Risk Management Guidelines

Abstract
These Guidelines supplement the Risk Management Policy.

Dates	Guidelines approved Guidelines take effect Guidelines are due for review (up to five years)	29/09/2011 29/09/2011 10/2016
	Guidelines amendment approved Guidelines amendment takes effect	11/12/2014 22/07/2015
Approved by	Deputy Vice-Chancellor (Corporate Services)	
	Latest amendment: Director, Governance Support Unit (see change history for details)	

Contents

1. Purpose

These Guidelines supplement the Risk Management Policy. The Policy and Guidelines describe UTS's approach to risk management. The Guidelines provide further detail on how risk management is to be embedded into UTS business processes and functions via key approval processes, review processes and controls.

2. Scope

These Guidelines apply to all staff at UTS and to emeritus professors, honorary appointees and contractors.

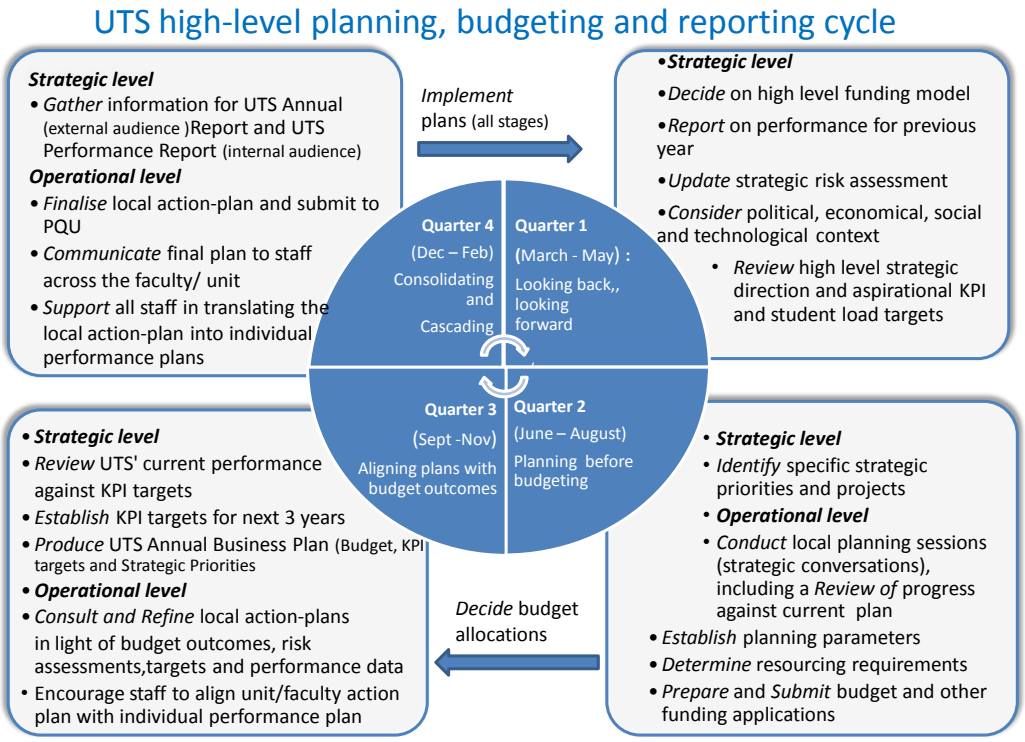
3. Definitions

Risk owner is the person or entity with the accountability and authority to manage a risk.

All other terms used within these Guidelines are defined in the Risk Management Policy.

4. Risk management at UTS

Risk management is embedded in the UTS Planning and Improvement Framework and the annual planning, budgeting and reporting cycle (depicted below).



The risk management elements in the cycle are described below.

4.1 Strategic risk assessment

The Deputy Vice-Chancellor (Resources), in consultation with the Senior Executive and senior staff where appropriate, will prepare an annual risk assessment of key strategic risks posed to UTS. The strategic risk assessment will focus on UTS's external context, strategic objectives and major UTS-wide risks. The strategic risk assessment will be monitored and reviewed by the Audit and Risk Committee and UTS Council. The risk assessment will be prepared annually in Quarter 4 for the following year and reviewed every 6 months. The strategic risk assessment will be used where appropriate, to inform university functional plans and operational risk assessments (see parts 4.2 and 4.3 below).

