

THE UNIVERSITY OF NEW
ENGLAND

RISK MANAGEMENT POLICY
GUIDELINES

UNE

THE UNIVERSITY
OF NEW ENGLAND

University of New England, Armidale NSW 2351
Email: insurance@une.edu.au
Phone: 02 67733495 or 02 67732124



The University of New England Risk Management Guidelines

1.	GENERAL INTRODUCTION.....	2
1.1	INTRODUCTION TO RISK MANAGEMENT	3
1.1.1	What is Risk ?	3
1.1.2	Why Should We Manage Risk?	3
1.1.3	How Can We Manage Risk ?	4
1.1.4	Training Processes	4
2.	RISK MANAGEMENT PROCESS	5
2.1	GUIDING PRINCIPLES.....	5
2.2	PROCESS OVERVIEW.....	5
2.3	Step I - ESTABLISH THE CONTEXT - UNDERSTAND THE BUSINESS AND CLARIFY OBJECTIVES.....	6
2.3.1	Tools that help us understand the business	6
2.4	Step 2 - IDENTIFY RISKS	6
2.4.1	Risk Identification Tools	6
2.5	Step 3 - ASSESS RISKS	7
2.5.1	Risk Assessment Tools Assessment Matrices	8
	4 Likely.....	9
	4 Major	9
2.6	Step 4 - RESPOND TO RISKS (Controls).....	10
2.7	Step 5- MONITOR AND REVIEW	14
2.8	Step 6- COMMUNICATION, CONSULTATION & REPORTING	14
2.8.1	Risk Reporting Tools	15
3	RISK MANAGEMENT FRAMEWORK.....	16
3.1	STRUCTURE.....	16
3.1.1	Risk Management Responsibilities.....	23
3.1.2	Risk Management Administration	27
3.1.3	External Requirements.....	28
3.2	RISK REGISTER REPORTS.....	29
3.3	RISK CATEGORISATION	31
3.4	MANAGEMENT SYSTEM RISK.....	31
3.5	CONSOLIDATION OF RISK.....	31
3.6	ASSURANCE TOOLS.....	31
4	GLOSSARY	33
	REFERENCES:.....	35
	ACKNOWLEDGEMENTS.....	35
	Appendix 1	36
	RISK MANAGEMENT POLICY	36
	Policy (As approved by the Vice-Chancellor 14/12/2004).....	36
	Commitment.....	36
	Responsibilities.....	36
	Appendix 2	38

1. GENERAL INTRODUCTION

The University of New England Risk Management Guidelines have been developed to meet two primary objectives:

1. It aims to provide consistency to business risk management practices throughout the University. In doing so it outlines a methodology, based upon qualitative risk assessment, which should be applied to the assessment of any risks of a general nature. This information is included in Section 2 — Risk Management Process.

2. The plan also outlines the **Corporate Assurance Framework**. The University framework has been designed to provide assurance that all key risks within the business are being identified and managed appropriately and to ensure the University, including management and the Council are aware of key business risks. This information is included in Section 3 — Risk Management Framework.

Purpose

The purpose for risk management is not to eliminate risk completely, but to provide a structural framework to effectively manage risks that may apply in all areas of the University. To achieve this, risk management must be an integral function of all managers within the University. All staff are recognised as having a significant role in the management of risk. This role may range from initially identifying and reporting risks associated with their own jobs to more active participation in the risk management process.

In summary, University activities must be undertaken in line with an understanding of risk and knowledge of the potential for unforeseen events to have an impact on the institution and its reputation.

1.1 INTRODUCTION TO RISK MANAGEMENT

1.1.1 What is Risk ?

Risk is defined as ‘the chance of something happening that will have an impact upon the objectives of the organisation’.

This definition highlights risk as an uncertainty of outcome. This uncertainty can relate to either a threat or an opportunity and risk management can relate to how we ensure threats do not lead to negative consequences and how we ensure opportunities are realised. In the case of a threat, we can take action to reduce this uncertainty by either reducing the likelihood that the event will happen and/or limiting the consequences that arise as a result.

1.1.2 Why Should We Manage Risk?

Risk means different things to different people although there is common ground based on the notion of uncertainty. The management of risk (risk management) has developed significantly in recent years.

The rate of change, increasing complexity of regulation, changes in technology, increasing expectations of customers (e.g. stakeholders, students), increasing accountability, funding constraints, increased involvement with other organisations and globalization. The consequent business risks that the University faces are becoming more complex and substantial. These factors demand a more structured approach to managing risk.

Risk Management is the systematic and ongoing process of risk identification, assessment, treatment and monitoring. It can be applied at any level of the University including strategic, operational and at project level. It is not solely about limiting risk but rather about fully appreciating and recognising the risks we carry and balancing risk and reward in an informed manner.

Properly applied, risk management should:

- improve the likelihood that University objectives will be achieved
- reduce the likelihood of unwanted ‘surprises’
- help the University maximise opportunities
- provide information to support University decision making
- provide a basis for effective resource allocation
- help the University meet compliance & governance requirements
- improve overall stakeholder confidence in the University

The overarching objective of risk management is to ensure that risk identification, assessment and management occurs continuously in accordance with changes in the internal and external environment and that the University has processes in place to enable it to provide assurance to University management, the Council and the external community that processes are effective in controlling risk.

1.1.3 How Can We Manage Risk ?

The University already has rigorous planning processes which include Strategic, Operational and Management Plans underpinned by an annual Cycle of Planning and Accountability. Inherent within the various plans is consideration of the various risks facing the University and our co-ordinated response(s) to these risks. However, to help ensure that important risks are not overlooked a rigorous and systematic approach to identifying and adequately managing risks at strategic, structural and operational levels is essential.

Risk management is an ever-present management responsibility. However, this does not mean that it happens automatically. All staff are required to be conversant with risk management concepts and practices and be able to utilise and demonstrate application of these within their areas of control. Staff familiar with the work undertaken in specific areas are well placed to recognise risks in their own areas and recommend suitable strategies for controlling the impact of those risks.

Risk management does not imply completely avoiding risk as this requires the cessation of all activities that contribute to an organisations' function. Effective risk management permits the balancing of the benefit of each activity against its inherent risk.

This plan explains a standard process for management of risk. It should be used throughout the University to ensure all risks are being managed effectively and consistently across the University. The plan also describes the Corporate Business Risk Management assurance framework. This framework, which operates alongside individual work areas assurance systems, provides information to assure the University, including the Council and other stakeholders, that effective risk management systems and processes are in place across the organisation and that all key risks are being managed effectively and efficiently.

1.1.4 Training Processes

For the past three years the University has provided risk management introductory workshops to all Directorates, Faculties, University Council and its Committees, and some University committees and associated entities.

More formal training has been facilitated by ODU, including risk management introductory sessions, basic training for '*KnowRisk*' users, and risk management co-ordinators and more advanced training for '*KnowRisk*' users.

ODU is developing documented programs of training, including advanced training and assesses competence for user access to the "*KnowRisk*" database.(Ref. Role of ODU pp)

2. RISK MANAGEMENT PROCESS

The University has opted for a qualitative process of risk assessment over a quantitative process. In doing so, those areas or projects which would benefit from using quantitative data, are not prevented from doing so.

A qualitative process is sufficiently accurate for the University's purposes and is more intuitive than an actuarial approach. The qualitative process is based on a 'sense of' or 'best guess' likelihood and impact assessment, compared with a quantitative process which depends on statistical or concrete data.

2.1 GUIDING PRINCIPLES

- Risk will be managed at the lowest and most appropriate level of the organisation
- Everyone in the organization is responsible for managing risk
- Every manager is a risk manager
- Accountability for risk management parallels the organisation structure unless a position description makes special provision
- A qualitative or subjective assessment of risk will be considered adequate for most management purposes
- Risks will be reviewed regularly and the risk process reviewed annually
- Risk management is part of management and not additional to or separate from management
- Risk management is an active process not an administrative task

2.2 PROCESS OVERVIEW

The University's Risk Management process is closely aligned to AS/NZS 4360 Standard 2004 and is broken down into the following steps:

- Step 1 - Establish the context - Understand the business and clarify objectives
- Step 2 - Identify Risks
- Step 3 - Assess Risks (without controls) = Inherent risk
- Step 4 - Respond to Risk - Including assignment of responsibility for actions (Controls)
- Step 5 - Manage & Review - Steps 5 and 6 take place throughout the risk cycle.
- Step 6 - Communicate, Consult & Report

2.3 Step I - ESTABLISH THE CONTEXT - UNDERSTAND THE BUSINESS AND CLARIFY OBJECTIVES

Risk Management takes place in the context of the environment (Internal/External) in which the University operates and within its wider goals and objectives. Therefore the objective of this step is to establish an understanding of the business environment in which the risks will be identified and assessed.

