Griffith UNIVERSITY

RISK MANAGEMENT FRAMEWORK

Approving authority	University Council
Approval date	5 August 2013 (3/2013 meeting)
Advisor	Vice President (Corporate Services) | vpcorporateservices@griffith.edu.au | (07) 373 57343
Next scheduled review	2018
TRIM document	2013/0014762
Document URL	http://policies.griffith.edu.au/pdf/Risk Management Framework.pdf

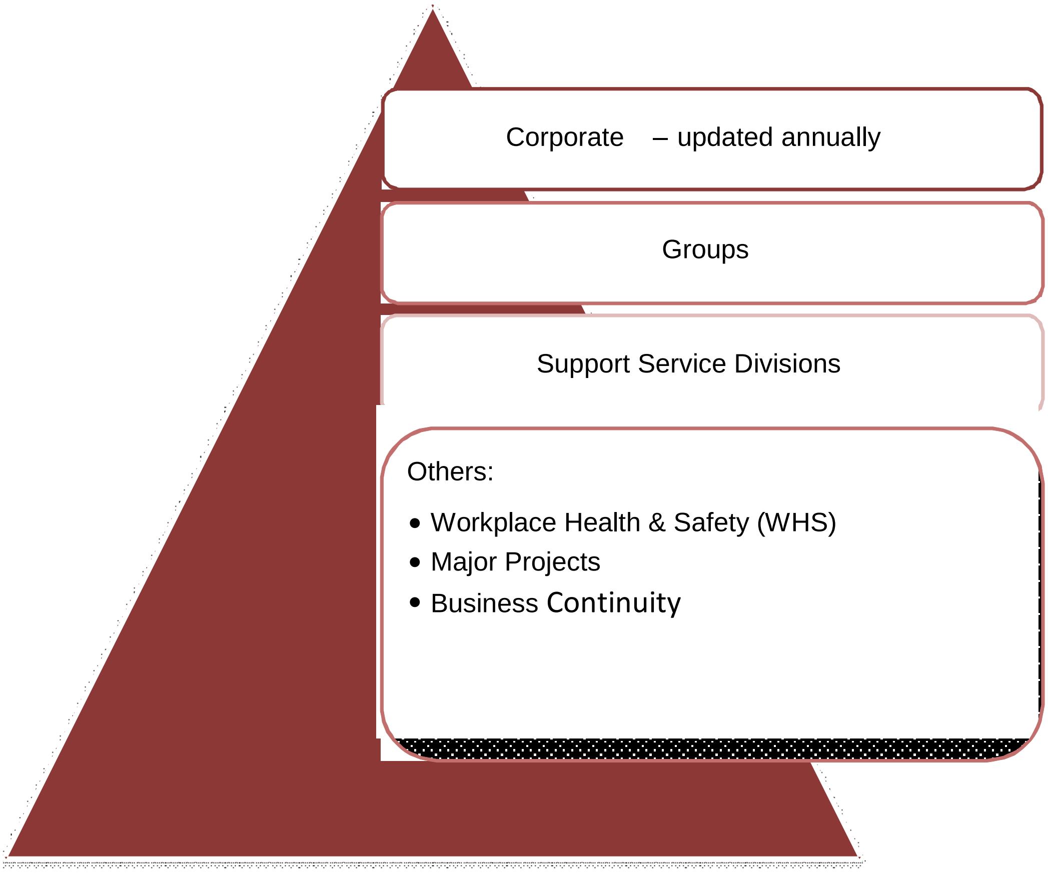
Table of Contents

1. Scope & Objectives of the Risk Management Framework

1.1 Scope of the Risk Management Framework

This document outlines the Risk Management Framework for activities within the University and all its operations and entities. The Framework defines the University's risk management process, methodology, appetite, training and reporting, and also establishes the responsibilities for implementation.

Risk management is part of the University's day-to-day operations and is undertaken at **Group and Divisional** levels as well as more broadly at the overall University level. The overall aim of risk management within the University is to ensure that organisational capabilities and resources are employed in an efficient and effective manner to manage both opportunities and threats. To this end, the University has a Taxonomy of Risk Management, i.e. the Risk Management Framework is both a top down (University wide) and bottom up approach (including assessments from Groups and support service Divisions, WHS, major projects, and business continuity). This taxonomy is illustrated below.


Corporate – updated annually
Groups
Support Service Divisions
Others:
• Workplace Health & Safety (WHS)
• Major Projects
• Business Continuity

1.2 Objectives of the Risk Management Framework

The objective of this Risk Management Framework is to provide a formal process to assist the University in:

- Encouraging understanding by managers and their staff of the implications of risk exposures, opportunities and their risk management, in their day-to-day work and in strategic and operational planning activities;
- Developing and implementing procedures to ensure that risks are identified, assessed against accepted criteria and that appropriate measures are implemented;
- Defining and documenting responsibilities and processes.

1.3 Why is Risk Management Important?

Risk influences every aspect of the operations at the University. Understanding the risks we face and managing them appropriately will enhance our ability to make better decisions, safeguard our assets, enhance our ability to provide services to our students and to achieve our University mission and goals.