4.2 University functional plans

University functional plans will address risks to key university-wide functions. These might include (but are not limited to):

- Environment, Health and Safety Plan
- Long Term Finance Plan

- IT Security and IT Disaster Recovery
- Business Continuity Planning
- Records Management, and
- major project plans (eg buildings, IT).

4.3 Operational risk management

Operational risk management by Faculties and Units will include:

- operational risk assessments, and
- maintenance of local risk registers resulting from these risk assessments.

Operational risk assessments will be conducted in accordance with the UTS risk management process (see Part 5 below) and will be reviewed annually during the planning, budgeting and reporting cycle and used to inform local action plans. Operational risk assessments will also be reviewed following significant and relevant changes to the external or internal environment.

Based on these operational risk assessments, each Faculty and Unit will maintain a local risk register including:

- all risks identified in the area
- the outcome of the risk assessment for each of the risks
- the risk treatments that have been selected, and
- the risk owners who are responsible for ensuring that controls, further actions and specific monitoring of risks are carried out.

A template for UTS local risk registers is included as Appendix 1.

4.4 University operational risk registers

The Office of the Deputy Vice-Chancellor (Resources) will maintain a university operational risk register collating the risk registers derived from the risk assessments of each Faculty and Unit. The Office of the Deputy Vice-Chancellor (Resources) will maintain copies of operational risk registers for all faculties and units, and will review these annually to identify emerging trends and common risks across the university.

4.5 Risk appetite document

UTS will maintain a risk appetite document which sets out criteria against which the significance of risks may be evaluated. The risk appetite document will be reviewed every 2 years. The current UTS risk appetite document is included as Appendix 2.

4.6 Review of risk management

UTS will undertake continuous monitoring and review of risk management. During the planning, budgeting and reporting cycle, each Unit and Faculty will review their performance against their current local action plan and review the impact of risk on the achievement of their objectives. This review will feed into the annual review of operational risk assessments and development of local action plans for the following year (see clause 4.3 above).

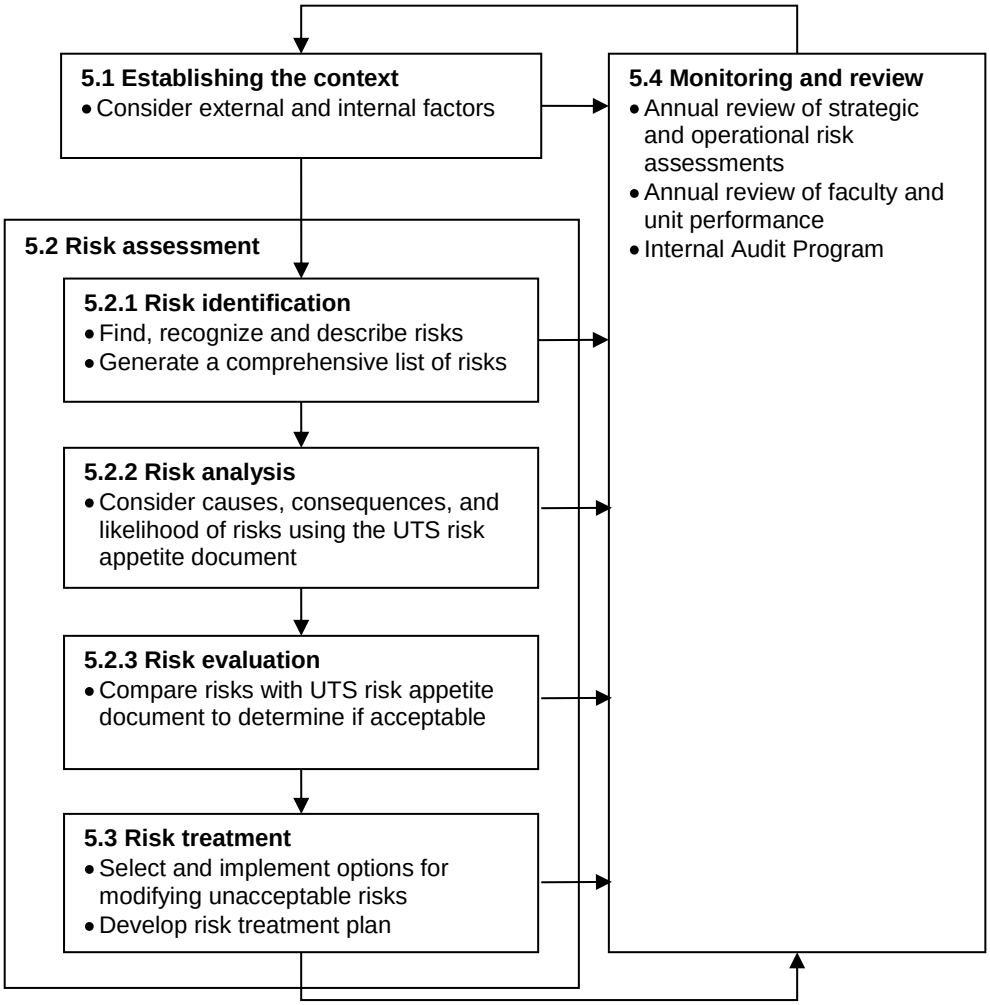
UTS will also undertake a structured internal audit program to assist with monitoring and review of risk. Areas to be audited will draw upon the strategic risk assessment