Since risks are the events or actions that will influence the achievement of business objectives it is essential that these business objectives are clear before the risk identification process commences. If business objectives change, risks should be reviewed. Business objectives should be an integral part of the business plan for each area. Key risks to these objectives should also be highlighted in the business plan.

2.3.1 Tools that help us understand the business

There are a number of tools that can help us develop our understanding of the risks facing the University:

- Personal experience, corporate history, incident and events
- Audits or physical inspections
- Brainstorming
- Survey questionnaires
- Expert judgment
- SWOT Analysis *

* A SWOT analysis is a convenient way to develop a better understanding of the business through a structured discussion around the internal Strengths and Weaknesses and external Opportunities and Threats to an organisation or business area.

2.4 Step 2 - IDENTIFY RISKS

The objective of this step is to identify a suitably comprehensive set of risks that have the potential to materially affect the University's capability to meet its objectives. A risk then is anything which limits or better enables us to achieve the business outcomes of the University and/or its component parts.

Risk can relate to any aspect of the University and identification should include all risks whether or not they are under the direct control of the University and whether or not they are currently being managed.

2.4.1 Risk Identification Tools

There are a number of risk identification methods. Depending on the situation the following may be useful:

Process Based

A process map of the area under review is created. The main risks associated with each process are then identified.

Outcome/Objective Based

Business objectives provide the basis for risk identification (i.e. each business objective is analysed to identify the risks associated with the achievement of this objective).

Checklists

Common areas of risk are detailed in AS/NZS Risk Management Standard 4360 Standard 2004.

Experience based

Where similar opportunities/operations/projects have been undertaken in the past or where similar issues and situations have arisen, it is helpful to examine the risks that were identified at the time. Where internal capability is limited, reference should be made to peer groups and/or experts in the particular field. The '*KnowRisk*' database can be particularly useful in sharing this type of corporate learning.

Brainstorming/Workshopping

Brainstorming is the free-association of ideas from a group. Brainstorming can be a useful tool to gather large amounts of data by grouping risk sets based on the natural relationship between each item. It is a creative rather than a logical process and is particularly useful when there are many issues and thoughts.

Templates

Templates will be developed and added to the '*KnowRisk*' database to provide risk managers with non exclusive core risks which might be expected for recurring activities, for example, projects or events. These templates will comprise risk modules of Risk, Consequences, and Controls which can then be attached to the relevant profile (position in the University) and assessed and managed in context.

Templates and use of other risk modules will allow all risk managers within the University to benefit from the efforts of others in the documentation of their management of risk.

2.5 Step 3 - ASSESS RISKS

The objective of risk assessment is to differentiate minor acceptable risks from major risks that require active management and to provide data to assist in the evaluation and treatment of risks.

Determine the existing controls -

The risk assessment involves consideration of the sources of risk, the likelihood, and the impact/consequences that may occur, assessed in the context of the control environment.

Controls include structures, capability, processes, policies and values, as well as the more traditional controls such as systems, procedures and authorities.

Controls can affect the likelihood of a risk eventuating, as well as the extent of the consequences that may result. Therefore, before we can assess a risk we need to assess the strengths and weaknesses of the controls. Controls should be fit for purpose, i.e. we should be neither under-controlling nor over-controlling. The objective is not to eliminate all risk, but to ensure that risk is maintained at an acceptable level in a cost effective manner.

When we assess risks without the mitigating effect of any controls (where it is assumed controls are either not present or have failed), this is known as the *inherent risk*.

This term is useful when we want to get an appreciation of the worst-case scenario. In practice this can be hard to assess since we rarely operate without any controls and it can be difficult to strip back all controls to allow meaningful assessment.

When we assess risk with controls this is referred to as the *residual risk*, i.e. the risk that remains after the mitigating effect of controls currently in place. This is the state of risk that is used most often and provides us with an assessment of where we stand at the moment. Where no controls currently exist they will need to be developed. This may require development of policy and procedure or adoption/modification of other best practices. It should be noted that the residual risk is not altered until such time as new controls are implemented. However, it is useful in the management process to reassess risks with proposed controls to gauge the residual rating so time and resources are not wasted on development of inadequate or ineffective controls.

Assessing the Risk

Armed with an understanding of the business environment and the effectiveness of the control environment, the risk likelihood and consequence can be assessed. Likelihood (the chance that the risk may be realised) and impact/consequence (if the risk is realised) are assessed against the University Risk Matrix to give an overall risk rating (see Figure 1).

2.5.1 Risk Assessment Tools Assessment Matrices

To provide a structured and consistent way of rating risks and to give risk relativity across the organisation, the following matrix should be used to assess likelihood, impact/consequence and calculate risk rating.

UNIVERSITY RISK MATRIX (Figure1)

Impact/(Consequence)	Likelihood				
	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
1 Insignificant	1 Negligible	2 Negligible	3 Low	4 Low	5 Tolerable
2 Minor	2 Negligible	4 Low	6 Tolerable	8 Tolerable	10 Tolerable
3 Moderate	3 Low	6 Tolerable	9 Tolerable	12 High	15 Extreme
4 Major	4 Tolerable	8 Tolerable	12 Extreme	16 Extreme	20 Extreme
5 Catastrophic	5 High	10 High	15 Extreme	20 Extreme	25 Extreme

See below for risk rankings (E, H,T, L &N) — *University Risk Matrix*

The University Risk Matrix has been designed to provide relativity of risk across all risk areas. While the core matrix fits all, some likelihood descriptors are more useful in some areas than others. In the assessment of business risk it is recommended that predictive headings (likely, possible etc) be used. While there is a large component of subjectivity in the predictive approach, this is accepted as a natural part of business risk assessment, something preferable to turning assessment into an absolute science (although you may need a greater level of accuracy in your economic evaluations). Figure 2 provides guidance on recommended quantitative measures for impact/consequence for use with strategic, operational and routine activities.

Risk Ranking

Risks are ranked according to the risk rating (catastrophic, major, moderate, minor, insignificant) in the first instance. If greater definition is required each risk matrix square has a corresponding number, which can be used to rank risks in terms of on a scale from:

- Extreme (E) – A description of the control description & its status must be included (e.g. new, existing, in progress)
- High Risk (H) - A description of the control description & its status must be included (e.g. new, existing, in progress)
- Tolerable (T) – managed within Faculty/School/Department
- Low (L) - managed within Faculty/School/Department
- Negligible (N) - managed within Faculty/School/Department

Measures of Likelihood of Occurrence (Figure 2)

Rare - Likely to occur only in very exceptional circumstances

Unlikely - Could occur at some time

Possible - May occur at some time

Likely - Will probably occur at least once

Almost Certain - Is expected to occur in most circumstances

Measures of Impact/Consequence

Insignificant -	For example, No personal injury, no adverse media attention, financial cost under \$2,000
Minor -	For example, Minor personal injury, adverse local media coverage only, financial cost between \$2,000 and \$50,000
Moderate -	For example, Serious personal injury, adverse capital city media coverage, financial cost between \$50,000 and \$250,000
Major -	For example, Multiple serious personal injury, adverse and extended national media coverage, financial cost between \$250,000 and \$1m
Catastrophic -	For example, Fatality(ies), government intervention, financial cost of more than \$1m

Other useful measures are invited e.g. Academic etc.

2.6 Step 4 - RESPOND TO RISKS (Controls)

The objective of the 'respond to risk' step is to identify and implement the most appropriate risk treatment options to arrive at the residual risk. This will involve identifying the full range of options, assessing these options, preparing risk treatment plans and implementing them. An important step in the treatment plans is the assignment of responsibility for actions. Not all risks will require treatment. This may be because the level of risk is acceptable or there may be no economically viable treatment options.

When assessing treatment options it is important to remember that options can address both the cause and the impact/consequence. There is sometimes a bias on treating the cause; however, it is just as important to consider ways of reducing the impact/consequence. A way to reduce risk impact/consequences is to perform business continuity and contingency planning and undertaking a cost benefit analysis. Responses to risk will utilise some or all of the following strategy/options — TAKE, TREAT, TRANSFER or TERMINATE. (Figure 3)

Take or Accept

To some extent, there is a degree of TAKE in the response to most significant risks. Many cannot be avoided, and few can be practically and affordably reduced to zero likelihood/zero impact. Risks which are inherent to the University's operations will often be accepted, particularly those which are reasonably predictable. Intentionally taking risk in order to pursue or sustain higher returns is clearly an option.

