

# Risk Management Procedure

## Section 1 - Purpose / Objectives

(1) This Procedure describes the processes to enable risks to be identified, assessed, mitigated, reported and reviewed.

## Section 2 - Scope

(2) This Procedure applies to:

- a. All staff, students, Council members, contractors, honorary and adjunct staff.
- b. All activities under the control or direction of the Victoria University ('VU'), whether conducted on or off University property.

## Section 3 - Definitions

(3) Nil

## Section 4 - Policy

(4) Refer to [Risk Management Policy](#).

## Section 5 - Procedures

### Part A - Summary of Roles/Responsibilities

(5) It is critical for the successful implementation of the risk management framework that there are clear accountabilities and responsibilities for the process.

(6) The overall responsibilities of various groups and individuals within VU are summarised in the table below.

Roles	Responsibilities
Council	<ul style="list-style-type: none"> <li>• Delegate risk management responsibility to the Compliance, Audit and Risk Committee (CARC).</li> <li>• Review all strategic and enterprise risks and significant operational risks.</li> <li>• Oversees CARC discharging its risk management responsibilities.</li> </ul>
Compliance, Audit and Risk Committee (CARC)	<ul style="list-style-type: none"> <li>• Ensures the risk management framework is being maintained by Management.</li> <li>• Elevate critical risks to the Council.</li> <li>• Approves the definitions of strategic, enterprise and operational risk profiles.</li> <li>• Approves the characterisation of specific risks as strategic, enterprise and significant operational risk.</li> </ul>

Roles	Responsibilities
Senior Executive Group	<ul style="list-style-type: none"> <li>Highlights any significant or emerging risks to CARC.</li> <li>Develops / refreshes the current strategic and enterprise risk registers which fall within CARC's approved profiles.</li> <li>Oversees the effectiveness of control mechanisms and treatment plan implementation for strategic and enterprise risks and significant operational risks.</li> </ul>
Senior Leadership Group	<ul style="list-style-type: none"> <li>Highlights significant operational risks to the Senior Executive Group (SEG).</li> <li>Develops / refreshes operational risk which fall within CARC approved profile.</li> <li>Implements effective control mechanisms and mitigation plans for operational risks.</li> </ul>
Planning and Performance Unit	<ul style="list-style-type: none"> <li>Collaborates with VU units and Colleges to embed risk management process and culture.</li> <li>Develops / refreshes the tools used to identify, assess, and manage risks.</li> <li>Maintains and updates records of strategic, enterprise and operational risks and provides a risk highlight report, at least quarterly to SEG.</li> <li>Provides proactive assistance, education and performance checks for all units and Colleges of VU.</li> </ul>
All staff	<ul style="list-style-type: none"> <li>Manage operational risks in their day-to-day roles.</li> <li>Bring any potential risks to the attention of management.</li> <li>Participate in the operational risk identification, recording and review processes whilst developing and implementing treatment plans where required.</li> <li>Following procedures and policies which govern the implementation of controls to manage risks.</li> </ul>

(7) Please see the Key Activities in Operationalising the Risk Management Framework, including who is responsible, accountable, consulted and informed as part of those activities.

(8) Greater detail regarding the activities of certain roles is found in the [Risk Management Framework Guidelines](#).

## Part B - General

(9) The purpose of these procedures is to implement the [Risk Management Policy](#). The process for managing Victoria University's risks is consistent with the risk management standard AS/NZS ISO 31000: 2009. The key steps include providing feedback through a monitoring, review and reporting process and appropriate communication and consultation.

(10) This is represented visually in Flowchart 1 and Flowchart 2.

### Characterisation of risks

(11) VU has defined three levels of risk:

- Strategic risks - risks which arise from, or threaten the success of the strategic choices that VU has made. They are often driven by change in the operating environment and ecosystem.
- Enterprise risks- risks so severe or material that their realisation could threaten the very survival of VU.
- Operational risks - risks which are managed within VU's units and Colleges and could jeopardise the achievement of their business plans. These risks may be escalated to the enterprise level if the impact would affect VU's license to operate or very existence.

### Step 1 - Communicate and Consult

(12) At the very start of any risk management activity, the answers to two simple questions should be sought:

- Who will have information that will be useful in identifying and managing risks?
- Who do I need to keep informed about what I am doing?

(13) The IRACI Communications Tool helps to ensure that appropriate persons are identified as stakeholders, and that these “providers” and “recipients” of information have their communication needs addressed during the risk management process. This should be considered for all risks identified to ensure that all stakeholders are communicated to.

## **Step 2 - Refresh Develop**

### **Set the context**

(14) 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.

(15) The key objectives of establishing the context are:

- a. To ensure that there is an appropriate level of understanding of the operations of the specific area of the VU under review;
- b. To determine the scope of the proposed risk management activity;
- c. To begin to identify the issues, constraints, etc. that could give rise to hazards, threats and risks.