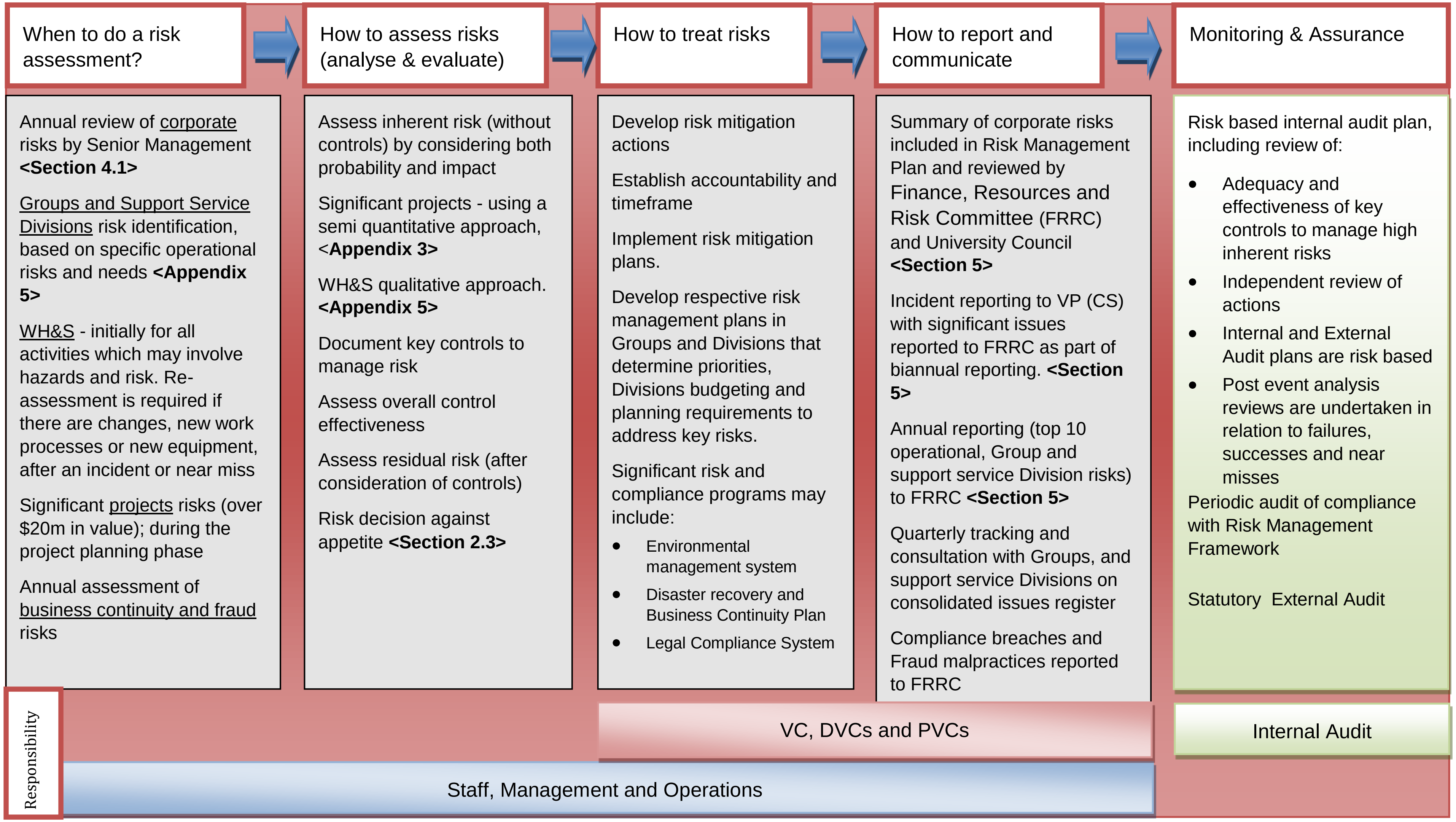
The University views the management of risks to its people, assets and all aspects of its operations as an important responsibility. It is committed to upholding its moral, ethical and legal obligations by implementing and maintaining a level of risk management which protects and supports these responsibilities.

An effective Risk Management Framework is not only good business practice but provides organisational resilience, confidence and benefits, including:

- Provides a rigorous decision-making and planning process;
- Provides the University with the flexibility to respond to unexpected threats;
- Takes advantage of opportunities and provides competitive advantage;
- Equips managers with tools to anticipate changes and threats that face the University and to allocate appropriate resources;
- Provides assurance to University Council, management and stakeholders that critical risks are being managed appropriately within the University; and
- Enables better business resilience and compliance management.

2. Risk Management Framework

Summary of the Griffith University Risk Management Framework



When to do a risk assessment?

Annual review of corporate risks by Senior Management **<Section 4.1>**

Groups and Support Service Divisions risk identification, based on specific operational risks and needs **<Appendix 5>**

WH&S - initially for all activities which may involve hazards and risk. Re-assessment is required if there are changes, new work processes or new equipment, after an incident or near miss

Significant projects risks (over $20m in value); during the project planning phase

Annual assessment of business continuity and fraud risks

How to assess risks (analyse & evaluate)

Assess inherent risk (without controls) by considering both probability and impact

Significant projects - using a semi quantitative approach, <**Appendix 3>**

WH&S qualitative approach. **<Appendix 5>**

Document key controls to manage risk

Assess overall control effectiveness

Assess residual risk (after consideration of controls)

Risk decision against appetite **<Section 2.3>**

How to treat risks

Develop risk mitigation actions

Establish accountability and timeframe

Implement risk mitigation plans.

Develop respective risk management plans in Groups and Divisions that determine priorities, Divisions budgeting and planning requirements to address key risks.

Significant risk and compliance programs may include:

- Environmental management system
- Disaster recovery and Business Continuity Plan
- Legal Compliance System

How to report and communicate

Summary of corporate risks included in Risk Management Plan and reviewed by Finance, Resources and Risk Committee (FRRC) and University Council **<Section 5>**

Incident reporting to VP (CS) with significant issues reported to FRRC as part of biannual reporting. **<Section 5>**

Annual reporting (top 10 operational, Group and support service Division risks) to FRRC **<Section 5>**

Quarterly tracking and consultation with Groups, and support service Divisions on consolidated issues register

Compliance breaches and Fraud malpractices reported to FRRC

Monitoring & Assurance

Risk based internal audit plan, including review of:

- Adequacy and effectiveness of key controls to manage high inherent risks
- Independent review of actions
- Internal and External Audit plans are risk based
- Post event analysis reviews are undertaken in relation to failures, successes and near misses

Periodic audit of compliance with Risk Management Framework

Statutory External Audit

Responsibility

VC, DVCs and PVCs

Internal Audit

Staff, Management and Operations

2.1 What is risk?

In this Risk Management Framework, risk is defined as an event that may have an impact on the achievement of the University's objectives. Risk may arise from external factors (e.g. risks from global economic crisis, change in student demographics and numbers, changing legislation) or internal sources (e.g. new projects, new faculty, infrastructure and capacity challenges, performances, etc.).