Whenever risk-taking is significant, it should be explicitly stated, understood and approved by an appropriate level of management.

Treat or Implement Controls

Because the response to most significant risks will be active rather than passive, there will be some degree of TREAT in response to most significant risks. Options for risk treatments are varied; they can be divided here into five categories: Organisation, People & Relationships, Direction, Operational and Monitoring. As a general rule, selective and intentional application of elements from all five TREAT categories, interlinked with particular elements described under TAKE, TRANSFER or TERMINATE, will result in reasonable assurance of achieving business objectives.

Transfer

It may be possible to reduce the impact of risks through various means of risk transfer. Risk transfer decisions will depend upon the nature of the risk, the criticality of the operation or service associated with the risk, and cost/benefit considerations. Explicit and detailed understanding and agreement up-front is essential to effective risk transfer or sharing arrangements. It is important to note that transfer of risk does not result in transfer of accountability; the risk owner will remain accountable. Therefore it is important to combine risk TRANSFER arrangements with risk treatments such as insurance and contracts.

Terminate

Risks can be avoided, for instance by ceasing a particular activity or withdrawing from a specific market. It is also possible to terminate some risks by changing the business objective or process. Some risks may be terminated in part through sale or divestment; however it is important to recognise whether all of the risks will indeed be terminated or whether some will remain with the University.

Risk Culture

Risk Culture is the corporate attitude to risk. Some organisations or parts of organisations are particularly risk averse; that is they keep away from risk while others are more inclined to accept high risk where there is a perceived benefit.

The University is essentially conservative in nature but there are areas which have a more aggressive attitude to risk.

In any event it is important to identify and assess the risks and document reasons for decisions particularly where they may fall outside predetermined thresholds or cultural precedent.

Risk management at every stage requires cost benefit analysis. Most cost benefit analysis is intuitive and not documented. There are times when the cost benefit should be assessed quantitatively and decisions based on that analysis. For example some risks are not documented because there is no management benefit in the time invested. The same risks may be documented in a particular context because it is important to demonstrate they have been identified.

Risk Threshold/Tolerance

Risk should be mitigated to a level that meets accepted organisational standards. While these standards are readily assessable in some areas (e.g. financial losses), there may be less clarity in others. It is important that the risk appetite for any particular type of risk is understood. Management of risk should be in line with the University's appetite (or tolerance) for that risk.

Thresholds of risk can be set for effective utilisation of resources. For example, the University has set a threshold which requires all risks with an *Inherent Rating* of **Extreme** and **High**, to have documented controls which reduce that risk to **tolerable** or **low**, (or an explanation as to why such controls are not identified). Managers at any level can determine the threshold level of risk which should be reported for their area, they should be notified, or the frequency of re-assessment.

Tolerance, defines a predetermined measure of variance for a particular risk, type of risk or control, before it is reported or reviewed. For example, the completion date for a control implementation may be plus or minus 7 days, or the failure rate for a piece of equipment is set at plus or minus 5%. In project management, thresholds could be set based on the inherent risk rating, which determines how, when and by whom, risks should be managed and reported and tolerances placed on the time for reporting or implementation of controls.

Figure 3 – RISK RESPONSE OPTIONS

<p style="text-align: center;">Take</p> <ul style="list-style-type: none"> • Intentionally pursue • Fully accept • Set reward / loss targets & tolerance levels • Establish & monitor key risk indicators • Charge premium price • Build in contingencies • Develop recovery plans • Investigate & take follow-up actions • Finance the consequences 	<p style="text-align: center;">Treat</p> <ul style="list-style-type: none"> • Organisational design & processes • People & Relationships – capability, shared understanding, teamwork • Direction – business guidelines, budgets, priorities • Operational – adherence to standards, protection of people & assets, continuity • Monitoring – learning, corrective action & improvements
<p style="text-align: center;">Transfer</p> <ul style="list-style-type: none"> • Insure • Share (Joint ventures, alliances, partnerships) • Contract out • Diversify/spread • Hedge 	<p style="text-align: center;">Terminate</p> <ul style="list-style-type: none"> • Cease activity • Pull out of market • Divest • Change or recalibrate objective • Redesign (eg business process, system, tools) • Reduce scale

Figure 4

RISK TREATMENT TOOLS

Actions to Reduce or Control Likelihood	Procedures to reduce or Control Consequences
<p>These can include but are not limited to:</p> <ul style="list-style-type: none"> • Review and compliance programs • Contract conditions • Formal reviews of requirements • Investment and portfolio management • Project management • Preventative action • Quality assurance, management and standards • Research and development, technological development • Structured training and other programs • Effective governance processes • Strategic, operational and tactical planning processes • Supervision • Testing • Organisational arrangements • Technical controls 	<p>These can include but are not limited to:</p> <ul style="list-style-type: none"> • Contingency planning • Contractual arrangements • Contract conditions • Design features • Business continuity and disaster recovery plans • Fraud control planning • Minimising exposure to source of risk • Portfolio planning • Pricing policy and controls • Separation or relocation of activities and resources • Succession planning • Insurance • Public relations • Ex Gratia payments

2.7 Step 5- MONITOR AND REVIEW

As risk controls are set up to manage known and understood causes, it should also be recognised that both the risk causes and/or controls may change in extent and effect and thus regular monitoring and review is required. It is important to note that changes in stakeholders should be considered as well as changes in the business risk management process. There should be regular reviews conducted by risk managers of the business environment to ensure that risks are correctly assessed and appropriately managed.

Audits

Audits should be conducted within each Directorate, Faculty and Business Unit as part of the risk management process & will also be conducted by the University to ensure the integrity of the risk management process, risks and controls.

2.8 Step 6- COMMUNICATION, CONSULTATION & REPORTING

Communication - The University encourages employees to identify and document risks. By sharing information we can learn from the experiences of others and share the ways in which we manage similar risks. Risk information sharing can be facilitated through organised discussion forums (e.g. Management Groups, University Committee's) and the '*KnowRisk*' data base.

Consultation - when identifying and assessing risks, the views of a range of stakeholders should be taken into account. Some common stakeholders include:

- Faculties and Schools
- Financial Services
- Insurance Office
- Human Resources
- Occupational Health and Safety
- Legal Services
- Facilities Management
- Residences
- Government communities
- Students
- Staff

Reporting

Risk information should be directed to the nominated Risk Management Co-ordinator within the Faculty, School, Department or Directorate concerned for entry into the '*KnowRisk*' database. Risk information, including mitigation measures, should be communicated via risk management plans, business plans, performance reporting and business contingency and continuity plans (BCCP), as well as included as an important part of business proposals.

An approved standard report that shows the inherent and residual ratings of risks identified within the University is submitted to the Audit & Compliance Committee.

There are additional corporate risk reporting requirements (detailed in section 3.2) relating to Units (Academic and Central Administration sections) level risks.

2.8.1 Risk Reporting Tools

Risk Register

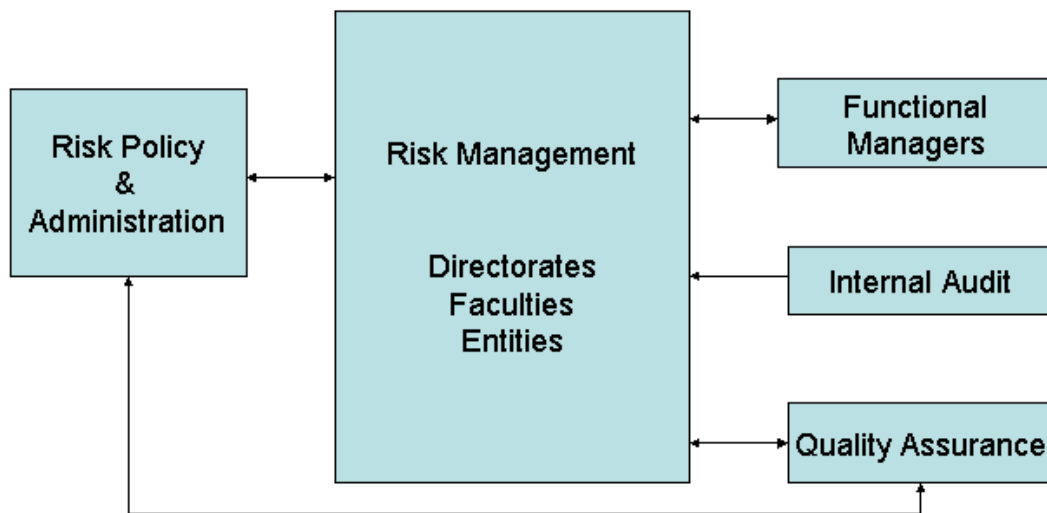
All Faculty, School, Department or Directorate level risk information should be stored centrally in the Risk Management Database '*KnowRisk*' to allow reporting and analysis of cross-organisational risk.

