation Matrix.....	16

## Related documents

*International Standard ISO 31000:2018 Risk Management*

[College Review Policy](#)

[Complaints Policy](#)

[Critical Incidents Policy](#)

[Information Technology Access and Use Policy](#)

*Cybersecurity Framework*

[Health and Safety Policy](#)

[Privacy Policy](#)

[Safeguarding Policy](#)

[Sexual Assault and Sexual Harassment Policy](#)

[Whistleblower Policy](#)

### **1. Purpose**

- 1.1 The Enterprise Risk Management Framework (ERMF) provides a comprehensive approach to risk management across all operations of the University and its Colleges. The ERMF aims:
- a) to enable people to agree on the highest priorities for action
  - b) to inform management decision making
  - c) to assist in creating more certainty in achieving the University's objectives.
- 1.2 Understanding and managing our risks is part of how we work. The consideration of risks and our appetite for risks must be a part of key business conversations, analysis, recommendations, and decision making. The ERMF sets out how the University manages its material risks through relevant governance, documentation, controls, monitoring, accountability, and reporting.
- 1.3 The ERMF replaces the University's previous Risk Management Policy, approved by Council on 7 June 2017 and last revised on 29 Sep 2021.

### **2. Approach**

- 2.1 The ERMF is based on the methodology of the International Standard ISO 31000:2018 Risk Management. The University of Divinity subscribes to the Risk Assessment Methodology (Figure 1) whereby risks are identified, analysed, evaluated and treated through effective communication and monitoring.

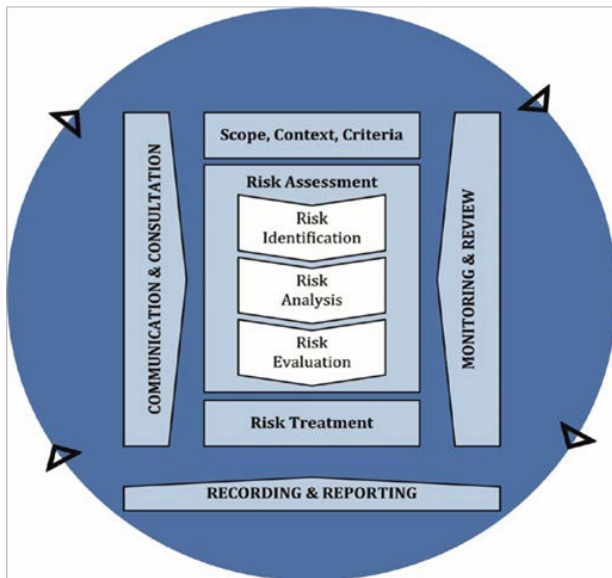


Figure 1

### 3. Scope

- 3.1 The ERMF applies to all University staff, students, contract staff, honorary appointments and visitors and covers all operations of the University.
- 3.2 The ERMF is implemented through procedures to manage specific risks that may be included in specific University policies, consistent with the ERMF.
- 3.3 Risks to personal safety or well-being are further addressed through related policies:
  - a) Critical Incident Policy
  - b) Health and Safety Policy
  - c) Safeguarding Policy
  - d) Sexual Assault and Sexual Harassment Policy.

### 4. Definitions

- 4.1 **Risk:** The effect of uncertainty on objectives.
- 4.2 **Risk Appetite:** The level of risk the University is willing to accept in the pursuit of goals.
- 4.3 **Risk Management:** The overarching cycle of processes of risk identification, risk assessment, risk evaluation, risk mitigation and risk treatment.
  - a) **Risk Identification:** A process to find, recognise and describe risks that might help or prevent the University in achieving its objectives
  - b) **Risk Assessment:** The identification, analysis, evaluation review and ranking of risk taking into account likelihood of risk and potential impact. The risk assessment matrix is set out in Schedule A which may be amended by the Finance and Risk Committee.

- c) **Risk Evaluation:** A process to compare the level of risk found during a risk assessment with the University's Risk Appetite to determine whether the risk or its magnitude are tolerable.
- d) **Risk Mitigation:** Activities or decisions in response to risk assessment designed to control, detect or respond to risk.
- e) **Risk Treatment:** The use of options to reduce a risk, including avoiding, sharing or mitigating a risk. This includes accepting and monitoring a risk that cannot be altered.

