# Risk Management Framework Guidelines

The implementation of risk management practices enables an effective risk culture by developing expertise and capability across VU.

The Risk Management Policy and Procedure provide the framework for effective risk-based decision making that maximises the achievement of opportunities, whilst preventing and minimising the impact of undesirable threats. Effective engagement of risk is critical to the achievement of VU's strategic objectives. These documents provide for:

- **Clear risk management objective**: a well-defined objective and role of risk management at the strategic, enterprise and operational levels that is supported by SEG, CARC and Council.
- **Support function**: a centralised corporate support function that possesses deep risk management expertise and proactively drives VU's risk agenda through an advisory model.
- **Dedicated resources**: that understand the needs and challenges of College's and organisational units and are available to provide regular support.
- **Accountability**: mechanisms to support risk ownership and accountability at all levels.

The above mechanisms amongst others will be the primary drivers in delivering the following process:

- **Communication and consultation**: the methods by which risk information is captured in an engaging manner and the method of communication to provide the right information at the right time.
- **Development / refresh of risk information**: a cycle of risk management activity which considers risk information on an ongoing basis and a formalised setting on a periodic basis.
- **Analyse and action**: risk identification, analysis and action to verify current activities or implement new management action where required.
- **Reporting**: a reporting cycle that reports the right information, to the right people, at the right time.
- **Monitor and review**: a monitoring and review cycle which identifies and considers risk information at all levels to provide insights to SEG and CARC as required.

Success will be achieved by applying risk management practices as part of strategic, business planning and day- to-day decision making. It is essential that there is a strong linkage between risk management activity and business plans to increase the likelihood of success.

### 1) Risk management responsibilities

The following summarises the key activities required by various critical areas in relation to risk management activity.

#### a) Compliance, Audit and Risk Committee of Council (CARC)

- A committee of Council, the Compliance, Audit and Risk Committee (CARC) is tasked with general oversight of governance matters on behalf of the Council and its accountabilities are defined in the CARC Terms of Reference. CARC is responsible for ensuring that the annual risk management review and reporting cycle is completed, which includes:
  - Annual review and approval of the risk management policy, procedure and process;
  - Reviewing and approving, at least annually, risk registers including strategic, enterprise and highlights (key risks) from operational risk registers;
  - Reviewing, recommending and approving the oversight and monitoring of internal processes for managing risk and ensuring that risk exposures of all types, across VU, are being managed effectively through the operation and implementation of the Risk Management Policy and Procedure;
  - An annual and forward-looking internal audit plan that adopts a risk-based approach to ensure assessment that management controls are operating effectively.

#### b) VU's units and Colleges

- Providing effective oversight to the strategic and operational functions of VU, to ensure that risk is appropriately managed via the establishment of appropriate structures, processes and informed decision making.
- Reviewing and considering, at least annually, the structure of risk exposures that are faced by VU as a whole (strategic and enterprise risk profiles) and ensuring that appropriate treatment actions are in place.
- Establishing appropriate delegations to ensure that the effective management of risk is cascaded through areas of their responsibility.
- Ensuring operational management and employees within their area implement an effective risk process, so that risk management is an enabler, which informs all day-to-day decision making.

#### c) Planning and Governance Portfolio

- Partnering with VU's units and Colleges and collaboratively working with them to embed risk management processes and culture throughout VU.
- Developing and enhancing processes, methodologies and a common risk language to identify, assess and manage risks of importance (review and update the Risk Management Policy and Procedure at least annually).
- Updating, at least quarterly, strategic and enterprise risk registers and reporting these to senior management and CARC, including a highlight report of risks considered to be outside an acceptable

level and changes to the risk registers in accordance with the annual risk cycle.