3 RISK MANAGEMENT FRAMEWORK

The risk management framework has been introduced to provide assurance at the corporate level that risks are being adequately managed.

3.1 STRUCTURE

Enterprise Risk Management Overview Structure

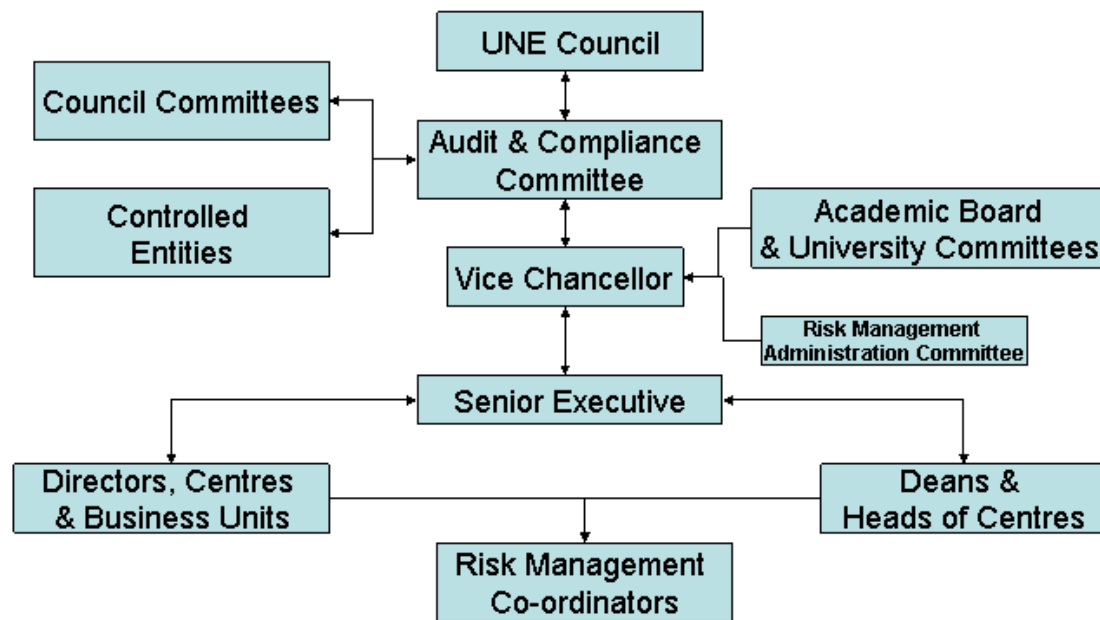


24/08/2005

UNE Risk Management Plan -
Framework

Enterprise Risk Management

Accountability Structure

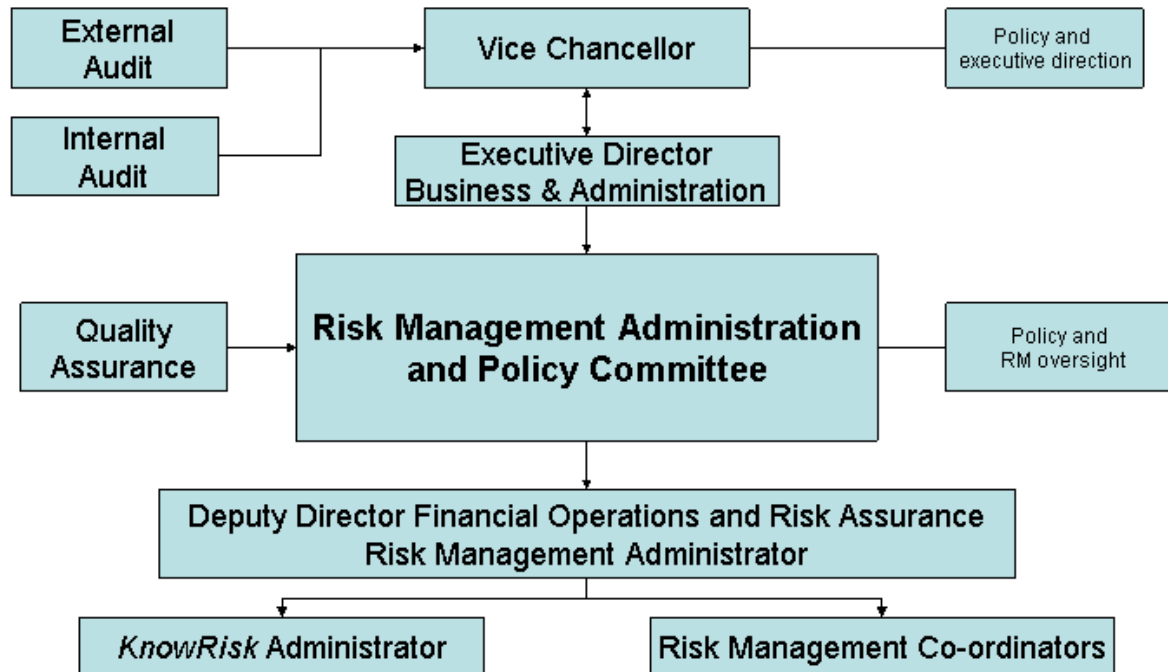


24/08/2005

UNE Risk Management Plan -
Framework

Enterprise Risk Management

Administration and Policy Structure

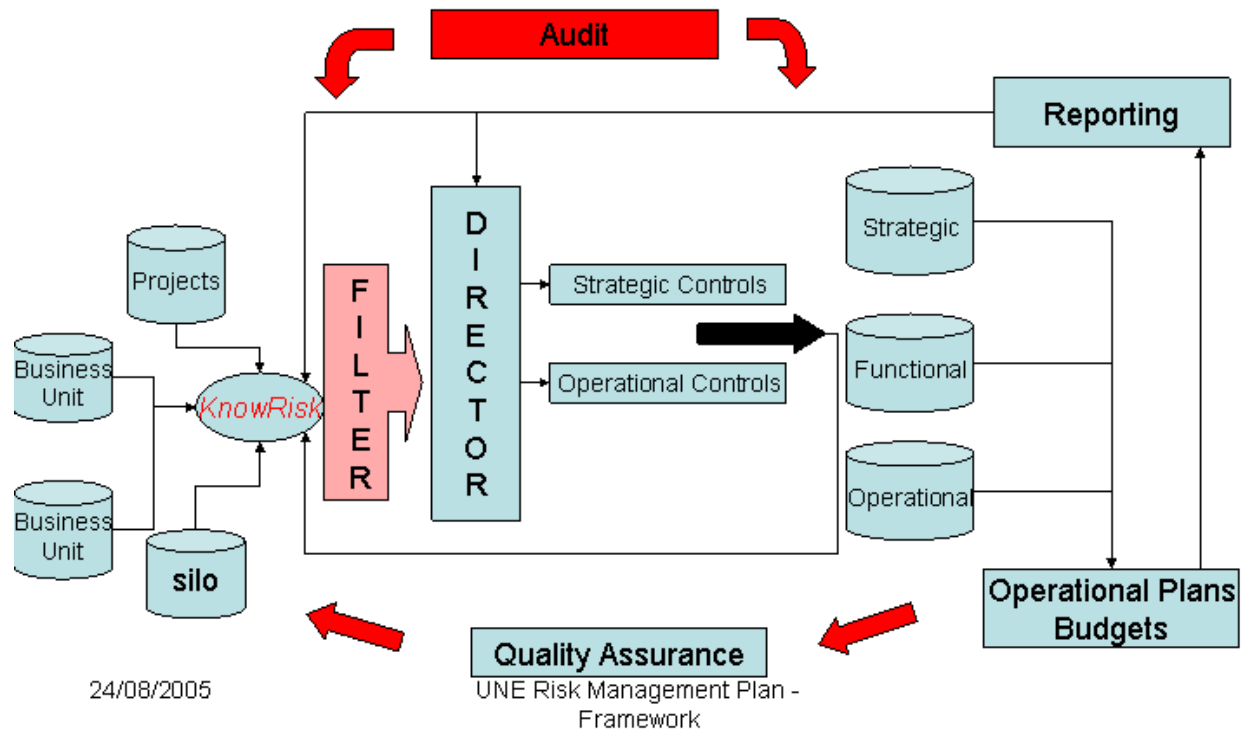


24/08/2005

UNE Risk Management Plan -
Framework

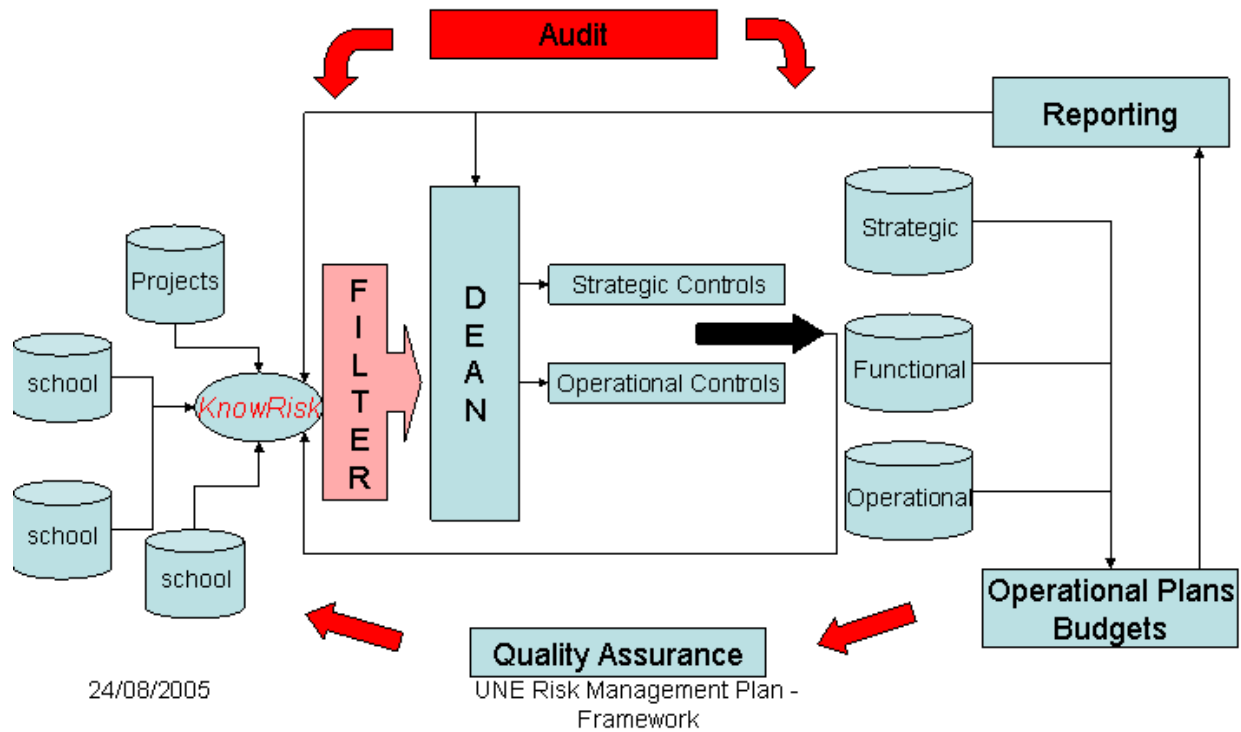