4.4 **Risk Tolerance:** The acceptable deviation from the risk appetite.

4.5 **Inherent Risk:** The level of risk assessed before actions are taken to alter the risk's impact or likelihood.

4.6 **Residual Risk:** The remaining risk after a risk treatment has been applied.

4.7 **General Management Controls:** The organisational structure, roles, responsibilities, policies, and systems that create a foundation for coordinated and consistent action and ensure effective control of activities, which in turn helps to manage risks. These are set out in Schedule D which may be amended by the Finance and Risk Committee.

4.8 **Impact:** The consequences for the University of a risk that is realised.

4.9 **Likelihood:** An evaluation of a particular threat or opportunity actually happening, including a consideration of the frequency with which this may arise.

4.10 **Risk Officer:** A position appointed by the Vice-Chancellor to identify and report risks and to manage the day-to-day implementation of the Enterprise Risk Management Framework.

## 5. Risk Management Policy

### 5.1 Principles

- a) The University's approach to risk management is consistent with the principles of AS/NZS ISO 31000:2018.
- b) The University defines risk as the effect of uncertainty on objectives, recognising that the consequences of uncertainty may be positive or negative.
- c) The University is committed to effective risk management and to maintaining a risk-aware culture.
- d) All members of the University must maintain awareness of key risks and accountabilities, foster an environment where there is willingness to raise issues, and act in line with the University's values. This includes raising and communicating risks, whether actual or perceived, when they become known, and raising any suspected breach of the University's policies.
- e) The University takes a responsible and managed approach to risks by recognising and managing risks. The degree of risk that is acceptable varies within core domains of the University activities.

- g) The University has defined processes for the identification, analysis and evaluation of risks and for responding to them through risk treatments.
- f) The University educates its members and stakeholders on the importance of risk management and the processes established in its Enterprise Risk Management Framework.
- h) The University's risk categories are aligned to key domains of its Strategic Plan, for consistency of planning and management.
- i) All activities and projects should be managed with an awareness of risks to the specific activity or project, including risk identification and management as a core component.
- j) The University allocates responsibility for managing identified risks to leadership and academic positions and to committees according to the category of risk.
- k) The University maintains risk management documentation as a primary tool for monitoring and reporting on risk.
- l) The University reports on risk to the Finance and Risk Committee and University Council in accordance with the *University of Divinity Act 1910* and the ERMF.

## 5.2 Risk Categories

The risk categories are intended to identify the root causes of risk and uncertainty in the University's operations. Other risks, such as reputational risks, may arise from untreated risks in these domains.

Primary Domain	Secondary Domain
Education	Quality and integrity
	Scholarship of learning and teaching (innovation)
	Curriculum (product - impact)
Research	Quality and integrity
	Impact and engagement
	Innovation
Governance and Relationships	Colleges and Churches
	Finance
	External Environment
People and Resources	Workplace (industrial relations and employment, health and safety, critical incidents)
	Information Management (privacy and record-keeping, IT security, intellectual property)

	Staff (equity, key person loss / succession planning, wellbeing)
Regulatory Compliance	Higher Education Standards Framework
	Other University Legislation
	Other Risks

### 5.3 Risk Assessment

The University's assessment of risks follows the process of identification, analysis and treatment.

#### 5.3.1 Risk Identification

The purpose of risk identification is to find, recognise and describe risks that might help or prevent the University in achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

#### 5.3.2 Risk Analysis

Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood of events and scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect several objectives. To help analyse risks, the University uses the Impact and Likelihood table shown in Schedule A.

#### 5.3.3 Risk Evaluation

Risk evaluation involves comparing the level of risk found during the risk analysis with the University's Risk Appetite to determine whether the risk or its magnitude are acceptable or tolerable to the University. If the risk is not acceptable or tolerable, a risk treatment will need to be considered. The University's Risk Appetite Statement (RAS) is provided in Schedule B which may be amended by the University Council.

### 5.4 Risk Treatment

#### 5.4.1 Risk treatment strategies aim to reduce the risk level. Options available to the University include:

- a) avoiding the risk by discontinuing or not commencing the activity
- b) removing the source of the risk
- c) changing the likelihood of the risk
- d) changing the consequences of the risk
- e) sharing the risk with another party (e.g. contracting or insurance)
- f) accepting a risk that cannot be altered.