- Proactive education and assistance to all areas and activities of VU for their risk management activities including:
    - Ensuring that all areas and activities complete, at least quarterly, risk management reviews to identify risks and review treatment plans for current risks;
    - Completing risk identification at the operational level at least quarterly (usually via team meeting agenda item, and escalating to the Planning and Governance Portfolio where risks are deemed to be outside an acceptable level determined by management;
    - At least annually physically attending and observing the risk management process discussion occurring in each of VU's units and Colleges to ensure VU-wide consistency;
    - Where risks are identified as a strategic or enterprise risk, escalating them to the appropriate risk register and ensuring they are reviewed and reported at the next review of these registers.
- Facilitating an improved understanding of risk information in key decision making and governance processes for all areas of VU.
- Ensuring that a consistent risk management system (Risk Wizard / Risk Profile Form / Reporting Template (Powerpoint)) is used to identify, record risks, manage risks and associated treatment activities.
- Completing performance reviews by exception as required to review controls and process environments in place for strategic and enterprise risk profiles.
- Developing a yearly risk management training, education and capability development calendar and plan to ensure that all staff are capable of completing their risk responsibilities.

## 2. Exceptional risks

Some areas of VU may require a specific or customised approach to risk management (risk management as required by, for example, regulation, industry standards, or contracts with third parties). These instances are dealt with on a case by case basis with the Vice President – Planning, Registrar & University Secretary.

Where a risk is identified to be outside of tolerance and an enterprise risk, ensuring that it is reported to the Vice-President Planning, Registrar & University Secretary. Based on the initial review, the risk may be escalated to the Vice Chancellor or CARC for review / acceptance. Upon their review, the appropriateness of treatment options should be evaluated, and the success of the implementation should be tracked to ensure the risk is adequately mitigated. These risks should be reported to CARC's next meeting for review and / or acceptance that VU can accept a risk outside of management's tolerance.

Any variations initially approved by the Vice President – Planning, Registrar & University Secretary are required to be approved by SEG prior to implementation. However, each approach must, at a minimum, align to the principles and minimum standards of the Risk Management Policy and Procedure to ensure a holistic risk management approach is implemented and a consistent risk management culture is maintained across VU. It is the responsibility of all staff, including management, to ensure that risk management is embedded across all decision making activities and day to day operations.

## 3. Detailed risk management process information

### a) Setting the context

- Establishing the context for the risk management activity sets the scope and boundaries for the whole risk management process. It is the key mechanism for providing the foundations for identifying and analysing the risks.
- The key objectives of establishing the context are:
    - To ensure that there is an appropriate level of understanding of the operations of the specific area of VU under review;
    - To determine the scope of the proposed risk management activity;
    - To begin to identify the issues, constraints, etc. that could give rise to hazards, threats and risks.
- Establishing the context involves a consideration of the external context, internal context and risk management context as articulated below.

#### i) External Context

- In establishing the external context one should be considering what issues exist within the external environment that could affect the area under consideration or influence the formation of risks, and how each of these external context issues could interact with VU.
- It is often beneficial to consider how these elements interact with each other and therefore items (ii) and (iii) below should be used as a prompter to inform the risk assessment process and discussion.

#### ii) Operating environment

- Economic
- Geo-political

- Natural
- Technological
- Demographic.

**iii) Operating ecosystem**

- Regulators
- Competitors
- Substitutes
- Complementors
- Partners and Suppliers
- Markets

**iv) Internal Context**

- The next step is to consider what issues within VU could be sources of, or could influence, risk. This should include consideration of:
  - VU's strategic or business objectives, strategies and plans;
  - VU's structure;
  - Business policies, functions, procedures and processes, and their interaction and interdependencies;
  - The status of physical (e.g. facilities) and technological (e.g. IT and telecommunications) infrastructure, and maintenance;
  - VU and local cultures;
  - Industrial relations (including staff morale and welfare);
  - Previous occurrences that have improved or detracted from the efficiency and effectiveness of VU;
  - Adequacy of existing and future resourcing;
  - The presence and effectiveness of other key controls;
  - Governance, organisational structure, roles and accountabilities;
  - Standards, guidelines and models;
  - Form and extent of contractual relationships.