2.2 Development of risk registers

Risk registers identify and record the risks facing different areas of business. Identifying risk is a critical step in managing it. Risk registers allow the University to assess the risk in context with the overall University strategy, and help record the controls and treatments of those risks. Risk registers are developed on three tiers, Corporate level, the operational level (Group and Support Service Divisions), and the project level (Refer **Section 4).**

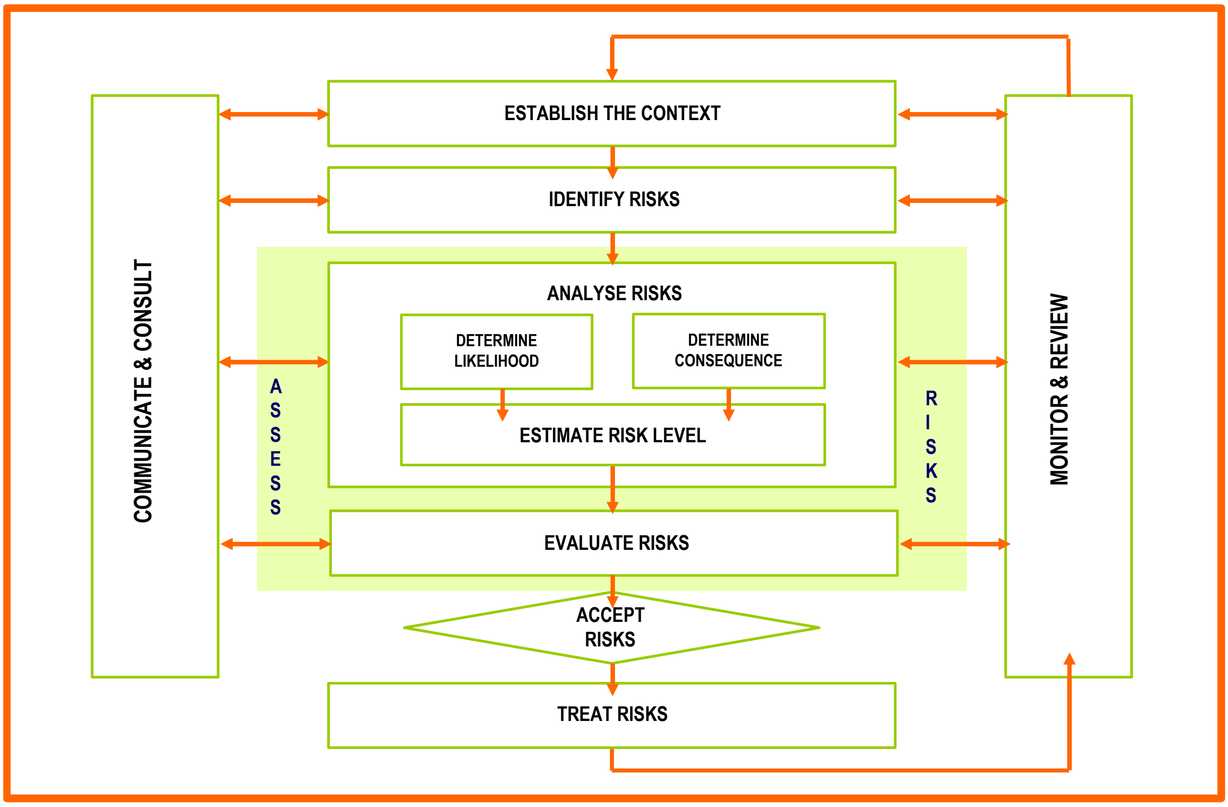
2.3 Risk appetite

Once risks are identified, the adequacy of controls must be considered within the context of the University's risk appetite at the time. This will vary with business and operational strategies, from year to year depending on the University's circumstances. The top 10 risks of each risk management plan should be submitted to the Finance, Resources and Risk Committee to monitor the level of acceptable risk for high risks, and extent of appropriate mitigating actions. Risk appetite is the amount of risk, on a broad level, that the University is willing to accept in pursuit of value, and should reflect:

- Risk management philosophy per location, project, process, etc;
- Capacity to take on risk;
- the University objectives, business plans and respective stakeholder demands;
- Evolving industry and market conditions; and
- Tolerance for failures with quantitative values, where applicable.

2.4 Risk management methodology

The Risk Management Process is based upon an internationally accepted standard: ISO 31000: 2009, as shown below



The above illustration is detailed within the key steps of the University Risk Management methodology below:

A Communication

Ongoing communication and consultation with all involved parties to ensure understanding of the process and its intended outcomes is performed by the Risk Administrator. This involves collating reports for presentation to the Finance, Resources and Risk Committee and University Council; facilitating ongoing operational reviews of risk registers, coordinating risk assessments for specific projects and ongoing advice and support to ensure compliance with the Risk Management Framework.

B Establish context

Risk management takes place within the goals and objectives of the University. Therefore, risk management must be placed into both a strategic and operational context.

Strategic Context

Strategic risk identification involves the relationship between the University and the broad external environment/community. A range of issues should be considered in examining the strategic content, including:

- Opportunities and threats associated with the local, regional, state and global economic, social, political, cultural, environmental, regulatory and competitive environments;
- Key thrusts of stakeholder strategies; and
- Strengths and weaknesses of the University in attaining corporate objectives and exercising a state of influence amongst local and national universities.

Operational Context

Operational risk identification involves gaining an understanding of the organisation’s capabilities, goals, objectives, strengths and weaknesses by considering:

- Organisational structure and culture;
- Geographics/demographics;

- The identity and nature of interaction with key stakeholders;
- The existence of any operational constraints;
- Objectives and key performance indicators;
- Business resilience vulnerabilities;
- Relevant issues relating to recent change management risk, performance or audit reviews;
- Relevant stakeholder community concerns or requirements;
- Regulatory and contractual requirements and constraints; and
- Business management systems.

C Risk identification

Risk identification is a critical activity at both a strategic and operational level. It needs to include all significant sources of risk, including those beyond the University's control. If a risk/threat is not identified, there can be no strategy to defend against it. The objective of this step is not to create an onerous and lengthy list of all possible risks, but to identify all significant risks that could impact Group or Support Service Divisions. The risk register format is included in **Appendix 4**.

How does the University identify risks?

Risk can be identified through the use of:

- Focus groups (using brainstorming approaches, SWOT analysis techniques, project categories, or broad business categories);
- Workshops;
- Interviews with respective management by the Risk Administrator; and
- The intranet is also a means of reporting incidents or risks to the Risk Administrator for consideration.

Enterprise wide risks to the organisation are identified and reviewed annually by Executive Group, Finance and Resource Committee and University Council. These risks form the basis of the overall risk profile for the organisation.

The Risk Administrator facilitates ongoing operational reviews to develop Group and Support Service Division risk registers and action plans. A consistent format is maintained throughout to facilitate reporting and summarising (separate templates are used for Project risk assessments **– refer Appendix 3).**

Categories of Risk

The following broad categories of risk are used to enable appropriate aggregation and to assist with the identification of systemic issues and trends across the University.