#### 5.4.2 The treatment strategy adopted for each major risk is stated in the Risk Register.

5.4.3 When identifying risk treatments, external obligations, budget constraints and the impact of external influences must be considered to determine the optimal treatment plan. A range of options should be considered. Consequential impacts and dependencies should also be considered, to ensure that in managing one risk, an unacceptable situation is not created elsewhere.

## **6. Risk Appetite**

- 6.1 The University's Risk Appetite Statement (RAS) is set out in Schedule B and is approved or amended by the University Council.
- 6.2 The RAS outlines the amount and nature of risk that the University is willing to accept in pursuit of its strategic objectives and business plans.
- 6.3 The purpose of the RAS is to summarise the University's risk appetite philosophy and posture, inform our employees, and raise awareness across the organisation. The RAS includes advice on the University's risk tolerance.
- 6.4 The RAS provides direction to management to guide their decision making. Management and staff are expected to be prudent and apply good judgement in interpreting the RAS to make sensible, risk-based decisions in the best interest of the University and its stakeholders.
- 6.5 The RAS is reviewed annually to remain appropriate for changes in the operating environment. The Council works with management to maintain appropriate risks settings in line with these changes.
- 6.6 It is acknowledged that in some circumstances the risk appetite statements may result in conflicting risk management objectives. Where this is the case, a trade-off in risk will be required in order to achieve the most beneficial outcome for the University.
- 6.7 The Risk Appetite Statement is reviewed annually by the Finance and Risk Committee with a recommendation to the next University Council meeting.

## **7. Risk Register**

- 7.1 The University's Risk Register is a living document that shows the most significant risks identified at a point in time. The Risk Register is maintained by the Risk Officer under the headings set out in Schedule C which may be amended by the Finance and Risk Committee.
- 7.2 The Risk Register must:
- a) Clearly identify headline risks to the University
  - b) Provide a system of risk assessment according to the likelihood of risks occurring and the consequences
  - c) Provide descriptive information on what elements of the risk are accepted
  - d) Provide descriptive information of what risk treatment and mitigation strategies are in place.

- e) Be available on request to University Council members, Finance and Risk Committee members and University employees.

7.3 The Risk Register is reviewed and updated:

- a) continuously by the Risk Officer as notification of risks are received
- b) at least quarterly by the Vice-Chancellor and Risk Officer
- c) at least every six months by the Finance and Risk Committee
- d) at least annually by the Council.

## **8. Procedures for Reporting and Management of Risks**

Any member of the University may identify new risks or alert the University to changes in the profile (likelihood or impact) of existing risks.

Risks can take many forms, so there are several different broad methods for reporting and managing risk. These are additional to the University's General Management Controls.

### **8.1 Immediate threats**

Risks to personal safety or security should be reported and handled using processes in the University's Critical Incident Policy, Health and Safety Policy, Safeguarding Policy, or Sexual Assault and Sexual Harassment Policy.

### **8.2 New risks or changes to profile of known risks**

Any member of the University who identifies a new or emerging risk or a change in the profile of an existing risk should make a report to their supervisor. The Risk Officer should be notified by email and then advises relevant parties after consultation with the Vice-Chancellor. A record must be kept of notifications.

Risks to integrity through misconduct or illegal activity may be disclosed in confidence through the Whistleblower Policy.

### **8.3 Known risks in defined areas of responsibility**

University or College operational and academic units are responsible for identifying, assessing, managing and mitigating the risks associated with their day-to-day operations, including the implementation of University policies and meeting legal obligations. As an example, under the domain of 'Education', risks to academic integrity should be addressed through the University's Academic Integrity Policy.

Each College or University unit should keep the GMCs under active review for their own activities.

Any new risks or changes to the risk profile of an operational or academic unit should be reported up the line and by an email to the Risk Officer. The Risk Officer must keep a record and advise relevant parties after consultation with the Vice-Chancellor.