**v) The risk management context**

- The primary purpose of establishing the risk management context is to develop the scope for the rest of the risk management activities, including:
  - Aims, objectives and proposed outputs;
  - Proposed commencement and completion times for the activities;
  - Other milestones and key performance criteria;
  - Areas of VU structure and / or activities that will be assessed;
  - The identification of key information sources, other human resources required, accountabilities and responsibilities;
  - Specific governance requirements (such as reporting, record keeping, assurance, audit, etc.);
  - Confirmation of key stakeholders and communication requirements;
  - Specific constraints or exclusions to the risk management activities;
  - Define the relationships between a particular project, process or activity and other projects, processes or activities;
  - Define the risk assessment methodologies;
  - Identify and specify decisions to be made;
  - Identify, scope or frame studies needed, their extent and objectives and the resources required;
  - The establishment of these three elements provides the context within which risks will be identified, assessed, evaluated and be treated.

**vi) Developing the evaluation criteria**

- The effort that should be put into establishing the context will depend upon the extent and complexity of the risk management activities concerned. The more comprehensive the context, the more information is developed to inform the risk management process. However, there will always be legitimate trade-offs that will limit the extent of, and effort put into the context.

**b) Identify the risks**

- Using the information developed for the context, as a guide, risks that will influence the achievement of objectives should be identified. The risk identification can be conducted using any one or combination of the following approaches:
  - Subject matter expert, or independent review of available information, such as management meeting agenda and minutes; management information reports, project briefs, performance analysis, audit reports, steering committee reports, industry reports, whitepapers, etc.
  - Workshops with key internal and / or external stakeholders (preferred).
  - One-on–one interviews or questionnaires conducted with key stakeholders.

- In identifying risks answers to the following questions should be sought:
  - What could happen?
  - How could it happen?
  - When could it happen?
  - Where could it happen?
  - Who could be involved in creating the risk?
  - Who or what could be impacted by the risk?
  - What measures are in place to prevent or manage the risk?
  - How reliable is the data / information?
  - What types of information are not available?
- The document in Annexure 1 should be used as a prompt to ensure that all relevant risks are identified.
- Where a risk has been identified to be financial in nature or there is the risk of fraud identified, management should ensure that all the sources / causes (contributing factors) have been identified, whilst importantly identifying current controls, where required developing and implementing treatment plans.

**c) Articulate sources / causes (contributing factors)**

- Capture the factors that cause the risk to exist. Consideration should be given to people, processes, technology, external factors, internal factors etc.

**d) Identify controls**

- The actions, activities or controls in place to prevent the risk from materialising. This may include, reviews, verifications, policies, procedures, system controls, plans, strategies, management activity etc.

**e) Analyse & Action**

**i) Assess the risks (residual assessment)**

- The aim of undertaking risk analysis is to develop a better informed understanding of the risks and, where required, prioritise those risks, for both the attention of decision makers and for action, such as for treatment of the risk.
- The assessment is conducted for each of the identified risks by determining:
  - Views of stakeholders;
  - Combinations of multiple risks taken into account;
  - The effectiveness of the different controls that could act upon the risk and modify (increase of decrease) the: chance of the event occurring, the consequences arising from the event, and the likelihood of the event occurring with those consequences;
  - Types, range and level of consequences that could occur should the risk eventuate;
  - The potential likelihoods for each of these consequences occurring;
  - An overall level of consequence and likelihood, which is the rating of that risk.The means by which an overall consequence could be determined will depend upon to a large extent upon the context, but could be based upon the most likely of the consequences, the most material of the consequences, a culmination of the range of consequences etc.
  - Existing controls in place to mitigate risk should be considered when assessing the likelihood and consequence so that the assessment reflects the residual level of risk.