1. Students
2. Financial
3. Operational
4. Information and communication technology
5. Environmental
6. Legal and Regulatory Compliance
7. Organisational effectiveness (resourcing and industrial relations)
8. Workplace Health & Safety
9. Reputation & Corporate Social Responsibility
10. Projects

D Risk Analysis and Evaluation

The objectives at this step are to separate the minor risks from major ones. The level of risk is determined by measuring the likelihood of each event arising and the associated consequences.

Measuring the Level of Likelihood and Consequence

Other than WHS Risks, consequence will generally be assessed against the direct financial and operational impacts to the University. However, for some risks the most significant consequence is the impact on the University's reputation rather than the direct financial consequence. For such risks, the direct financial consequence of a risk may be negligible, but continuing reoccurrences may result in significant damage to the University's reputation and standing which impacts the attractiveness of the University to students or prejudices future projects or government funding.

As the University-wide risk management program focuses on operational and corporate risks, the financial loss given to each rating has been determined in the light of what impact would be felt by the University as a whole. For Group/Division specific risk assessments, the same consequence and financial loss criteria should be utilised. However, a specific Project consequence criterion has been established.

Probability or likelihood estimations are established giving due consideration to the effectiveness of existing control measures. The qualitative terms have been adopted from the Australian Standard. The likelihood criteria are included in **Appendix 1**.

The Consequence Rating Evaluation Criteria Chart (included in **Appendix 2**) defines the consequence criteria, assessed against potential financial loss, reputation impact, health and safety, legal and regulatory compliance and management time and effort.

The limits contained in this Consequence Rating Evaluation Criteria are based on the management's assessment of the University's ability to continue operation in the event of a risk being realised. The setting of the lower limit of $1M as "Insignificant" has been fixed in light of the test of materiality. The upper limit of $50M is based on management's assessment of the ability of the University to support an unexpected loss of this magnitude whilst still remaining solvent. As the University's capacity to bear loss changes, the values attributed to these rating will be reviewed.

Inherent risk rating

An inherent risk rating represents the level of risk in the absence of a control environment and is arrived at after measuring the likelihood and the consequence of an event occurring.

The matrix format ranking has been adopted for the University in which potential risks are ranked as Extreme, High, Moderate or Low. This is as follows:

Table of Risk Ranking

Table 2: Risk Ranking matrix

Likelihood	**Consequences**				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost Certain	**Low**	**Medium**	**High**	**High**	**Extreme**
Likely	**Low**	**Medium**	**Medium**	**High**	**High**
Possible	**Low**	**Low**	**Medium**	**Medium**	**High**
Unlikely	**Low**	**Low**	**Low**	**Medium**	**Medium**
Rare	**Low**	**Low**	**Low**	**Low**	**Medium**

Prioritising risks

The purpose of prioritising the risk is to determine the level of action needed for the identified and assessed risks.

Table of Management Action

Risk Score		**What should I do?**
9-10	**Extreme**	Immediate action required
7-8	**High**	Action plan required, senior management attention needed
5-6	**Medium**	Specific monitoring or procedures required, management responsibility must be specified
2-4	**Low**	Manage through routine procedures. Unlikely to need specific application of resources.

Evaluate and record existing controls

Existing controls are identified and the control effectiveness is assessed based on management's understanding of the controls effectiveness. The University's Internal Audit function may assist in the evaluation of control effectiveness, if required. However, this remains a management responsibility.

Table of Control Levels

Level of Control	**Audit Definition**
Good	A high degree of reliance can be place on the system of internal control. Compensating controls are in place such that even if part of the system breaks down, the four control criteria will probably still be met
Satisfactory	The controls can be relied upon; however, some improvements to controls can be made
Marginal	The system can generally be relied upon in most circumstances but there are some circumstances where one or more of the four control criteria may not be met
Weak	The system of internal control cannot be relied upon to meet the four control criteria. If there has not already been a significant breakdown, it is only a matter of time before this occurs

The four control criteria are:

- *Reliable and accurate information.*
- *Compliance with policies, plans, procedures, laws, regulations and contracts.*
- *Safeguarding of assets.*
- *Economic and efficient use of assets.*

Determine the Level of Residual Risk

Residual risk represents the level of risk after taking into account existing controls for each risk. By relating the likelihood and consequence ratings after considering controls for each risk using the Evaluation Criteria, the level of residual risk is determined. The Consequence Risk Analysis and Evaluation Criteria for the University's various categories of risk are detailed in the following table.

E Risk treatment

The objective of this step is to identify how the identified risks will be treated. Risk treatment involves identifying the options for treating each risk, evaluating those options, assigning accountability (for Extreme, High and Moderate residual risks) and taking relevant action. The following options are available for treating risks and may be applied individually or in combination, with due consideration of risk appetite:

Avoid the risk	Not to proceed with the activity or choosing an alternative approach to achieve the same outcome. Aim is risk management, not aversion.
Mitigate	Reduce the likelihood - Improving management controls and procedures.
	Reduce the consequence - Putting in place strategies to minimise adverse consequences, e.g. contingency planning, Business Continuity Plan, liability cover in contracts.
Transfer the risk	Shifting responsibility for a risk to another party by contract or insurance. Can be transferred as a whole or shared.
Accept the risk	Controls are deemed appropriate. These must be monitored and contingency plans developed where appropriate.

F Monitoring and Reporting

The objective for this step is to monitor the risks and effectiveness of the risk treatment program. Risks should be reviewed regularly to ensure relevancy and currency. Refer **Section 5** for detail.

3. Roles and Responsibilities

University Council will oversee risk management within the University, on the advice of the Finance, Resources and Risk Committee.

The Vice Chancellor will be responsible for the implementation of risk management within the University, and for responding to and reporting on significant risks that may emerge from time to time. The implementation of an effective Risk Management Framework is a leadership responsibility requiring the support of University Council, Vice Chancellor, Deputy Vice Chancellors and Pro Vice Chancellors. University Council and the Vice Chancellor have set out the University's expectations in a Risk Management Policy. The Vice Chancellor and Senior Managers provide support in a number of ways as outlined below.