Enterprise Risk Management

From Business Units to Director



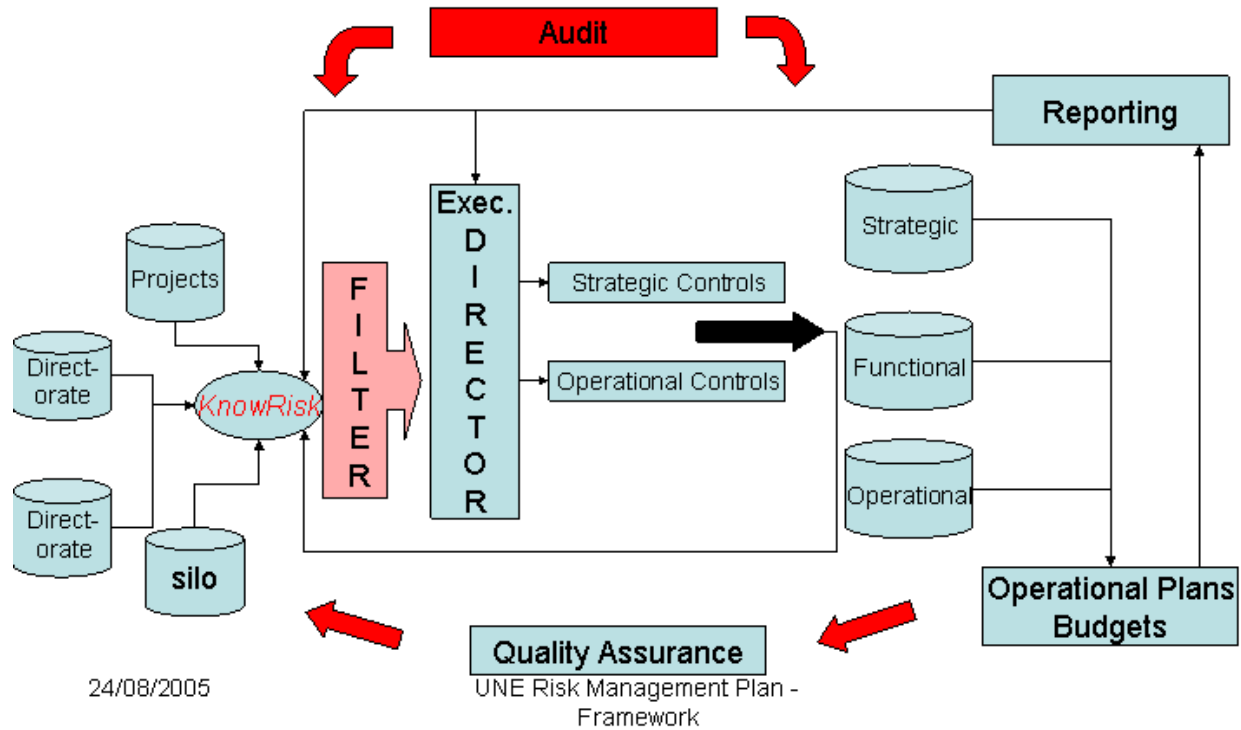
Enterprise Risk Management

From Schools to Dean



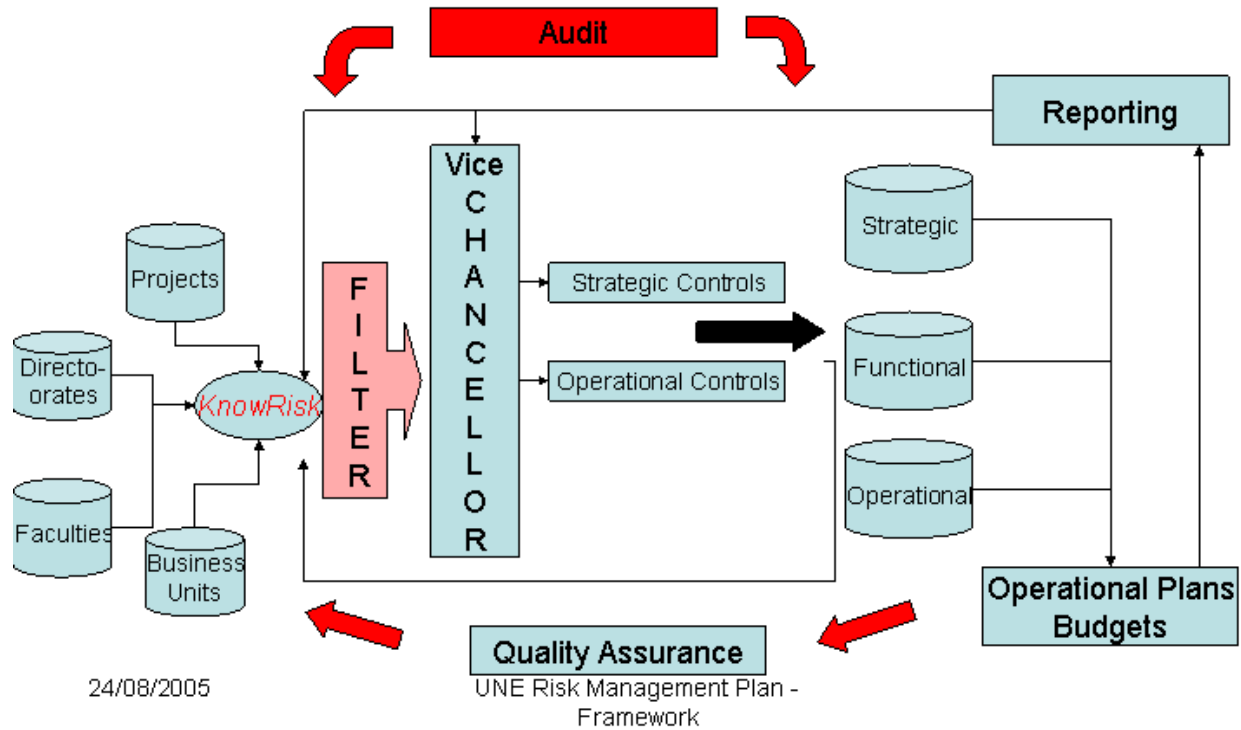
Enterprise Risk Management

From Directorate Silos to Enterprise



Enterprise Risk Management

From Operational to Enterprise Risk



3.1.1 Risk Management Responsibilities

Role of the University Council

As the body ultimately accountable for the governance of the University, the Council has a responsibility to ensure good governance with respect to risk management as well as to identify and manage at a policy level, the University's strategic and governance risks.