**ii) Determine gap (is the residual level of risk acceptable?)**

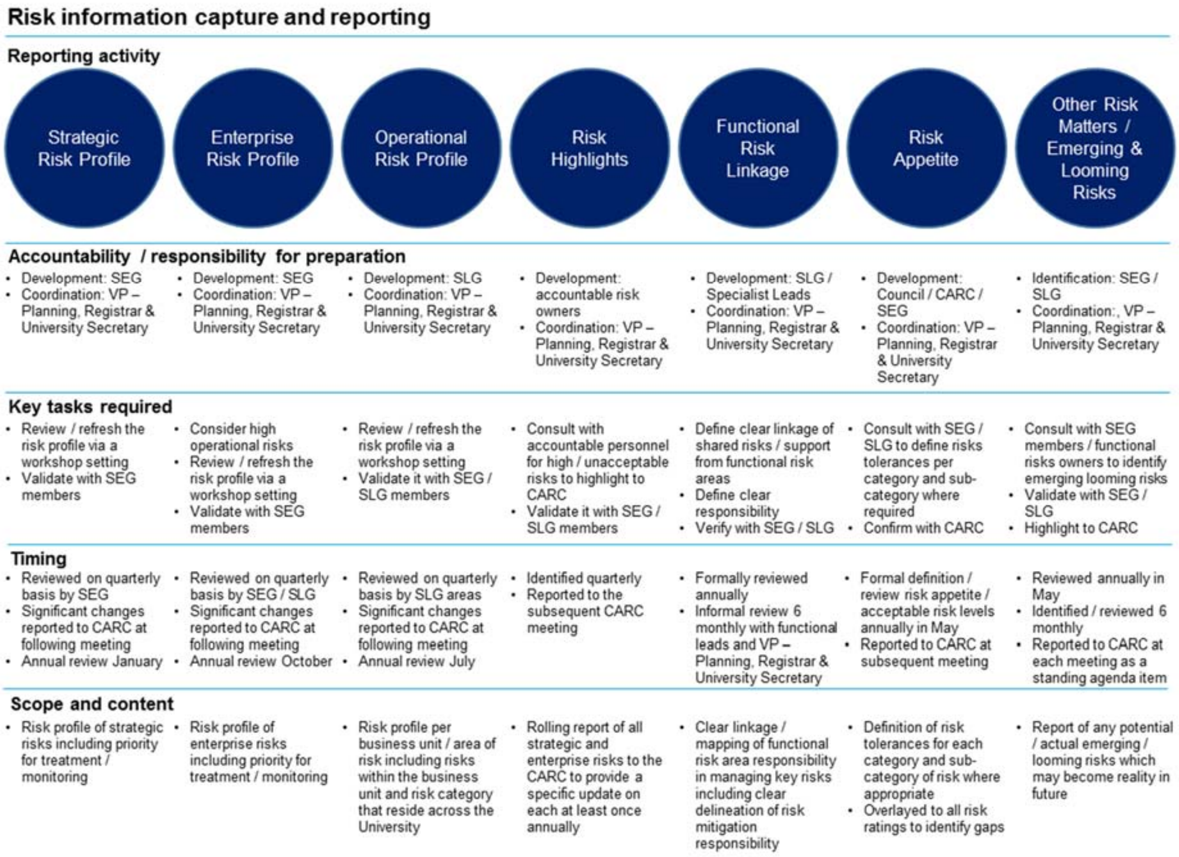
- Evaluating risks involves determining which risks that can be tolerated, and those that cannot and will require treatment options to be developed. Risk tolerability should originally be agreed when establishing the context. However, each risk should be reviewed by the management group completing the assessment by asking the following questions:
  - Are we comfortable accepting the residual level of risk?
  - Does more need to be done to mitigate the risk to an acceptable level?
- Tolerability will be determined to a large extent by the context, and the decision to treat or not will need to be evaluated on a risk by risk basis. However, as a general guideline any risk with a:
  - rating of ‘High’ should be considered immediately for treatment.
  - rating of ‘Major’ should be considered for treatment in the short term
  - rating that is outside the acceptable level determined by management should be considered for treatment in the mid-long term.
- There are other factors that need to be considered, for example a ‘Major’ risk that has a likelihood of ‘likely’ or higher may require more urgent attention than a higher consequence risk with much lower likelihood. Furthermore any risk rated at ‘Moderate’ or higher, where the effectiveness of the controls is inadequate or worse should be considered for treatment in the short term.
- Decisions should be made in accordance with legal, regulatory and other requirements, while also considering risk borne by other parties other than VU’s unit or College that benefits or is affected by the risk.