### **8.4 Education risks – Academic Board oversight**



Educational risks, including changes in risk levels, must be considered annually by Academic Board. Any new risks or changes to the risk profile for educational matters will be identified by the Academic Board, informed by reporting on specific matters, such as academic performance and outcomes and academic integrity. Academic Board may assess risk and propose risk treatments to manage educational risks. Advice from Academic Board is notified to the Risk Officer and reported to the Finance and Risk Committee and to Council.

#### 8.5 Health, safety and environment risks – Committee oversight

Health and safety risks are considered by the Health and Safety Committee at each meeting. This Committee may assess risk and propose risk treatments. Advice from this Committee is notified to the Risk Officer and reported to the Finance and Risk Committee.

#### 8.6 College Risk Assessments

Every College of the University is required to complete an annual risk assessment via a pro-forma survey and attestation by the relevant College Executive. The risk assessment includes, as a minimum, an assessment of each of the areas covered by the University Risk Appetite Statement and notification of any critical incidents in the areas covered by the University Incident Reporting requirements. College Risk Assessments are rated and form part of the reporting dashboard.

The College Risk Assessments are reviewed by the Finance and Risk Committee, which provides an annual attestation to the University Council. Any major increase in a College's risk profile or major incident must be reported immediately to the Chair of Finance and Risk Committee, and as appropriate to the next Finance and Risk Committee and University Council meeting.

#### 8.7 TEQSA Provider Risk Assessments

The University is subject to the annual TEQSA Provider Risk Assessment process. While based on prior year data and limited in scope (Risk to Students and Risk to Financial Position), the Annual Provider Risk Assessment provides a benchmark for testing the University's own assessments and monitoring, as well as highlighting potential areas for action.

The TEQSA Provider Risk Assessment is considered by the next Finance and Risk Committee meeting after it becomes available and reported with any recommendations to the next University Council.

#### 8.8 Finance and Risk Committee of Council

The Council delegates oversight of risk management to its Finance and Risk Committee. The Terms of Reference for the Finance and Risk Committee are found in Schedule 1 to Regulation 1 Council.

The Finance and Risk Committee is responsible for identifying any new or emerging risks that have not been identified elsewhere, particularly risks that arise from changes in the University's external environment.

#### 8.9 Risk awareness

The Vice-Chancellor, supported by the Risk Officer, is responsible for raising awareness of risk across the University and discussing risk management with Colleges and Schools annually.

8.10 Risk Escalation

In addition to the risk reporting and management responsibilities outlined above, guidelines for the escalation of specific risks to senior levels of the University are set out in Schedule E, Risk Escalation Matrix.

**9. Acknowledgement**

9.1 This Framework has been developed using examples from several Australian universities, including the University of Queensland and Western Sydney University. The University of Divinity acknowledges these sources with gratitude.

**10. Date of Next Review**

10.1 The ERMF is reviewed annually by the Finance and Risk Committee with a recommendation to the next University Council meeting.

10.2 The ERMF is subject to an external review no later than 31 December 2029.

## SCHEDULE A

### IMPACT AND LIKELIHOOD MATRIX

Approved by Risk Committee: 2 Nov 2022

Revised by Finance and Risk Committee:

Risk Rating Matrix: Impact x Likelihood gives a score for inherent and residual risks in the Risk Register.

Impact	Likelihood				
	Rare (1) (remote)	Unlikely (2) (uncommon)	Possible (3) (occasional)	Likely (4) (probable)	Almost Certain (5) (frequent)
Catastrophic (5)	Moderate	Moderate	High	Critical	Critical
Major (4)	Low	Moderate	High	High	Critical
Moderate (3)	Low	Moderate	Moderate	Moderate	High
Minor (2)	Very Low	Low	Moderate	Moderate	Moderate
Insignificant (1)	Very Low	Very Low	Low	Low	Low

#### Impact Scale

- 1. Insignificant:** some localised inconvenience, but no impact to the organisation, absorbed within business running costs.
- 2. Minor:** disruption to operations with no permanent or significant effect on the organisation.
- 3. Moderate:** some impact on the organisation's operational performance, less impact on strategic goals in the medium term.
- 4. Major:** significant effect on operational performance which will require operational resource reallocation (financial, assets and /or people) to manage and resolve in the medium term to avoid non achievement of strategic goals.
- 5. Catastrophic:** achievement of operational and strategic goals in the medium term jeopardised and the existence of the organisation is under threat.