Audit & Compliance Committee

As a Committee of the University Council, the Audit & Compliance Committee has been a driving force in the introduction and implementation of risk management across the University.

The primary role of the Audit & Compliance Committee is to monitor the process of risk management to ensure the University has, and is able to demonstrate that it has in place, a strategy, structure and process to effectively identify and manage in a timely fashion and at an appropriate level, its exposure to risk.

In addition to receiving the reports from Internal Audit, University executive, and management the Audit & Compliance Committee will continue to play a significant governance role in the auditing process and risk management and in the future the Audit & Compliance Committee could also facilitate the identification of strategic and governance risks on behalf of the Council.

The Audit & Compliance Committee retains the responsibility within the overall risk management framework on behalf of the Council for monitoring the integrity of the risk management process.

In addition the Audit and Compliance Committee will monitor the management systems and processes in place for:

- Compliance with laws and regulatory requirements and,
- Addressing significant business risks and the framework of management controls.
- Monitoring implementation of managements letters e.g. Auditor General.

Role of other Council Committees

Apart from monitoring the exposure and management of the University, the Committees of Council should seek to examine the alignment of resource allocation which best manages risk exposure. To be effective in this, it requires risk reporting which clearly identifies the resources required to mitigate significant risk exposure and opportunities. Their expertise in this area can assist the Council in determining strategy and decisions with respect to resource allocation.

Budgets and other resource recommendations to council committees should be accompanied by appropriate risk assessments.

Vice-Chancellor

The Vice-Chancellor is responsible on behalf of the Council for ensuring that risk management is maintained in accordance with the risk management policy and procedure.

Senior Executive (PVC's and Executive Director)

All Pro Vice-Chancellors, Executive, Dean's and Director's have the overall responsibility for their delegated areas and therefore the responsibility to ensure that their managers are implementing the University's risk management process. This includes the initial identification, documentation and assessment of risks, and appropriate reporting and monitoring processes. Any risk with an inherent rating of *high* or *extreme* must have adequate controls documented to ensure the inherent rating can be reduced to an acceptable level. Prioritising available resources against the University's risk exposure should be integrated into the planning and budget process. It is the responsibility of each executive to ensure timely reporting of risk exposure which is outside their positional delegated authority or where controls fail or are inadequate.

The Role of Boards and University Committees

There are numerous committees recognised within the University. Each has terms of reference (documented or otherwise). Each committee is responsible for the initial identification, documentation and assessment of risks to the University from the perspective of that committee and ensuring that identified controls are delegated and monitored as part of the committee's operation. Where risks are reported to the committee as part of its role then it is the responsibility of the committee to have in place adequate processes for managing those risks, including but not limited to; referral to an executive or functional manager and review and monitoring of the risk and controls implemented. Where the committee has resource delegations then it will also make decisions as to priority for risk management within its delegation.

Deans & Directors

Consistent with the University's Risk Management Policy all Deans and Directors are responsible to ensure that the University's risk management process for the effective management of risks within their operational area of responsibility is being implemented and used in day to day operations. This includes:

- Complying with University standards relating to particular types of risks.
- Establishing and maintaining a risk register which meets the requirements defined in the guidelines.
- Identifying and evaluating the significant risks that may influence the achievement of the University's objectives.
- Defining acceptable levels of risk taking and applying risk mitigation measures where necessary.
- Providing a system of ongoing risk review that is capable of responding promptly to new and evolving risks.
- Monitoring the effectiveness of the risk management systems that are in place; and

- Providing an annual assurance to senior management regarding the extent of their compliance with policy.
- In addition, Deans and Directors are to nominate a senior staff member who will be recognized as their Risk Management Co-ordinator.

Role of the Manager

Every employee who has a defined responsibility for other staff or assets is also responsible for the day to day management of risk for that work unit. Where management of the risk is outside the delegation of the manager then it is their responsibility to document and refer the risk to that manager or those managers who can manage the risk.

Day to day management of risk includes involving all staff in the active recognition of risk, its management and documentation as appropriate including, where required controls and ongoing monitoring of those controls, to ensure they effectively manage risk. (In most organisations there are controls for risk which no longer exist or which do not reduce risk at all. Such controls use up resources and leave insufficient resources to adequately treat other risks.) It is often at the manager or employee level that these are best identified.

The Roles of Functional Managers (e.g. Security, OH&S, Insurance, Media)

The role of functional managers is to use their professional expertise and resources to facilitate the management of risks, related to their functional role across the University.

These risks can be identified through category reporting from the '*KnowRisk*' database, or through the proactive efforts of the functional manager, entered to the Knowledge base as risk modules, and advised to other managers for assessment in their own context.

Functional managers can help identify controls for already identified risks and make these available on the risk register for all users.

Risk Coordinator

The risk coordinator will provide the primary point of contact for the business unit with respect to registration of the University's risk.

Risk coordinators will be provided with basic training in the risk management process being used by the University and the operation of the '*KnowRisk*' risk management database.

Their primary role will be to facilitate and/or maintain the risk register for their area either directly to the database, if an authorized user or in hard copy or softcopy so that the information can be added to the University wide Risk Register, by an authorised user.

It is the responsibility of the Director/Dean/Business Unit Manager to determine the specific role of the risk coordinator for their area.

Employees

It is the responsibility of every staff member to manage risks associated with their specific area

of employment. Where identified risks fall outside their area of responsibility, refer the risk via their managers to the area which controls the risk.

This includes:

- Identifying risks.
- Documenting & assessing risks.
- Identifying effective controls.
- Managing risks within their day to day duties.
- Reporting risks which exceed their delegated threshold.

Role of Project Managers

Any staff responsible for projects within or for the University or its associated campuses and entities shall initiate and maintain a process of Risk Management consistent with the University's Risk Management Plan and maintain the documentation on '*KnowRisk*'. All scoping documents should include an initial risk assessment and proposals for funding must be accompanied by a risk assessment.

Where project managers are responsible for the engagement and or management of contractors they shall ensure that the contractor provides an initial risk assessment and has an effective process of risk management which is maintained throughout the project.

Role of Information Technology Directorate

As the principal manager of hardware and software for the University, ITD will provide the technical infrastructure support for '*KnowRisk*' and facilitate the process for user access and security of the database and associated programs.

The ITD 'Help Desk' will be the first point of contact for '*KnowRisk*' users and the Administrator with access or technical issues related to the operation of the software.

Organisational Development Unit

Training: Responsibility for the content, delivery and integrity of risk management training rests with the Organisational Development Unit (ODU). Whereas every manager has a responsibility for development and monitoring the performance of their own staff, ODU will provide, and or, facilitate core training and development for initial and ongoing training in risk management and use of '*KnowRisk*'

Competence and Quality Assurance: ODU will be the final authority for certifying competence in the use of '*KnowRisk*' for the levels of access to the software. ODU will make known the competence required for different levels of access and facilitate timely programs of learning to allow staff to attain the level necessary for satisfaction of their responsibilities and conduct competency testing as required to assure that users are knowledgeable and competent in the use of the '*KnowRisk*' in compliance with policy. ODU will ensure that within the unit (or by some other means) there is always a person who is able to assess competence in the use of '*KnowRisk*'.

It will be the responsibility of ODU to ensure the ‘*KnowRisk*’ Administrator is advised in a timely manner of the competence of ‘*KnowRisk*’ trainees and maintain the Human Resource records of the University with respect to training undertaken and assessed competence.

3.1.2 Risk Management Administration

Risk Management Policy & Steering Committee

Role:

See appendix 2

The purpose of the risk management committee is to provide a leadership and directional aspect to the risk management process within the University.

At present the risk management facilitation / coordination is undertaken within the Financial Services Directorate and at the Audit and Compliance Committee. There is no direct management overview of the process. This often results in the issues being raised directly with the A&C rather than through management and therefore resulting in the A&C taking on management direction.