### f) Create remediate actions

- For each of the risks identified as ‘intolerable’, one or more treatment options should be developed, bearing in mind that generally it will never be possible to completely control all risk. The aim is to manage the level of risk to an acceptable level.
- The majority of risk treatment options that will be developed within VU will usually involve some form of improvements to process / activity controls (such as project management controls) that are already in place, or may require the introduction of new control mechanisms. Alternatively management may consider changing business practices or the business decisions that are made to avoid the risk. Potential treatment options that should be considered are:
  - **Tolerate, retain and monitor**: the decision is made that further treatment of the risk is not warranted or is impracticable because:
    - Risk treatments have been applied and further treatment of the residual risk is not cost effective
    - The activities creating the risk are deemed to be critical and must proceed at the current level of risk
    - Treatments being implemented for the management of other risks will have some collateral effect on the risk in question and lower the risk to a more tolerable level
    - At the current time, capability or resources to implement the required improvement activities are unavailable
    - Treatment of the risk is not cost-effective and / or the risk level is deemed to be as low as is reasonably practical in the prevailing circumstance
    - Align with management’s acceptable level of risk to pursue a possible opportunity.
  - The only option may be to continue to monitor the risk until circumstances change and action can be taken to then manage the risk.
  - **Share**: The “management” of the risk may be shared with, or transferred to a third party. For example this may involve increasing certain types of insurance cover, or outsourcing certain activities (such as safety testing of biological products)
  - **Reduce**: consequence and / or likelihood of the risk through the implementation of improvements to existing controls or through the introduction of new controls (treatment plans).
  - **Avoid**: stop undertaking the activities that are creating the risk exposure, thereby avoiding the risk.
- Depending upon the circumstances, these treatments may be applied either individually or collectively to move the risk to a level where it can be tolerated. While treatment options must be chosen on the basis of managing the risk in an appropriate manner, some types of treatment may be better suited to types of risk with certain levels of consequence and likelihood. Selection of treatment plan options will need considerations of legal, regulatory and other requirements.
- However, caution needs to be exercised in formulating suitable treatment options. Consideration must be given, that the decision to undertake a particular treatment is not solely dependent upon considering the level of risk and VU’s tolerance to it. It must also consider:
  - The availability of practical treatment options
  - The degree to which treatment options will provide effective management of the risk, without introducing new risks
  - The cost-benefit of each potential treatment option, including the cost-benefit of accepting the risk without further treatment
  - The cultural or social acceptance of treatment options
  - Industry standards or practices that may require the risk to be managed to certain parameters.

### g) Report

Summarised below is the process for developing these outputs for CARC amongst other operational reporting requirements.