(16) Establishing the context involves a consideration of the: external context, internal context and risk management context as further described in the [Risk Management Framework Guidelines](#).

### **Developing the evaluation criteria**

(17) 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.

## **Step 3 - Define ‘What Must Go Right’ to Achieve Objectives**

(18) Management needs to identify ‘What Must Go Right’ to achieve the objectives. This will be ‘What Must Go Right’ for the:

- a. Strategy for the strategic risk assessment;
- b. University to be financially viable and retain its license to operate for the enterprise risk assessment;
- c. Achievement of the unit / College business plan for the operational risk assessment.

## **Step 4 - Identify the Risks**

(19) At first, a broad list of possible risks should be developed but prioritisation of risks should lead areas to identify all high, major and moderate risks which would impact the achievement of VU’s objectives, whether or not they are under the control of VU.

(20) Risks are to be identified as they arise any time but risk management is a critical component of the development of VU unit or College's strategic plan; so that both operational and strategic risks are aligned with VU's strategic plan.

### **Risk Identification Methods**

(21) There are many methods for identifying risk, including:

- a. facilitated brainstorms, interviews, questionnaires, workshops, data analysis, stakeholder feedback;
- b. SWOT analysis; scenario planning and gap analysis are also useful management tools.

(22) Risks are likely to arise in the following circumstances:

- a. Lack of clarity about what needs to be done and what should not be done.
- b. When it is not clear who is responsible and who is accountable to deliver a key output and key outcome.
- c. When strategies are not clear and KPIs are not aligned with policy/project objectives.
- d. Lack of knowledge about university policies, stakeholder needs and government requirements.
- e. When decisions are made without analysing relevant, accurate and up-to-date data.
- f. Whenever there is a lot of staff turnover — including senior management.
- g. When managing a complex project that is new and/or challenging and/or requiring stakeholder engagement and/or requiring a whole-of-university approach.
- h. When a policy or program is not communicated well to key stakeholders.
- i. Lack of capability.
- j. Whenever organisational units experience a negative collegiate culture.
- k. When managing large expensive projects.
- l. When few are asked to do more work to compensate for the lack of resources.
- m. When organisations undergo drastic changes.

## **Step 5 - Analyse the Risk Level by Combining the Likelihood and Consequences Ratings**

(23) Risk analysis is about developing an understanding of the risk and the extent to which it can prevent an organisation achieving its goals.

(24) Once all risks have been identified they are analysed in terms of how likely the risk event is to occur (likelihood) and the possible magnitude (consequence) of the risk event.

(25) Rating Risk Likelihood (see Likelihood Criteria Table): requires an assessment of the risk's frequency of occurrence. The likelihood of a risk is rated on a score from 1 (rare) to 5 (almost certain).

(26) Rating Consequences (see Risk Consequence Rating) represent the magnitude of the risk or its impact if it were to occur — they are rated on a scale of 1 (insignificant) to 5 (catastrophic).

(27) The final ranking of a risk is obtained by combining the selected likelihood and consequence rating for each risk. Please see the [Risk Matrix](#). Note that 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.

(28) A risk assessment can generate a large number of risks and dealing with such a quantity in a meaningful way may well be beyond the capabilities, resources and time limitations of an individual assessment. It is therefore entirely appropriate to conduct an initial 'screening' assessment in order to create a 'shortlist' of risks for a more in-depth analysis.

(29) The consequence and likelihood criteria referred to above have been developed for most risk management activities down to project level. However, the applicability of these criteria needs to be examined as part of establishing the context for each individual risk assessment activity.

(30) The consequences reflect the amount and type of risk that VU is willing to accept in order to meet its strategic objectives. It is the responsibility of the Planning and Performance Unit to refresh this table if VU's risk appetite changes and to facilitate SEG obtaining CARC's approval of any such changes.

(31) The interrelation of risk across VU needs to be assessed and plotted in accordance with Risk Management Profile Structure and Responsibilities to ensure an holistic view of VU's risk is obtained and communicated.

## **Determining the Level of Risk**

(32) The level of risk is determined by aligning the consequence and likelihood using the risk rating matrix outlined above to derive a level of risk. As each risk will require different levels of management attention at different times based on the complexity of the control environment and factors causing the risk to exist, the management priority focus should be captured for each risk using the Risk Priority Rating.

## **Step 6: Evaluate Approach to Managing Risks**

(33) Each risk will need to be assigned a Risk Priority Rating, depending on the rating derived from the risk matrix and the ability of VU to control the risk. Further information is in the [Risk Management Framework Guidelines](#)).