3.1 Vice Chancellor

The Vice Chancellor is responsible for ensuring that the University takes appropriate measures to identify, assess and manage corporate risks. The ability to assess risk accurately, formulate effective policy and monitor compliance is an essential function of good corporate governance.

The Vice Chancellor has a number of responsibilities in relation to the management of risk, including ensuring that —

- A control environment supporting the University's strategic direction and culture is implemented and maintained;
- the University's risk appetite is aligned with strategy;
- the University operates within its legal and regulatory obligations;
- the University can continue to function in the face to major disruptions;
- Major policies keep abreast of any material changes in the operating environment.

3.2 Vice President (Corporate Services)

The Vice Chancellor has delegated to the Vice President (Corporate Services) responsibility for the establishment of an effective risk management framework throughout the University.

3.3 Deputy and Pro Vice Chancellors

The Deputy Vice Chancellors and Pro Vice Chancellors are responsible for implementing risk management within their portfolio areas to;

- Understand their risk management obligations;
- Ensure the means for identifying and reporting risks and exposures are provided;
- Develop and maintain risk registers;
- Ensure regular reporting against the ten (10) most significant risks in each Group and Support Service Divisions.

3.3 Risk Administrator

The Risk Administrator is a key position with the responsibility to facilitate the implementation of risk management processes by —

- Facilitating risk assessments and risk management activities;
- Providing advice and support;
- Monitoring the application of the risk management process across the University and reporting on the level of risk management implementation; and
- Promoting acceptance of risk management techniques.

It is not the Risk Administrator's role to manage risks on behalf of other parties. The appointment of a Risk Administrator therefore does not remove the responsibility from management and staff to manage risks and controls for which they are accountable.

3.5 Internal Audit Responsibilities

Internal Audit is responsible for providing some independent assessment of the effectiveness of the University's processes for managing particular areas of business risk. The scope of Internal Audit's risk-based program is agreed as part of an Annual Internal Audit Plan which is approved by the Audit Committee.

4. Development of Risk Management Plans

A Risk Management Plan (or register) outlines the foreseeable risks and provides a set of actions to be taken both to prevent the risk from occurring and reduce the impact of the risk should it eventuate (template detailed in **Appendix 4**). More specifically, the plan includes:

- List of foreseeable significant risks;
- Rating of the Likelihood and Consequence of each risk occurring;
- Set of preventative actions to reduce the probability of the risks occurring;
- Set of contingent actions to reduce the impact should the risk eventuate; and
- Process for managing risks.

4.1 Enterprise Risk Management Program

The Vice Chancellor through the Vice President (Corporate Services) arranges an annual review of the key corporate risks. Key enterprise risks are the highest potential risk before controls and treatment strategies are applied (inherent risk). These risks and their controls are reviewed at the University executive level and reported annually to the Finance, Resources and Risk Committee and University Council.

To support this, senior management will annually prepare Group/Divisional risk registers as required. Due dates will be established and communicated to all responsible executives within respective Group and Support Service Divisions.

Managers will present their Risk Plans to the Vice Chancellor for review and confirmation of the acceptability of the risk plan.

Operational risk management program

The Risk Administrator facilitates ongoing operational reviews to develop Group and Support Services Division risk registers and action plans, as required. A consistent format is maintained throughout to facilitate reporting and aggregation. Risks are linked to objectives to appropriately develop controls and strategies. The operational register template is detailed in **Appendix 4**.

4.2 Project Risk Management

Major projects are subject to risk examination and will maintain sufficient risk management plans to provide an effective response in the event of significant operating risks. A major project is a projects (other than building projects) over $20m.

The University's Project Risk Assessment procedures (template is detailed in **Appendix 3**) outline a methodical and informed decision making process for evaluating risks associated with major projects. This template is a semi quantitative guideline only and sections may be added, removed or redefined to meet particular project circumstances. In addition, PRINS II may also be utilised as a project risk management tool, where available. The process is facilitated by the Risk Administrator in conjunction with the University project consultants. Each major project will have its own risk register.

The risk plan should be documented early in the project – during the planning phase, and prior to execution phase. This will ensure any risks identified are addressed during the execution phase itself.

5 Risk Management Reporting

5.1 Risk Management Reporting Objectives

Documentation of risk management plans is designed to be brief, but with sufficient detail to provide understanding of the risk, key controls and rationale for mitigation strategies.

Monitoring and reporting against the University's risk management function is achieved through a number of complementary processes, illustrated below:

Business Unit and Finance & Resource Committee reporting

Key operational risks are discussed at Group and Divisional management meetings on a quarterly basis. The Risk Administrator will aggregate and develop a 6 monthly report (top ten (10) significant risks - detailed template in **Appendix 5**). More frequent reporting against high level risks occurs as deemed necessary, including direct reporting by the manager accountable –refer chart overleaf.

The Group/Divisional level risks are collated by the Risk Administrator, and presented annually, to the Finance, Resources and Risk Committee (illustrated overleaf). This report will include:

- Risk register of top 10 corporate risks;
- Executive summary of key changes in risk profile and appetite; and
- Commentary on significant residual risks (for committee consideration).

Third Party Reviews

Reviews by independent assurance providers such as internal and external audit, overseen by the Finance, Resources and Risk Committee, provide an objective view of the University's controls and therefore the elements of the University's Risk Management Framework.

Internal audit and external audit planning is risk-based to identify and focus on the University's most significant business risks.

Post event Analysis

Post event analysis reviews are undertaken in relation to failures, to provide focused reviews of the strengths and weaknesses of the University's Risk Management Framework.

Annual University Council Review

The Finance, Resources and Risk Committee undertakes an annual assessment of University's control environment for the purposes of providing advice to University Council. This assessment includes —

- Changes in the nature and extent of the University's most critical risks since the last assessment and the University's ability to respond to those risks;
- The scope and quality of the ongoing monitoring of risks by management and assurance providers such as internal audit;
- The level of reporting on the outcome of the risk monitoring process and its contribution to University Council's knowledge of the effectiveness with which risks are being managed; and
- The occurrence of significant control failures, the implications arising from these failures, corrective action undertaken and controls to manage future occurrences of the threat.

The Committee reports its assessment to University Council for consideration.

6 Audit and Assurance

6.1 Internal Audit

Internal Audit is a key component of the University's assurance framework.

The primary objective of Internal Audit is to provide an assurance framework to underpin the risk management program. This includes reviews of processes and controls over high risks as determined through the risk planning process. The internal audit function provides independent appraisal of the adequacy and effectiveness of internal controls. Recommendations will be provided, where applicable, for improvements to controls, efficiency and effectiveness of processes.