and operational risk assessments. Internal audit plans will be presented to the Audit and Risk Committee for review.

In addition, UTS undertakes major reviews of key areas identified through ongoing performance reporting and planning processes.

5. Risk management process

The risk management process to be adopted at UTS appears below. Communication and consultation with external and internal stakeholders should take place as appropriate at all stages of the risk management process.



5.1 Establishing the context

UTS's objectives and external and internal factors need to be considered when managing risk.

UTS's external context may include:

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local. This might include factors such as government policies

around higher education; economic trends like the Global Financial Crisis; new legislative or regulatory instruments such as the Government Information (Public Access) Act 2009 (NSW); and/or the activities of other universities, such as the development of linkages between vocational and higher education.
- key drivers and trends having impact on UTS's objectives. These might include government priorities, such as widening participation in higher education; or changes in the number of international students choosing to study in Australia; and
- relationships with, and perceptions and values of external stakeholders. These might include governments (both Australian and overseas); potential students; industry and/or the local community.

UTS's internal context may include its:

- governance, organisational structure, roles and accountabilities. This might include the university's organisational structure and responsibilities under the University of Technology, Sydney, Act 1989 (NSW) and UTS policy;
- university policies, objectives (including those in the UTS Strategic Plan), and the strategies that are in place to achieve them (as detailed in Strategy Implementation Plans and local area Action Plans);
- capabilities, understood in terms of resources and knowledge (including capital or funding, time, people, processes, systems and technologies);
- information systems, information flows and decision-making processes (both formal and informal). These might include formal systems for information sharing such as CASS, BI and PACE; informal communication channels between areas; and processes established under UTS policies;
- relationships with, and perceptions and values of, internal stakeholders. These might include staff, students and members of Council;
- culture;
- standards, guidelines and models; and
- form and extent of contractual relationships. These might include contracts with suppliers, staff, collaborators (including members of industry and other universities) and external funding bodies.

5.2 Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

5.2.1 Risk identification

Risk identification is the process of finding, recognizing and describing risks. This involves the identification of sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on events that might create, enhance, prevent, degrade, accelerate or delay the achievement of UTS's objectives.

5.2.2 Risk analysis

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. These factors should be categorised in accordance with the UTS risk appetite

document. Risk analysis should take into account any existing controls and their effectiveness and efficiency. Any uncertainty or limitations of risk analysis should be acknowledged.

5.2.3 Risk evaluation

Risk evaluation involves comparing the level of risk found during the risk analysis with the UTS risk appetite document to determine whether the risk and/or its magnitude are acceptable or tolerable to UTS. If the risk is not acceptable or tolerable, a risk treatment will need to be considered.