(34) Mitigation strategies may include:

- a. Developing a decision making process including the assignment of authority and responsibility.
- b. Refinement of policies and practices.
- c. Addressing any gaps in the competence of personnel.
- d. Refreshing the communication of policies, procedures etc to internal staff and key stakeholders.
- e. Regular monitoring and reviewing of risk management actions to ensure that the reasons for taking the risk are met.

(35) Except in exceptional circumstances VU will only accept risks which have a final risk rating (as a result of mitigation strategies or otherwise) which is acceptable.

## **Step 7: Treat Risks**

(36) The person proposing that VU accept the risk must develop an action plan to mitigate these risks to an acceptable level (see [Risk Management Framework Guidelines](#)). Action plans must be implemented.

## **Step 8: Recording Risk**

(37) The Risk Management Form must be used to document the risk treatment for each risk. The form requires identification of the risk (including what is causing the risk); management action for each cause; a target date; the name of the person responsible to complete each action point.

(38) It is critical that there are clear and concise communication channels to provide management with the mechanisms to elevate specific risk information whilst providing the transparency and oversight to Council, CARC and SEG. The accuracy and timeliness of risk information is critical to providing the right information to specific groups so that they can make informed risk based decisions.

## **Risk Registers**

(39) Risk registers must be developed and maintained.

### **Strategic Risk Register**

(40) The Planning and Performance Unit is responsible for the planning and facilitation of any strategic risk register refresh.

(41) The register must be focused on risk to and from VU's strategic plan.

(42) SEG and the CARC will participate in annual workshops to develop and refresh the register of strategic risks.

(43) It is the responsibility of the Planning and Performance Unit to finalise the register of these risks and report to

SEG and CARC in accordance with the Annual Risk Planning and Review Cycle. Out of cycle reports must be made if there is a material change to VU's Strategic Plan.

### **Enterprise Risk Register**

(44) The Planning and Performance Unit is responsible for the planning and facilitation of the quarterly review and annual refresh of the enterprise risk register following the strategic register.

(45) The register must be developed based on risks identified in the strategic risk register related to operations and those risks identified in operational risk registers which, if they were to materialise, would result in significant consequences for VU.

(46) SEG will conduct quarterly reviews and annually refresh the enterprise risk register.

(47) It is the responsibility of the Planning and Performance Unit to finalise the enterprise risk register and report to SEG and CARC in accordance with the annual risk cycle in Annual Risk Planning and Review Cycle.

### **Operational Risk Register**

(48) The Planning and Performance Unit is accountable for ensuring that the quarterly review and annual refresh of the operational risk registers is completed by each VU unit and College.

(49) The operational risk registers must be developed based on risks to the achievement of VU units' and Colleges' business plans and the enterprise risks which affect the whole of VU.

(50) The head of VU's unit or College is responsible for ensuring that, on a quarterly basis, the operational risks are appropriately reviewed and updated. Annually a then operational risk register must be finalised.

(51) It is the responsibility of the Planning and Performance Unit to ensure that the operational risk registers are finalised so that it can report to SEG and report highlights to CARC in accordance with the annual risk cycle in Annual Risk Planning and Review Cycle.

(52) The [Risk Management Framework Guidelines](#) provide details regarding the requirements of reports.

## **Step 9: Monitoring and Reviewing risks**

(53) Monitoring and reviewing risks is an important part of risk management. It allows risk owners to identify any new risks arising or changes in existing risk rating due to changing circumstances and to review the extent to which risks have been mitigated.

(54) Risk owners should monitor and review risks regularly and ensure that changes are recorded in appropriate risk registers on an ongoing basis.

## **Step 10: Risk Management Continuous Improvement Cycle**

(55) The risk management methodology is aligned with the principles of continuous improvement. It requires all individuals and groups within VU to continually identify, assess, mitigate, review and report risks within their areas of operation, so that all risks are mitigated and managed to an acceptable level in accordance with the risk appetite that has been approved by CARC.

(56) The Risk Management Continuous Improvement Flowchart illustrates the risk management continuous improvement cycle.

## Section 6 - Guidelines

(57) Refer to [Risk Management Framework Guidelines](#).

## Status and Details

<b>Status</b>	Historic
<b>Effective Date</b>	8th August 2017
<b>Review Date</b>	8th August 2020
<b>Approval Authority</b>	Vice-President, Planning and Registrar
<b>Approval Date</b>	3rd August 2017
<b>Expiry Date</b>	16th November 2022
<b>Accountable Officer</b>	Matthew Walsh Chief Financial Officer officeofCFO@vu.edu.au
<b>Responsible Officer</b>	Anne Siegers Chief Risk Officer anne.siegers@vu.edu.au
<b>Enquiries Contact</b>	Thomas Odiero Senior Risk and Compliance Officer +61 3 9919 5345