The internal audit function reports directly to the Audit Committee. Internal Audit also provides an ongoing cycle of compliance audits of key controls, which is built into the annual audit planning process as approved by the Audit Committee.

6.2 Business Continuity Management

Insurance Strategy

Insurance is a means of transferring residual risk. The University's insurance program is reviewed on an annual basis, taking into account the risk profile, the prevailing status of the insurance market and the University's risk appetite at the time.

Disaster Recovery Planning

Operating processes will maintain plans to provide effective response in the event of a significant safety, technology, or environmental incident. Such plans will provide for expedient response to protect the safety and well being of personnel, the protection of the University's assets, and strategies for recovery from unwanted events and minimising disruption to operations.

Business Continuity Planning

A Business Continuity Plan will be maintained to ensure that the University is able to effectively deal with any issue that may constitute a significant risk to our University's reputation, or may adversely impact on the normal operation of the University.

IT – Resilience and Disaster recovery planning

A primary objective in developing an Information and Communication Technology (ICT) strategy is to ensure the resilience of ICT infrastructure and support systems.

A University ICT Disaster Recovery Plan will be maintained to ensure the continuity of ICT systems availability and protection of data in the event of an unwanted event.

6.3 Compliance

The University has an effective system to ensure the University is aware of and in compliance with legislative, contractual and policy requirements.

7 Training & Communication

The University has clarified roles, responsibilities accountabilities and authorities at all levels of the University. The University Risk Management Framework is embedded in operations through a number of communication, training and support systems, including:

7.1 Training

To ensure that adequate risk management competency levels are achieved and maintained, the University provides regular training courses in the risk management process and its application in the University.

Specific risk management training sessions will be held on an annual basis, aimed at providing an overview of the Risk Management Framework. The training will be facilitated by the Risk Administrator. Additional ad-hoc training will be provided as required.

Instruments providing training on appropriate controls include job descriptions, inductions, policies, procedures, terms of reference, charters, performance planning and review programs, contracts and delegations.

7.2 Communication of responsibilities and Accountabilities

Risk management responsibilities, accountabilities and authorities are set out in:

- The Risk Management Policy;
- Positions descriptions;
- Delegations
- the University's intranet;
- Project documentation;
- Performance planning and review documentation; and
- Risk registers.

7.3 Advice and Support

Risk management responsibilities, accountabilities and authorities are also available on the University's intranet. Advice and support in relation to risk management is available by consulting;

- The Risk Administrator;
- Vice President (Corporate Services); and
- University's Risk Management Framework document.

Appendix 1 –Likelihood Rating: Evaluation Criteria

You will determine how likely it is that Griffith will be exposed to each specific risk after taking into account current internal controls and considering factors such as:

1 Anticipated frequency of occurrence;
2 The external environment (e.g. regulatory, economic, competition, community expectations and market issues);
3 The procedures, tools and skills currently in place; and
4 History of previous events – both Griffith and other providers.

Likelihood rating			
The number of times within a specified period in which a risk may occur either as a consequence of business operations or through failure of operating systems, policies or procedures.			
Rating	**Description**	**Occurrence**	**Probability**
Almost Certain	Expected to occur in most circumstances	Multiple / 12 months	> 80%
Likely	Will probably occur in most circumstances	Once / 12 months	61 – 80%
Possible	Might occur within a 5 year time period	Once / 12 months – 5 years	41 – 60%
Unlikely	Could occur during a specified time period	Once / 5 – 10 years	21 – 40%
Rare	May only occur in exceptional circumstances	Once / > 10 years	< 20%

Appendix 2 – Consequence Rating: evaluation criteria

Business risks are assessed in terms of the consequence of their impact on strategic objectives. Indirect financial consequences such as reputation and management effort are key considerations. In addition financial impacts are also considered. The following table is used to guide the assessment of impact of each identified risk.

Factor of Consequences / categories of risk		Consequence Category				
		Insignificant	Minor	Moderate	Major	Catastrophic
Corporate, Group or Support Service Division Activity	Compliance with Legislation.	Oversight on reporting activity that is under control. No penalty or imprisonment.	Minimal non-compliance to relevant legislation, within Group or Divisions. Breaches by an individual staff member. Penalty may be incurred.	Non-compliance with legislation affecting other Group or Divisions. Possible closure of a course or Research Centre, penalty and/or imprisonment.	Non-compliance with legislation affecting Group or Divisions activities. Closure of several non-core operations. High possibility for individual/corporate penalty and/or imprisonment.	Non-compliance with legislation affecting closure of core Group or Divisions operations or key business activities and/or large penalty (individual/corporate) and/or imprisonment.
	Damage to Reputation.	Minimal adverse publicity in local press. Letters received and printed but no further action taken.	Adverse publicity in local/state press. Letters to the Editors, with follow up comments from the readership or interested parties.	Extended negative local/state, plus national media coverage. Requirement to manage key stakeholders.	Longer-term nation wide and international coverage. Need to increase focus on management of a broader group of stakeholders.	Extended negative national and international wide coverage. Requirement to implement a communication plan for all stakeholders.
	Disruption to Established Routines and operations.	No interruption to service. Inconvenience to localised operations.	Some disruption manageable by altered operational routine. Reduction in operational routine.	Disruption to a number of operational areas/campus. Closure of an operational area/campus for up to one day.	Several key operational areas closed. Disruption to teaching / course schedules or key business activities for up to **one week.**	Disruption to services causing campus closure or key business closure for **more than one week**.
	Financial.	Less than $1M	$1M to $5M.	$5M to $20M.	$20M to $50M.	Greater than $50M.
	General Environmental & Social Impacts.	No lasting detrimental effect on the environment i.e., harm, nuisance, noise, fumes, odour or dust emissions of short-term duration.	Short term, detrimental effect on the environment or social impact, E.g. Minor discharge of pollutants within local neighbourhood.	Serious, discharge of pollutant or source of community annoyance within general neighbourhood that requires remedial action.	Long term detrimental environmental or social impact i.e., chronic &/or significant discharge of pollutant.	Extensive detrimental long term impacts on the environment and community i.e., catastrophic &/or extensive discharge of persistent hazardous pollutant.
	WHS	Incident – no lost time. No injury.	Injury – no lost time. First aid required.	Injury – lost time compensable injury. Medical treatment required.	Fatality or serious injury/stress resulting in hospitalisation.	Multiple fatalities (not natural causes).
	Management Time and Effort	Event absorbed by normal activity.	Management effort required to minimise the impact.	A significant event managed through normal practices.	A critical event, which with proper management can be endured.	Executive Management focus away from day to day key functions for extended periods.
Major Project	Project Budget #	<1% of project budget	1 to 5% of project budget	5 to 10% of project budget	10 to 25% of project budget	>25% of project budget
	Program delays	Little or no delay	Short delay Duration increased >2%	Significant delay Duration increased >10%	Major delay Duration increased >25%	Project halted major delay Duration increased >50%
	Relationship - Managing Contractor	Either party is irritated but no formal complaints	Resolved at working level	Resolved at senior management level	Departmental Head intervention	Legal recourse initiated.