5.3 Risk treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- taking or increasing risk in order to pursue an opportunity
- removing the risk source
- changing the likelihood of the risk
- changing the consequences
- sharing the risk with another party or parties (including contracts and risk financing), and/or
- retaining the risk by informed decision.

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment.

Once risk treatment(s) have been selected, a risk treatment plan should be developed which documents how the chosen treatment options will be implemented. Treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained
- those who are accountable for approving the plan and those responsible for implementing the plan
- proposed actions
- resource requirements including contingencies
- performance measures and constraints
- reporting and monitoring requirements, and
- timing and schedule.

Risk treatment involves a cyclical process of:

- assessing a risk treatment
- deciding whether residual risk levels are tolerable
- if not tolerable, generating a new risk treatment, and
- assessing the effectiveness of that treatment.

Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk.

5.4 Monitoring and review

UTS will undertake continuous monitoring and review of the risk management process to:

- ensure controls are effective and efficient in both design and operation
- obtain further information to improve risk assessment
- analyse and learn lessons from events (including near-misses), changes, trends, successes and failures
- detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities, and
- identify emerging risks.

The success of the UTS risk management process will be assessed against the following criteria:

- risk does not prevent UTS from achieving its strategic objectives in accordance with the *UTS Strategic Plan 2009–2018*
- opportunities and threats are effectively identified before they eventuate
- UTS complies with relevant legal and regulatory requirements
- available resources are effectively allocated and used to treat risk, and
- appropriate risk treatments are in place to reduce all identified risks to acceptable levels (consistent with the UTS risk appetite document).

6. Roles and responsibilities

Accountable Officer: the Deputy Vice-Chancellor (Resources) has primary oversight of the operation of these guidelines. They will also provide reports to the Vice-Chancellor and the Audit and Risk Committee on the status of risk management implementation and effectiveness across the University.

Implementation Officer: the Executive Officer to the Deputy Vice-Chancellor (Resources) is the primary point of contact for advice on the implementation and administration of these guidelines.

UTS Council and Council committees: Council will oversee risk management and risk assessment across UTS, on advice from the Audit and Risk Committee, the Vice-Chancellor and other Council Committees within their terms of reference.

More specifically Council will:

- Assess and approve the Risk Management Policy.
- Monitor key risks and where applicable approve major decisions affecting the University risk register/exposure.
- Approve the risk appetite or agreed level of exposure for the University on advice from the Vice-Chancellor.

Council Committees and Groups (as listed in the University's Calendar), including the Academic Board, will advise Council on the management of risks within their areas as per their terms of reference.

Audit and Risk Committee of UTS Council: the Committee is to monitor the effectiveness of risk management at UTS and the implementation of the policy and assist in its review.

Specifically the Committee will:

- Ensure that audit plans are adequate to give assurance that risks are well managed.
- Advise Council annually on risk management effectiveness and the risk appetite or agreed level of exposure for the University.

Vice-Chancellor: The Vice-Chancellor will ensure that a risk management system is established, implemented and maintained in accordance with the Policy and these Guidelines. The Vice-Chancellor has specifically delegated this responsibility to the Deputy Vice-Chancellor (Resources). The Vice-Chancellor will provide timely and adequate information to Council on the status of the University's key risks. The Vice-Chancellor through the Senior Executive will propose the tolerance of the University in accepting certain risks.

Provost and Deputy Vice-Chancellors: are responsible for overseeing the operation of these Guidelines and the management of risks within their areas of responsibility and will ensure risk management is embedded into the key controls and approval processes of all major business processes and functions within their respective areas of responsibility. They are required to own all risks within their area of responsibility and are responsible for ensuring Deans and Directors collectively fulfil their risk management responsibilities in their respective areas. They will also ensure that risk registers are maintained by each Faculty and Unit within their areas of responsibility.

They will evaluate and ensure prioritised and effective action is taken to mitigate the key risks faced by the University and ensure that this prioritisation process and resulting actions are incorporated into the University's annual planning and budget process.