#### Likelihood Scale

- 1. Rare:** only in exceptional circumstances
- 2. Unlikely:** small chance of occurring at some time.
- 3. Possible:** might occur at some time
- 4. Likely:** will probably occur in some circumstances
- 5. Almost Certain:** expected to occur or a common occurrence.

## SCHEDULE B

### RISK APPETITE STATEMENT

Approved by Council: 22 Nov 2017

Revised by Council: 8 Dec 2021, 9 Nov 2022, 14 Jun 2023

The University of Divinity's risk appetite is informed by its fundamental values, as expressed in its Graduate Attributes: Learn, Articulate, Communicate, Engage, and Serve.

The University accepts a **moderate** to **high** level of risk in activities that contribute to attainment of its Vision, Mission and Strategic Plan and a **low** level of risk in activities which are not aligned with its Vision, Mission and Strategic Plan or which may cause harm to people. This risk appetite is expressed below in relation to specific areas of activity.

Risk	Owner	Appetite
<b>EDUCATION</b>		
1. Quality and Integrity	Chair of Academic Board	Low
2. Scholarship of learning and teaching (innovation)	Dean of Academic Programs	Moderate
3 Curriculum (product - impact)	Dean of Academic Programs	Moderate
<b>RESEARCH</b>		
4. Quality and Integrity	Dean of Research Strategy	Low
5. Impact and Engagement	Dean of Research Strategy	High
6. Innovation	Dean of Research Strategy	High
<b>GOVERNANCE AND RELATIONSHIPS</b>		
7. Colleges and Churches	Vice-Chancellor	Low
8. Finance	Vice-Chancellor	Low
9. External environment (culture)	Vice-Chancellor	Moderate
10. External environment (reputation)	Vice-Chancellor	Low
<b>PEOPLE AND RESOURCES</b>		
11. Workplace (industrial relations and employment, health and safety, critical incidents)	Vice-Chancellor	Low
12. Information Management (privacy and record-keeping, IT security, intellectual property)	IT Manager	Low
13. Information Management (learning environment)	IT Manager	Low
13. Staff (equity, key person loss / succession planning, wellbeing)	Vice-Chancellor	Low
<b>REGULATORY COMPLIANCE</b>		

14. Higher Education Standards Framework	Vice-Chancellor	Low
15. Other Higher Education Legislation (including University of Divinity Act)	Vice-Chancellor	Low
16. Other Risks	Vice-Chancellor	TBD

## SCHEDULE C

### RISK REGISTER HEADINGS

Approved by Risk Committee: 2 Nov 2022

Revised by Finance and Risk Committee:

- 1. Risk Categories**
  - Primary
  - Secondary
  
- 2. Risk Identification (major risks)**
  - Name of Risk
  - Brief Description
  - Impact and related risks
  
- 3. Risk Assessment**
  - Data or evidence to support risk analysis
  - HESF Domain and risk area
  - Likelihood (1-5)
  - Impact (1-5)
  - Inherent Risk (L x I)
  - Risk Appetite
  
- 4. Risk Treatment**
  - Treatment
    - Avoid
    - Transfer
    - Accept
    - Mitigate
  - Risk controls in place
  - Other mitigation required
  - Residual risk (L x I)
  
- 5. Accountability**
  - Responsible position
  - Reporting
  - Date of most recent change to Risk Register
  - Author of change

**SCHEDULE D**  
**GENERAL MANAGEMENT CONTROLS**

Approved by Risk Committee: 2 Nov 2022

Revised by Finance and Risk Committee:

The GMCs are implemented and assessed for their effectiveness within each organisational unit of the University and each College.