**Risk information capture and reporting**

| Reporting activity | Strategic Risk Profile | Enterprise Risk Profile | Operational Risk Profile | Risk Highlights | Functional Risk Linkage | Risk Appetite | Other Risk Matters / Emerging & Looming Risks |
|---|---|---|---|---|---|---|---|
| **Accountability / responsibility for preparation** | • Development: SEG<br>• Coordination: VP – Planning, Registrar & University Secretary | • Development: SEG<br>• Coordination: VP – Planning, Registrar & University Secretary | • Development: SLG<br>• Coordination: VP – Planning, Registrar & University Secretary | • Development: accountable risk owners<br>• Coordination: VP – Planning, Registrar & University Secretary | • Development: SLG / Specialist Leads<br>• Coordination: VP – Planning, Registrar & University Secretary | • Development: Council / CARC / SEG<br>• Coordination: VP – Planning, Registrar & University Secretary | • Identification: SEG / SLG<br>• Coordination:, VP – Planning, Registrar & University Secretary |
| **Key tasks required** | • Review / refresh the risk profile via a workshop setting<br>• Validate with SEG members | • Consider high operational risks<br>• Review / refresh the risk profile via a workshop setting<br>• Validate with SEG members | • Review / refresh the risk profile via a workshop setting<br>• Validate it with SEG / SLG members | • Consult with accountable personnel for high / unacceptable risks to highlight to CARC<br>• Validate it with SEG / SLG members | • Define clear linkage of shared risks / support from functional risk areas<br>• Define clear responsibility<br>• Verify with SEG / SLG | • Consult with SEG / SLG to define risks tolerances per category and sub-category where required<br>• Confirm with CARC | • Consult with SEG members / functional risks owners to identify emerging looming risks<br>• Validate with SEG / SLG<br>• Highlight to CARC |
| **Timing** | • Reviewed on quarterly basis by SEG<br>• Significant changes reported to CARC at following meeting<br>• Annual review January | • Reviewed on quarterly basis by SEG / SLG<br>• Significant changes reported to CARC at following meeting<br>• Annual review October | • Reviewed on quarterly basis by SLG areas<br>• Significant changes reported to CARC at following meeting<br>• Annual review July | • Identified quarterly<br>• Reported to the subsequent CARC meeting | • Formally reviewed annually<br>• Informal review 6 monthly with functional leads and VP – Planning, Registrar & University Secretary | • Formal definition / review risk appetite / acceptable risk levels annually in May<br>• Reported to CARC at subsequent meeting | • Reviewed annually in May<br>• Identified / reviewed 6 monthly<br>• Reported to CARC at each meeting as a standing agenda item |
| **Scope and content** | • Risk profile of strategic risks including priority for treatment / monitoring | • Risk profile of enterprise risks including priority for treatment / monitoring | • Risk profile per business unit / area of risk including risks within the business unit and risk category that reside across the University | • Rolling report of all strategic and enterprise risks to the CARC to provide a specific update on each at least once annually | • Clear linkage / mapping of functional risk area responsibility in managing key risks including clear delineation of risk mitigation responsibility | • Definition of risk tolerances for each category and sub-category of risk where appropriate<br>• Overlayed to all risk ratings to identify gaps | • Report of any potential / actual emerging / looming risks which may become reality in future |

### h) Monitor and Review

- The context will generally be under constant change (hence the status of controls and risks will be under constant change), as will the status of various treatment options being undertaken. Ongoing monitoring and review of each of the steps of the risk management process is therefore required to ensure that the process continues to meet VU’s needs. In particular the following areas should be addressed:
  - External, internal and risk management contexts
  - The risks identified and subsequent analytical outputs
  - The continuing appropriateness of treatment plans and the efficiency and effectiveness of treatment options
  - Relevance and success of communications
  - Improvement opportunities for the conduct of the risk management process
  - The governance of the risk management process
  - Results of risk management practices should be reported and recorded internally and externally in accordance with the procedure.
  - Analysing and learning lessons from events, changes, trends, successes and failures
  - Identifying emerging risks.

## Annexure 1: Risk types

The following risk types are used as a checking mechanism to ensure that all sources / types of risk have been considered by management.

### Teaching & Learning

All activities related to delivering core services.
*e.g. Course portfolio is not attractive to the market.*

### Markets

Market sustainability and financial viability to drive growth, including the recruitment and management of students and research opportunities from chosen markets.
*e.g. Inability to grow Asian market.*

### Governance & Compliance

All activities in relation to good governance and complying with relevant legislation.
*e.g. Poor governance of strategic projects.*

### Operational

Activities that support the delivery of all core services.
*e.g. Processes are capable of changing with market needs.*

### People

The management of all people including staff and students.
*e.g. Not having the capacity and capability within the current workforce to deliver teaching, learning and research needs.*

### Infrastructure & Systems

Supporting assets and systems that enable the delivery of products and services.
*e.g. Buildings are not equipped to support the technological innovation required to meet student demand.*

### Financial

Availability of finances to maintain operations and implement strategic initiatives.
*e.g. Unavailability of funds to enact the strategy, limiting its effectiveness.*

### Health & Safety

Providing a safe workplace for all staff, students and those visiting campuses.
*e.g. Increased safety requirements as a result of previous failures, cause an inability to be agile.*

### Research

All activities related to the delivery of research in the form of grants and publications which contribute to the Universities rankings.
*e.g. Failure to commercialise research to grow new revenue stream and increase ranking's.*