The establishment of the committee, being a committee of the Executive Director (B&A) and therefore a management committee, enables the management to have a direct input into the oversight of the process and identification and direction of issues to be addressed. It will provide a direct link to the Vice-Chancellor as the person directly responsible for the implementation of the risk management process, while enabling matters to be directed within the management structure.

The committee will also facilitate the integration of the overlap between internal audit and risk management and ensure that the internal audit is aware of and has input into the risk management process and resultant information. In addition it will ensure that the interrelation between the risk management process within operational units and the direct corporate risk management responsibilities (OH&S, EEO, Legal, Security, Environmental etc) is maintained.

The committee, however, does not take on the responsibility of the risk management process itself, this remains the responsibility of the individual managers as part of the management role.

Support:

The committee will be directly supported by the Director Financial Services in their role as Risk Management Facilitator, who in turn will be supported by the Risk Management Policy and Steering Committee, Risk Management Working Group, Risk Management Co-ordinators and the Internal Audit team.

Role of ‘KnowRisk’ Administrator

The ‘*KnowRisk*’ Administrator is primarily responsible for maintenance and management of the University Risk Management database. The role has no policy responsibility, but the Administrator would be required to provide support and feedback to users and policy makers. Effective management of the database is critical to the usefulness of the risk management process from day to day and over time. Maintenance of the integrity and security of the database and standards of documentation and policy decisions with respect to the risk register is the primary role.

The primary activity is sorting of ‘unapproved risks’ into the ‘UNE Risk Categories’ on a frequent and regular basis so that these are available to all users in a timely manner and the design and production of reports for the University.

Internal Audit

A plan for review and audit of controls to manage risk will be provided to the Audit and Compliance Committee as part of the annual audit plan.

Internal Audit will provide reports to Directors, Deans and other Executive Managers with respect to:

- Adherence to process.
- Appropriateness and effectiveness of controls in managing risks.
- Integrity of ‘*KnowRisk*’ data and other documentation processes.

In addition to assuring the integrity of the risk management process, internal audit will also provide advice and recommendations to managers and the executive as to how the process can be more effectively or usefully implemented.

3.1.3 External Requirements

Role of Associated Entities

All entities associated with the University of New England either through incorporation, partnership, affiliation, use of its trademarks or brands, shall implement a process of risk management consistent with the Australian Standard AS/NZS 4360-2004 or later.

Where the University of New England, requires annual or other regular reporting, from the entity, then that report shall include reporting of risks and its risk management process.

Where the entity identifies a risk, which even with controls, that is residual risk, exposes the University of New England at a rating of extreme or high, then it shall report such a risk to the University, immediately, regardless of the reporting regime.

Contracts

All contracts with the University shall include a requirement that contractors have an acceptable process of risk management consistent with the Australian Standard AS/NZS 4360-2004 or later, and a requirement that, where the contractor identifies a risk, which even with controls (residual risk), exposes the University to a rating of Extreme or High, then it shall report such a risk to the University as soon as it is identified.

3.2 RISK REGISTER REPORTS

Risks identified will be entered into the risk management database. A range of system reports are available, or specialized reports can be developed.

All reports prepared for the Audit and Compliance Committee must be in a standard format unless otherwise requested. This standard report format has been created and is available within the '*KnowRisk*' database. Key risks at the Unit level will be collated and analysed at the corporate level to produce a strategic risk profile.

Reporting Risk

In 2002 the executive and the Audit & Compliance Committee agreed to focus on risks which were 'extreme' and 'high' and progressively address those which were rated lower.

Each Directorate, faculty, functional area and associated entity was asked to identify the top 10 risks to the University from their perspective. Since 2003, the Audit & Compliance Committee has rostered two managers to appear before the committee each meeting, with identified controls for risks rated 'extreme' or 'high'. The risks are entered on and included in the Audit & Compliance.

This has been the principle process for corporate monitoring of the introduction of risk management. Some management committee's, such as that of directors, have risk management as a standard agenda item and some directors have implemented mandatory risk assessment for all projects, with a monitoring process.

Following a widespread program of introductory training across the whole University, it is timely to introduce a more structured reporting and management of risk across the institution. This will reinforce the culture of active risk identification, assessment and treatment and more importantly enable the University to more adequately manage its risk and appropriate its limited resources in the most effective way.

This process can be facilitated by the '*KnowRisk*' database which is being made available across the University on a gradual basis. (Operation of this database covered elsewhere). Management and reporting however are not dependant on '*KnowRisk*'.

As with the introduction of other aspects of risk management, integrating the process into existing operations and functions seems the most appropriate rather than creating new and additional structures and administrative processes.

Existing management committees should include risk management on their agenda on a regular basis. The way risk is dealt with may vary significantly for different committees but should include:

- Initial identification, documentation and assessment of risks to the University from the perspective of that committee and its terms of reference.
- Identification and documentation of treatments for those risks assessed as ‘extreme’ or ‘high’
- Education or training for members of the committee with respect to risk management
- A process for monitoring:-
 - Risks and their ratings (as time and environment changes)
 - Treatments-effectiveness or otherwise of controls
 - Progress on implementation of new controls
 - Monitoring of existing controls
- Communication across, up and down the organisation with respect to risks and controls
- The quality assurance of risk management and
- Documentation of actions and decisions on the ‘KnowRisk’ database.

Some committees, for example Audit & Compliance, VCC or Director’s should also exercise a broader management perspective. This would include:

- Periodic review of the risk management process
- Identification and monitoring of risk reporting required
- Audit of process and control implementation

At all times the cost/benefit of the risk management process itself, and management of individual risks, is part of effective risk management. If the process or controls are more ‘expensive’ than the risk if it was realized, then risk management has become compliance and administratively focused rather than management focused.

This plan identifies and documents the principles, processes, structures and accountabilities for risk management. Where any question arises as to accountability the existing management accountabilities take precedence.

All risk will be reported with its inherent rating and the controls which will bring it to an acceptable residual level.

Note: There have been significant examples of organisations which have reported only residual risk to their management, governance bodies and stakeholders. Such reporting may give a false understanding of the organisations exposure, as such risk is only ‘true’ if all treatments are implemented and are in fact effective. If the controls fail, or are not implemented and the risk is realised, the exposure is the same as if the controls did not exist.

A schedule of risk reporting will be determined by the Executive and Audit and Compliance Committee and reviewed annually.

3.3 RISK CATEGORISATION

Categorisation of risks allows more effective analysis of risk trends, identifying common causes of risk and control weaknesses so that treatment options can be optimised. The University has adopted the following risk categories.

- Academic & Research
- Commercial Activities & Associated Entities
- Corporate Governance/Management Practices & Legislation
- External, Government
- Faculties, Utilities, Buildings & Environment
- Financial (Assets, Fraud & Corruption)
- Image/Reputation
- Information Technology
- Personal Safety (Including OH&S)

3.4 MANAGEMENT SYSTEM RISK

For risk management purposes risk is separated into two different types of risks:

1. Unit Risk — these risks are specific to the Unit with risk management actions sitting within the Unit/functional area.
2. Strategic Risks — these risks sit across the University and may relate to an internal or external influence. Risk management actions might sit with the process area, however, some actions will be the responsibility of other organisational areas and will be managed through the normal management structures.

3.5 CONSOLIDATION OF RISK

The consequence of one risk can often be a cause of another risk. Hence you might have several smaller risks contributing to one larger risk. For example the 'Interruption of systems in the Library due to failure of the power supply' may be a high level risk however there are a number of contributing risks. Risks should be assessed at a level that supports the most effective management of that risk and risks should be reported at a level appropriate to the audience (i.e. the Library risk should be assessed and reported as a single risk at the Unit level and as multiple risks at the asset level). Often only when related risks are consolidated can the full extent of exposure be appreciated.

3.6 ASSURANCE TOOLS

A number of assurance tools have been developed to support risk management assurance. These include the following:

- The Risk Assessment Tools (detailed in Section 2.4.1)
- Risk User Guide '*KnowRisk*' (in preparation) to assist Units in assessing their risks.
- Risk Management Plan
- Training Documentation

4 GLOSSARY

Based on the definitions from AS/NZ S 4360 Standard

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.

Cost

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

Hazard

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

Incident/Event

An occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences.

Inherent Risk

A measure of risk in its natural state. Under the worst case conditions i.e. measure the likelihood and impact/consequence of the risk occurring in the event with are no controls in place.

Likelihood

A qualitative description of probability or frequency.

Loss

Any negative consequence, financial or otherwise.