Deans and Directors: are responsible for overseeing the operation of these Guidelines and the management of risks within their areas of responsibility. Deans and Directors are required to:

- Own all risks within their area of responsibility.
- Ensure appropriate processes are in place within their areas to ensure that all risks impacting on achieving objectives or realising opportunities are identified, assessed, managed and reviewed on a regular basis within agreed tolerance levels.
- Champion risk management and ensure risk awareness is promoted within their area.
- Update relevant risk registers.

- Review and approve the risks and responses identified by managers in their area.
- Ensure that actions on risks impacting multiple areas of responsibility are agreed, co-ordinated and implemented by appropriate staff members.
- Ensure the cost-effective management of risk.
- Identify any issue for consideration for inclusion or action as a University-level risk.
- Inform Senior Executive of significant changes to key risks which impact upon the University.
- Consider risk as a part of their decision-making process.
- Ensure effective risk management for all projects in their domain
- Report to the Senior Executive as required on the effectiveness of their risk management systems and specific identification of and actions on significant risks.
- Ensure that less significant risks are being appropriately managed, and have effective controls in place.
- Nominate a Risk Coordinator to implement and manage risk processes in the area.

Risk Coordinators: will be key administrators or academics, nominated by each Dean and Director, who will undertake the role of 'in house' risk practitioners. In Faculties, the Risk Coordinator is likely to be the Faculty Manager. Risk Coordinators have responsibility to ensure:

- Appropriate risk management processes are supported and administered within their area.
- The local risk register is updated following the review of the key risks.
- Necessary risk reporting and supporting documentation is prepared.

Risk Coordinators are also expected to:

- Act as a knowledge base within their area, ie to be a point of contact for colleagues with questions on risk management.
- Provide feedback on risk related issues and participate in periodic advisory panels.

Controlled and associated entities: Heads of UTS controlled entities and associated entities operating under the name or legal status of University will be responsible to their respective Boards for the implementation and maintenance of appropriate risk management processes; and will provide reports to the Vice-Chancellor as directed on the implementation of these risk management processes.

Supervisors, Project Managers and Contract Managers: are expected to:

- understand the risk management framework in place at UTS
- adopt a risk-based approach in their management
- lead by example in their behaviour in the workplace, and
- ensure operational risk assessments are conducted for all key risks in their area.

Performance and commitment in these areas will form part of the performance review and planning processes.

All staff: are required to take responsibility for ensuring the integrity of UTS's management and administrative practices, including by identifying risks in their area and contributing to the implementation of risk treatments.

7. Related documents

AS/NZS ISO 31000:2009 Risk management — Principles and guidelines

Risk Management Policy

UTS Planning and Improvement Framework

8. Version control and change history

Effective date	Version	Approved by, resolution no. (approval date)	Amendment
29/09/2011	1	Deputy Vice-Chancellor (Corporate Services) (29/09/2011)	New Guidelines.
22/07/2015	1.1	Director, Governance Support Unit (GSU) (11/12/2014)	Changes (approved under Delegation 3.17) to implement 2014 Senior Executive restructure.

Appendix 1 — Local risk register template

Unit/Faculty: _____

Risk title	Risk description and impact	Initial risk rating (before risk treatment)			Risk treatment plan	Residual risk rating (after risk treatment)			Risk owner
		Risk likelihood rating	Risk consequence rating	Risk rating		Risk likelihood rating	Risk consequence rating	Risk rating	

Risk Register Template (Microsoft Word document)

Appendix 2 — Risk appetite document

This document sets out criteria against which the significance of risks may be evaluated. During a risk evaluation (see cl. 5.2.3), the level of risk found during a risk analysis should be compared with this document to determine whether the risk and/or its magnitude are acceptable or tolerable to UTS. If the risk is not acceptable or tolerable, a risk treatment will need to be considered.