#The consequence category for “Project Budget” may differ according to the overall value of the project itself. Likewise, the criteria for “Program Delays” may also vary depending on the specific Project deadlines.

Appendix 3 – Project Risk Assessment Template

Project Title					**Period:** March 2010	
Project Description / Scope / Background	Please describe the key aspects of the project to clarify the nature , background and scope of the project					
Risk Category Select the risk category being considered	Requirements	Benefits	Schedule	**Budget**	Deliverables	Scope
	Issues	Suppliers	Acceptance	Communication	Resource	Other
Project Risks / Issues - Budget ● Consider a workshop during the "Risk Planning" stage, involving each of the key project stakeholders (project sponsor, manager, team, suppliers, customer), to identify risks ● List the likely risks, which may affect the project, consider each risk category	**Consequence:** ● Quantitative and qualitative ● List all the potential consequences of each risk ● List the consequences in $ terms, to enable better judgement in the decision making process. E.g. The project exceeds the allocated budget by $500k		**Likelihood**: ● List the issues that would affect the likelihood of the risk eventuating		**Consequence Rating:** E.g. **High** -Using the scoring system below, what is the potential impact of the risk	**Likelihood Rating:** E.g. **Medium** -Using the scoring system below, what is the probability of the risk eventuating
					Score: **40**	**Score:** **60**

Current Controls (these are controls in place)	**Future Mitigating Actions**	**Responsibility**	**Action Date**
● List all controls in place that would limit our exposure to the risk occurring (i.e. reduce the likelihood of the risk occurring and reduce the potential consequence of the risk) ● How are these controls enforced (Who, when, how evidenced?)	● List all Preventative actions (reduce possibility of risk occurring) and Contingent (reduce the impact) including estimated completion dates and accountability for each action.	● List responsible persons for each action	● List due date for each action
Priority Risk Rating - *Priority equals average of Likelihood and Consequence scores. After considering the above controls - in place only)*		**50 (ave of above)**	**Moderate**

Matters for consideration	List any other matters for consideration that are relevant to the decision as to whether the University should accept the risk		
Issues for insurers	For Risk Administrator to complete		
Risk decision	Accept, Mitigate, Transfer or Avoid		
Prepared and recommended by:	**xxx**	**Reviewed and endorsed by:**	**Xxx**
	Date		**Date**
Approved	**PVC Administration**		**Date**

Appendix 3 - Project Risk Assessment Template continued

Risk Quantification

Table of Probability (Project Risks only)

Rating	Score	Description
Almost Certain	100	Highly likely to occur as the circumstances which will cause the risk to eventuate are also very likely to be created
Likely	80	Very likely to occur, based on the circumstances of the project
Possible	60	Likely to occur, as it is clear that the risk will probably eventuate
Unlikely	40	Unlikely to occur, based on current information, as the circumstances likely to trigger the risk are also unlikely to occur
Rare	20	Highly unlikely to occur; however, still needs to be monitored as certain circumstances could result in this risk becoming more likely to occur during the project

Table of Consequence (Project Risks only)

Rating	Score	Description
Catastrophic	100	Major impact on the project, e.g. >25% deviation in scope, scheduled end-date or project budget.
Major	80	Significant impact on the project, e.g. 10-25% deviation in scope, scheduled end-date or project budget.
Moderate	60	Measurable impact on the project, e.g. 5-10% deviation in scope, scheduled end-date or project budget.
Minor	40	Minor impact on the project, e.g. <5% deviation in scope, scheduled end-date or project budget.
Insignificant	20	Insignificant impact on the project, It is not possible to measure the impact on the project as it is minimal

Prioritising risks

The purpose of prioritising the risk is to determine the level of action needed for the identified and assessed risks. Establish the priority of each project risk by identifying the probability of the risk eventuating and its impact on the project. The priority score is calculated as follows:

- Priority equals the average “Likelihood” and “Consequence” scores
- This is calculated as Priority = (Likelihood + Consequence) / 2

Table of Management Action (Project risks only)

Priority	Score	Action required	
Extreme	81-100	Immediate Action Required (Executive management)	Assign accountability
High	61-80	Executive Management attention required	Assign accountability
Medium	41-60	Management by specific reviewing and monitoring of procedures (Managers)	Assign accountability
Low	0-40	Manage by routine procedures, unlikely to need specific application of resources (managers and key staff)	Business as usual