Residual Risk

A measure of risk when the effect of existing controls, structures and treatments within the organisation are taken in to account.

Risk

Any event or action that could influence the achievement of business objectives. Risk is measured in terms of likelihood and impact/consequence.

Risk Acceptance

An informed and formal decision to accept the likelihood and impact/consequences of a particular risk.

Risk Analysis

A systematic use of available information to determine how often specified events would occur and the magnitude of their consequences. Refer University matrix.

Risk Assessment

The overall process of risk analysis and evaluation. Refer University matrix.

Risk Avoidance

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

Risk Control

The implementation of policies, standards, procedures and physical changes to eliminate or minimise adverse risks, or maximise opportunities.

Risk Engineering

The application of engineering principles and methods to manage risk

Risk Evaluation

The process used to determine risk management priorities by comparing the estimated risk level against pre-established criteria.

Risk Financing

The methods applied to fund risk treatment and the financial consequences of risk

Risk Identification

The process of determining what can happen, why and how events arise as the basis for further analysis.

Risk Management

The systematic and ongoing process of risk identification, assessment, treatment and monitoring. It can be applied at any level of the University including strategic, operational and at project level. It is not solely about limiting risk but rather about fully appreciating and recognising the risks we carry and balancing risk and reward in an informed manner.

Risk Management Process

The systematic application of management policies procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. This includes the University's Risk Management Policy & Risk Management Plan.

Risk Rating

The risk rating is the combined effect of the likelihood of occurrence of the event and the severity of the impact and is an indication of the overall exposure to the University. Refer University matrix.

Risk Reduction

The application of appropriate techniques to reduce either the likelihood of an occurrence or its consequences, or both.

Risk Transfer

This is shifting the responsibility for loss or gain to another party through legislation, contract or insurance.

Risk Treatment

This involves the selection and implementation of appropriate options for dealing with specific risks usually referred to as controls.

Stakeholders

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

REFERENCES:

Australian/New Zealand Risk Management Standard 4360:2004

ACKNOWLEDGEMENTS

Acknowledgment is given to the:
University of Western Australia

Appendix 1

RISK MANAGEMENT POLICY

The cornerstone of the Risk Management Plan is the Risk Management Policy (below), which outlines the expectations that Council and Executive have of all employees with respect to risk management. Implementation of the policy will ensure management can demonstrate that risks in all parts of the University are being identified and managed in a way that is appropriate for the business environment and objectives.

Policy (As approved by the Vice-Chancellor 14/12/2004)

Commitment

The University recognises that risk management is an integral part of good management practice and considers it an integral part of good corporate governance. The University is committed to achieving best practice in the area of risk management, and will apply its principles and practices throughout the University in accordance with AS/NZS:4360 Standard 2004. As a result of this process the University will have, and be able to demonstrate that it has in place a strategy, structure and process to effectively identify and manage its exposure to risk. Risk management is recognised as an integral part of day to day operations.

Objectives

The main policy objectives for managing risks are to:

- Assist the University in achieving its strategic objectives and goals.
- Safeguard the University's assets – people, finances, property and information; and
- Create an environment where all staff members assume responsibility for risk management.

Responsibilities

As a committee of the University Council, the Audit and Compliance committee retains the responsibility to oversee the process within the overall risk management framework on behalf of the Council. Responsibility within Cost Centres resides with the respective Dean, Director or Manager while the Senior Executive are responsible for ensuring that Risk Management is addressed at all levels in their portfolios. The Academic Board has the responsibility of ensuring that Risk Management is addressed within the context of the responsibilities and actions of the

Board. Staff at all other levels are responsible for developing an understanding of and becoming competent in the implementation of risk management principles and practices in their work areas.

The University's governance, Council and Council Committees are responsible for ensuring that the University management apply appropriate risk management practices and for actioning such practices within the context of their own activities.

Risk management is a multifaceted process, appropriate aspects of which are often best carried out by a multi-disciplinary team. It is an iterative process of continuous improvement.

All Deans/Directors/Cost Centre Managers are required to:

- Nominate one senior staff member who shall be recognised as their Risk Management Coordinator.
- Ensure Design, resource, operate and monitor internal control systems.
- Ensure that a risk-based approach to controls are communicated to staff and embedded in operational processes.
- Assign accountability for managing risks within agreed boundaries; and
- Report the results of assessments regarding the effectiveness of the risk controls to the Audit & Compliance Committee and Vice Chancellor as required.
- The University's governing Boards (e.g. Academic Board, Council & Council Committees) are responsible for risk management in the context of the operations of their activities and the overall operations of the University.

All Deans/Director/Cost Centre Managers are accountable for:

- Complying with University standards relating to particular types of risks.
- Establishing and maintaining a risk register which meets the requirements defined in the Guidelines.
- Identifying and evaluating the significant risks that may influence the achievement of the University's objectives.
- Defining acceptable levels of risk taking and applying risk mitigation measures where necessary.
- Providing a system of ongoing risk review that is capable of responding promptly to new and evolving risks.
- Monitoring the effectiveness of the risk management systems that are in place; and
- Providing an annual assurance to senior management regarding the extent of their compliance with the policy & Procedures.

Appendix 2

The University of New England Risk Management Policy & Steering Committee

Terms of Reference for the Committee:

The Committee's role is to provide a broad overview and direction to the risk management process within the University, specifically overseeing the administrative component and providing feedback and input into the management structure.

Broadly the Committee's responsibilities will encompass in relation to risk management and audit the following activities:

- provide management with comment and recommendations in relation to the progress of the risk management process being undertaken
- provide direction and recommendations regarding process to the Risk Management Facilitator
- review and provide comment to management on risk management audit requirements and reports
- provide input to functional managers to facilitate strategic management of functional risks
- provide input (strategy and process) to executive management to identify and manage risk
- review and comment on policy and procedures for effective risk management
- examining and comment on the implementation of process and procedures for Fraud and Corruption policy
- review and refer to applicable operational management or committee any identified major corporate risks
- provide a conduit in relation to risk management to and from the Audit and Compliance Committee
- provide input to the internal audit plan in relation to risk management issues

Reports/Makes Recommendations to: Vice-Chancellor

Chaired By:

Executive Director (Business and Administration)

Membership:

Director Financial Service Directorate

PVC (Teaching and Learning)

A Dean

Risk Management Co-ordinator's representative

Co-option

The Committee has the power to co-opt up to two members

In Attendance

Director Financial Services

Internal Audit Manager

Risk Management Database Administrator

Gender Balance:

When co-opting members, the Committee will consider

gender balance.

Quorum: A quorum shall consist of a simple majority of members of the Committee.

Term of Office: Positional

Meetings: The Committee will meet at least five times per year.

Support: The Director Financial Services will provide support.

Context –

Initial Risk Identification and Classification											
Issue/ Category	Risk	Fraud Aspect Yes/No	Assessment		Risk Rating	Control Assessment	Reassessment		Risk Rating	Target Rating	Further Action Yes/No
			Likelihood	Consequence			Likelihood	Consequence			

Explanation of terms: **Assessment** = Likelihood & consequence without controls; **Reassessment** = Likelihood & consequence after control(s) implemented

Likelihood - of Occurrence

- Rare** Likely to occur only in very exceptional circumstances.
 - Unlikely** Could occur at some time.
 - Possible** May occur at some time.
 - Likely** Will probably occur at least once.
 - Almost Certain** Is expected to occur in most circumstances.
- Consequence/Impact**
- Insignificant** No Personal Injury; No Adverse Media Attention; Financial Cost under \$2,000.
 - Minor** Minor Personal Injury; Adverse Local Media Coverage only; Financial Cost of between \$2,000 and \$50,000.
 - Moderate** Serious Personal Injury; Adverse Capital City Media Coverage; Financial Cost of between \$50,000 and \$250,000.
 - Major** Multiple Serious Personal Injury; Adverse & Extended National Media Coverage; Financial Cost of between \$250,000 and \$1m.
 - Catastrophic** Fatality(ies); Governmental Intervention; Financial Cost of more than \$1m.
- Control Assessment**
- Damaging** Increases likelihood &/or consequence of risk or introduces other unacceptable risk(s)
 - None** No effect
 - Deficient** Some effect on likelihood &/or consequence but not sufficient to reduce risk to a satisfactory level
 - Marginal** Barely sufficient to reduce risk to an acceptable level
 - Qualified** Some effect but not guaranteed to reduce risk to acceptable level on all occasions
 - Effective** Reduces risk to acceptable level
 - Excessive** More than required to reduce risk to an acceptable level; resources are being wasted

RISK MANAGEMENT WORKSHEET