#	Control Objective	Principal Question ('Yes' responses must be supported by verifiable evidence)
1	Clarity of objectives, strategies and KPIs	Have the objectives and strategies been clearly defined, aligned, prioritised, and communicated to those who need to know?
2	Stakeholder management	Have the primary stakeholders been identified and strategies put in place to recognise and protect their rights and develop respectful, equitable and mutually beneficial relationships with them?
3	Enabling organisational structure	Does the organisational structure facilitate the effective and timely implementation of the strategy and the monitoring, measuring, and reporting of performance?
4	Proper plans and budgets	Are there approved plans and budgets for all objectives, strategies, initiatives/projects and have these plans and budgets been communicated to those who need to know?
5	Clarity of roles and accountabilities	Are the roles, responsibilities, and accountabilities for the delivery of outcomes clearly articulated and assigned to individuals or teams?
6	Capable staff	Are organizational and academic roles staffed by competent people?
7	Authority and delegations	Do managers and staff have appropriate authorities and delegations and mandate to achieve the outcomes expected of them?
8	Supportive culture	Do managers and staff behave in accordance with the UD Code of Conduct?
9	Safety	Are processes and protocols in place to protect people from harm?
10	Compliance	Is there a robust process in place to demonstrate compliance with applicable laws and regulations and are regulatory breaches (if any) recorded, reported, and promptly rectified?
11	Security of assets	Is there effective security over assets including systems, information, and vital records?
12	Performance monitoring and reporting	Are College, School and staff performance against their respective KPIs and plans measured, monitored, and reported on and timely actions taken to help improve performance?
13	Responsible use of resources	Are there controls in place to ensure responsible, sustainable use and management of University resources including natural resources?
14	Appropriate records and reports	Are records and reports required for business or legal/regulatory reasons produced and are they relevant, reliable, timely and retained?
15	Continuity of operations	Are there robust plans and processes in place to ensure continuity of business-critical operations?
16	Supervision, monitoring and review of internal controls	Is there effective supervision, monitoring and review of the effectiveness of implemented controls so that staff observe (local) operating procedures, systems, and processes?
17	Management assurance	Does management provide reliable assurance and/or evidence to demonstrate effective performance, risk management and compliance?

**SCHEDULE E**  
**RISK ESCALATION MATRIX**

Approved by Council: 14 Jun 2023

Revised by Council:

All risk issues, potential or realised, must be appropriately escalated for consideration at senior levels of the University. Escalation is based on the level of impact and the urgency required.

1. Level of Impact

1.1 Risks with insignificant impact must be reported as soon as possible to the Risk Officer and then to the appropriate committees within the University for monitoring and consideration of whether further investigation and/ or process improvements are required. Note that ‘weak signals’, or what appear to be isolated, individual cases, may be symptoms of a systemic issue with more significant impact and must be reported nonetheless.

1.2. Risks with impact greater than insignificant must be escalated and/ or reported to the appropriate levels within the University according to the table below.

2. Urgency

2.1 Immediate escalation (i.e. consultation as soon as possible with the Vice-Chancellor, relevant senior leader and/ or Chair of the relevant committee or Council, is required in the any of the following circumstances:

- a) a critical incident has occurred or there is an extreme risk of a critical incident
- b) the University’s reputation may be quickly jeopardised (e.g., through media exposure)
- c) a (potential) breach of law or non-compliance with Government regulation may occur
- d) there is a critical risk to student academic continuity and/ or tuition assurance.

2.2 Routine escalation, i.e., developing an action plan, reporting and discussion at the next meeting of the relevant committee or of Council, may be sufficient in the following circumstances:

- a) Where the level of risk (including residual risk) exceeds or is likely to exceed the thresholds set out in the Risk Appetite Statement (Schedule B)
- b) Where responding to a risk involves multiple stakeholders within the University.

Impact level (Per Schedule A: Impact and Likelihood Matrix)	Escalation/ reporting
<b>1. Insignificant:</b> some localised inconvenience, but no impact to the organisation, absorbed within business running costs.	<b>Risk Officer and relevant committees</b>



<b>2. Minor:</b> disruption to operations with no permanent or significant effect on the organisation.	<b>Vice Chancellor and other relevant senior leaders</b>
<b>3. Moderate:</b> some impact on the organisation's operational performance, less impact on strategic goals in the medium term.	<b>Finance and Risk Committee and other relevant committees</b>
<b>4. Major:</b> significant effect on operational performance which will require operational resource reallocation (financial, assets and /or people) to manage and resolve in the medium term to avoid non achievement of strategic goals.	<b>Council</b>
<b>5. Catastrophic:</b> achievement of operational and strategic goals in the medium term jeopardised and the existence of the organisation is under threat.	<b>Council</b>
<b>Note:</b> This table sets out the minimum level of escalation, however any issue requiring timely consideration may be directly referred to Council.	