Risk Plan

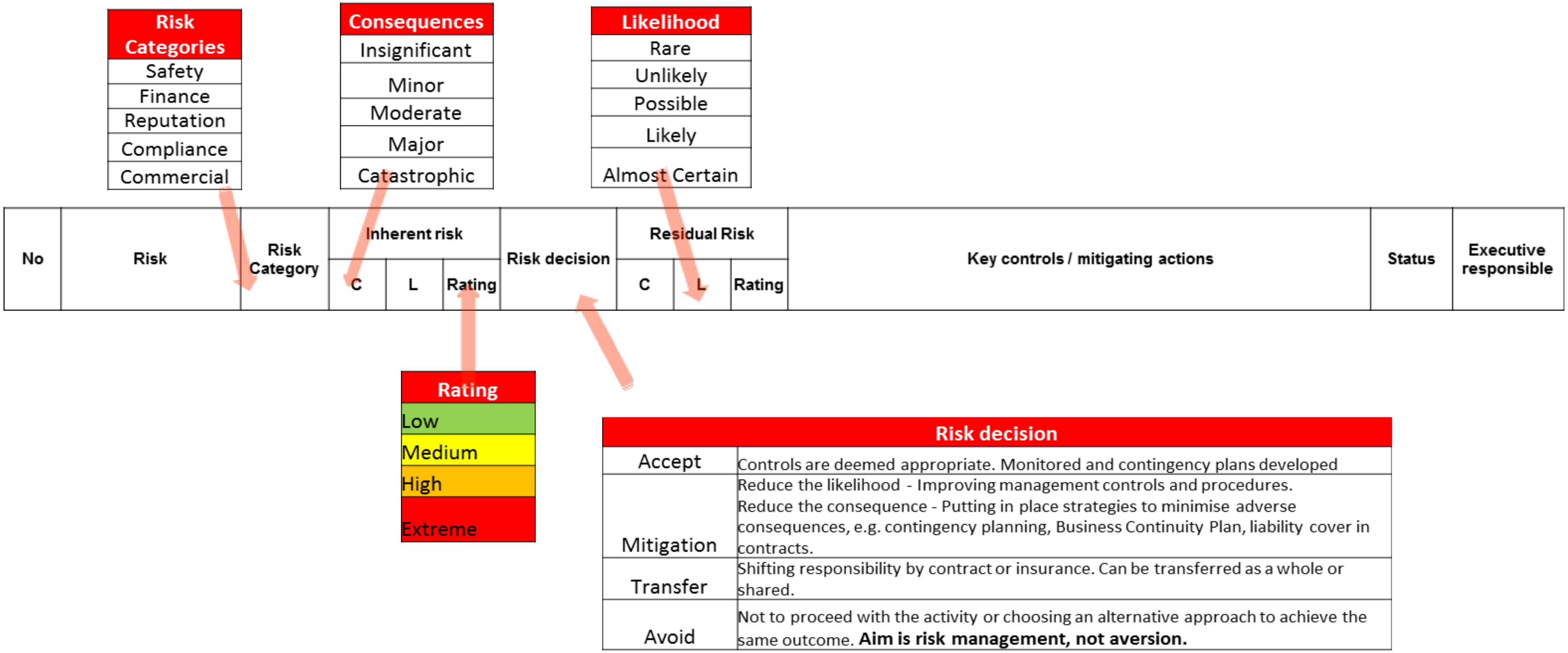
The risk plan includes a set of actions to be taken to avoid, transfer or mitigate each risk, based on the priority of the risk assigned.

For each risk identified and in order of priority, list:

- **Preventative actions** – reduce the likelihood of the risk occurring.
- **Contingent actions** – reduce the consequence should the risk eventuate.

Appendix 4 – Operational Risk Management Plan Template

Example only – not based on actual risks



Risk Categories
Safety
Finance
Reputation
Compliance
Commercial

Consequences
Insignificant
Minor
Moderate
Major
Catastrophic

Likelihood
Rare
Unlikely
Possible
Likely
Almost Certain

No	Risk	Risk Category	Inherent risk			Risk decision	Residual Risk			Key controls / mitigating actions	Status	Executive responsible
			C	L	Rating		C	L	Rating			

Rating
Low
Medium
High
Extreme

Risk decision	
Accept	Controls are deemed appropriate. Monitored and contingency plans developed
Mitigation	Reduce the likelihood - Improving management controls and procedures. Reduce the consequence - Putting in place strategies to minimise adverse consequences, e.g. contingency planning, Business Continuity Plan, liability cover in contracts.
Transfer	Shifting responsibility by contract or insurance. Can be transferred as a whole or shared.
Avoid	Not to proceed with the activity or choosing an alternative approach to achieve the same outcome. **Aim is risk management, not aversion.**

Appendix 5 - Glossary of Risk Management Terms

Consequence
The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Control
Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

Cost
Of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, and goodwill, political and intangible losses.

Contingency
Budget (cost benefit) or time (duration) that may be used in the event of a risk occurrence.

Event
An incident or situation, which occurs in a particular place during a particular interval of time.

Frequency
A measure of the rate of occurrence of an event expressed as the number of occurrences of their event in a given time. See also Likelihood and Probability.

Hazard
A source of potential harm or a situation with a potential to cause loss.

Inherent limitations
Those limitations of all enterprise Risk Management Frameworks. The limitations relate to the limits of human judgment; resource constraints and the need to consider the cost of controls in relation to expected benefits; the reality that breakdowns can occur; and the possibility of management override and collusion.

Inherent risk
High inherent risks that are well controlled may fall out of our field of view if only the residual risk is assessed. The purpose of assessing inherent risk is to ensure that we maintain focus on compliance with controls.

The inherent risk should be considered in the absence of the University added controls.

Likelihood
Used as a qualitative description of probability or frequency of a risk occurring.

Loss
Any negative consequence, financial or otherwise. Can be differentiated as follows;

- **Maximum foreseeable loss**- highest possible loss after considering controls
- **Maximum possible loss** – highest possible loss without considering controls

Monitor
To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.

Probability
The likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes.

Reasonable assurance
The concept that enterprise risk management, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met. This is because of inherent limitations in all Risk Management Frameworks.

Residual risk
The remaining risk after management has taken action to alter the risk's likelihood or consequence.

Risk
The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of consequence and likelihood.

Risk acceptance
An informed decision to accept the consequences and the likelihood of a particular risk.

Risk acceptance criteria
Management's formal establishment of criteria or boundaries designed so that the residual risk does not exceed the selected range of financial and operating outcomes.

Risk analysis

A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk appetite

The level of risk that is acceptable to the board or management. This may be set for the organisation as a whole, for different groups of risks or at an individual risk level.

Risk assessment

The overall process of risk analysis and risk evaluation.

Risk avoidance

An informed decision not to become involved in a risk situation.

Risk evaluation

The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.

Risk identification

The process of determining what can happen, why and how.

Risk Management Framework

The totality of the structures, methodology, procedures and definitions that an organisation has chosen to use to implement its Risk Management Processes.

Risk Management Processes

Processes to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organisation’s objectives.

Risk Plan / Register

The means by which an organisation elects to manage or treat the individual risks. The main categories are to accept the risk; to mitigate it by reducing its consequence or likelihood; to transfer it to another organisation or to avoid the activity creating it.

Risk Register / Risk Management Plan

The summary report of all individual risks within each assessment, which include; risk ratings (inherent, residual and targeted), level of control, risk decision, risk owner and summary of key controls and/or mitigating actions.

Stakeholders

Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.