This document includes four tables which should be used to assess each risk. These tables include:

- Table 1 — Risk Likelihood Ratings
  This table is used to determine what the likelihood is that a risk may occur. The likelihood will be affected by the effectiveness of controls already in place, if any.
- Table 2 — Risk Consequence Ratings
  This table is used to determine what the impact will be to the University if the risk transpires. A risk might have consequences for a number of risk categories. In that case, the category with the highest impact is used to map the risk on Table 3.
- Table 3 — Risk Matrix
  The readings on Tables 1 and 2 (above) are used to map the risk on the risk matrix.
- Table 4 — Escalation of Findings
  Using the reading on the Table 3 risk matrix, Table 4 is used to determine what the level of escalation for the risk should be and how the risk's treatment plan should be prioritised compared to those for other risks.

Table 1 — Risk Likelihood Ratings

Rating Description	Likelihood of Occurrence
Almost Certain	The risk is expected to occur in most circumstances, say many times a month or already is happening.
Likely	The risk will probably occur in most circumstances say once a year.
Moderate	The risk should occur at some time, say once in three years.
Unlikely	The risk may occur at some time, say once in ten years.
Rare	The risk may occur only in exceptional circumstances.

Table 2 — Risk Consequence Ratings

Rating Description	Financial	Health and Safety	Business Interruption (depending on type and timing)	Reputation and Image	Legal Liabilities
Catastrophic	Threatens University Viability; Above $40m or >6% of operational budget	Single or Multiple Deaths	Business interruption greater than 6 weeks	Reputation of the University affected nationally and internationally; front page news. Demand for Government inquiry.	Breaches of legislation; (eg Financial management act, work cover, EPA, trade practices, corporations law) Found Guilty — Multiple Jail sentences; Fines/Claims > $40m
Major	Above $5m–$40m or 6% of operational budget	Intensive Care Hospital	Business interruption between 4–6 weeks	Embarrassment for the University; including adverse media coverage.	Breach of legislation; Found Guilty — Single jail sentence; Fines/Claims between $5m–$40m
Moderate	Above $250,000–$5m or 2% of operational budget	Injury/hospital	Business interruption between 2–4 weeks	Student, staff and/or community concern; heavy local media coverage.	Breach of legislation; Found Guilty — Fines/Claims between $250,000–$5m
Minor	Above $50,000–$250,000 or 1% of operational budget	Injury/ treatment	Business interruption between 1–2 weeks	Issue raised by students; staff and/or local press	Breach of legislation; Found Guilty - Fines/Claims between $50,000–$250,000
Insignificant	Up to $50,000 or 0,05% of operational budget	First Aid	Business interruption up to 1 week	Issue resolved promptly by day-to-day management process	Breach of legislation; Found Guilty — Fines/Claims up to $50,000

Table 3 — Risk Matrix

Likelihood (Table 1)						
	Almost Certain 5	6 High	7 High	8 Critical	9 Critical	10 Critical
	Likely 4	5 Moderate	6 High	7 High	8 Critical	9 Critical
	Moderate 3	4 Moderate	5 Moderate	6 High	7 High	8 Critical
	Unlikely 2	3 Low	4 Moderate	5 Moderate	6 High	7 High
	Rare 1	2 Low	3 Low	4 Moderate	5 Moderate	6 High
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
		Consequence (Table 2)				

Table 4 — Escalation of Findings

Risk Ranking	Description
Critical Risk (8–10)	Risks that significantly exceed the risk tolerance and need urgent and immediate attention. Needs active management, planning and decision making at Senior Executive levels of management within three months to reduce risk to acceptable levels.
High Risk (6–7)	Risks that exceed the risk acceptance threshold and require proactive management. Senior management attention and action needed within three to six months to reduce risk to acceptable levels. Existing good controls should be maintained and any additional risk treatment actions required should be defined and implemented.
Moderate Risk (4–5)	Risks that lie on the risk acceptance threshold and require active monitoring. Line management responsibility must be defined to ensure risks are being monitored and managed effectively. Risk should be monitored in conjunction with a review and improvement of existing controls.
Low Risk (2–3)	Risks that are below the acceptance threshold and do not require active management. No major concern and can be managed by routine controls or procedures. Improvements could be implemented depending on resource availability. Significant management effort should not be directed towards these risks.