

Risk Management Policy

Section 1 - Summary

(1) This Policy establishes Victoria University’s (VU) commitment to managing risk through implementation of a risk management framework and accountability structure.

Section 2 - Scope

(2) This Policy applies to:

- a. All staff, students, Council members, Committee members, contractors, honorary and adjunct staff.
- b. All activities under the control or direction of Victoria University, whether conducted on or off University property or in a digital environment.

Section 3 - Policy Statement

(3) Managing risk is an essential component of good governance and leadership. Effective risk management both creates and protects value in an organisation by improving decision making.

(4) To achieve its strategic objectives, the University must accept a measured degree of risk. Through the identification and analysis of risk, the University is able to be creative, adaptive and progressive in working to deliver its vision to be a global leader in dual sector learning and research.

Risk management principles

(5) VU’s risk management framework is based upon the International Standard for Risk Management [AS ISO31000:2018](#), consistent with the [Victorian Government Risk Management Framework](#) and takes into account key risk considerations of the [TEQSA](#) and [ASQA](#) risk frameworks.

(6) The framework is underpinned by the following principles:

Principle	Demonstrated by
A positive risk culture	<ul style="list-style-type: none"> • Creating a culture where risk identification and management is acknowledged as a driver of positive outcomes. • A culture where identifying and managing risk is accepted as everyone’s responsibility. • Driving excellence in corporate governance by increasing accountability, awareness and a positive attitude to risk management.
Accountability	<ul style="list-style-type: none"> • Clear accountability for each category of risk, individual risk and treatment plan to ensure action and monitoring is implemented.
Transparency	<ul style="list-style-type: none"> • Providing transparency and oversight to senior management and the University Council that strategic, enterprise and significant operational risks are managed effectively.
Risk based decision making	<ul style="list-style-type: none"> • Decision making, resource allocation and investment are prioritised and informed by risk analysis.

Principle	Demonstrated by
Embedded risk management	<ul style="list-style-type: none"> All operational functions and process should include a link to risk. Risk analysis and identification will include broad stakeholder consultation.
Informed investment	<ul style="list-style-type: none"> The consideration of the balance between risk and benefit in the development of investment strategies.
Informed resource allocation	<ul style="list-style-type: none"> Adoption of a risk-based approach to the allocation of resources to mitigate future risks.

Three Lines Model of Assurance

(7) VU adopts the Three Lines Model of Assurance to effectively coordinate and oversee enterprise risk management activity:

Line	Role	Key duties
First Line - management and internal controls	Vice Chancellor's Group and Senior Leadership Group	Identify and manage risk in daily operations, projects and pursuit of strategic objectives. Develop policies, procedures and controls to mitigate risks. Implement treatment plans to reduce risks where appropriate.
Second Line - oversight	Risk and Compliance	Develop and implement the enterprise risk management framework and tools. Provide advice, assistance and training in identifying, assessing and managing risk of all types. Drive self-assurance across the University by promoting clear accountability and respectfully challenging the first line activity. Coordinate monitoring, reporting and escalation of risk to appropriate bodies.
Third Line - assurance	Internal Audit	Undertake independent review of internal controls. Provide analysis and improvement insights to the Vice-Chancellor's Group (VCG). Provide assurance to Council on application and appropriateness of risk controls.

(8) The University Council approves the Risk Management Policy (this document), the Risk Appetite Statement and changes to the VU Risk Profile.

(9) It delegates to the Audit and Risk Committee (ARC) the responsibility to ensure that management has implemented the risk management framework, that it remains fit for purpose, and the authority to approve the Risk Management Procedure, including the articulations of risk tolerances.

(10) ARC will review and refer proposed changes to the VU Risk Profile prior to approval by Council.

(11) The Vice-Chancellor's Group is accountable for first and second line assurance activity, including managing risks, establishing controls, and providing guidance and monitoring within their areas of responsibility.

(12) University Council provides oversight, via the ARC, of the third line by receiving independent assurance from Internal Audit on the effectiveness of risk controls, internal governance processes and the overall adequacy of the University's risk management framework.

University risk management governance

(13) VU manages risk across two interconnected domains, including Enterprise Risk Management and Local Risk Management. These domains operate at different management levels and utilise separate frameworks to support

integrated risk management across the University.

(14) The University has defined four fundamental types of risk within the enterprise risk management framework with varying accountabilities to enable effective management of risk and appropriate self-assurance:

Risk Type	Domain	Ownership
Strategic Risk	Enterprise	Vice-Chancellor's Group
Institutional Risk	Enterprise	Vice-Chancellor's Group Member
Portfolio risk	Enterprise	Portfolio Lead
Operational risk	Enterprise	College/Research Centre/Department Lead

Enterprise risk management framework

(15) The enterprise risk management framework forms part of the University's governance system. The primary purpose of the framework is to enable coordinated and consistent identification and management of all university risks and generate appropriate assurance to support strategic and operational decision making by senior leaders.

(16) VU's enterprise risk management framework comprises:

- a. [Risk Management Policy](#)
- b. [Risk Management Procedure](#)
- c. [Risk Appetite Statement](#)
- d. [Risk Matrix](#)
- e. Risk Management System

(17) There are four fundamental types of enterprise risk recognised by the enterprise risk management framework, comprising Strategic, Institutional, Portfolio and Operational risk profiles.

Enterprise Risk Type	Defining Characteristics
Strategic Risk	Risks that could impact achievement of strategic objectives and are linked to the strategic plan. Typically large scale, long horizon or external scenarios outside the University's control.
Institutional Risk	University-wide risks with potential to threaten sustainability or licence to operate. Large or complex internal threats identified through strategic reviews and enterprise-level oversight.
Portfolio Risk	Cross-directorate risks affecting a collective portfolio and common operational themes. Often linked parent-child relationships with operational risks across Colleges/Research Centres/Business Units.
Operational Risk	Risks associated with operational plans and activities carrying potential for enterprise-level impacts. May reflect themes shared across areas that inform parent Portfolio risk

Local risk management frameworks

(18) Local frameworks may be developed to manage operational-level risks where enterprise tools are not suited, provided they support good practice risk management.

(19) These local approaches must not override, replace or conflict with the Enterprise Risk Management Framework.

(20) First line areas may design their own tools, categories, rating criteria and escalation processes if effective for local needs and not contradictory to enterprise requirements.

(21) Local frameworks must be documented in operational policies or procedures, with Risk and Compliance providing guidance to ensure alignment with University expectations and integration with enterprise reporting and escalation pathways.

Section 4 - Procedures

(22) [Risk Management Procedure](#)

Section 5 - HESF/ASQA/ESOS Alignment

(23) HESF: 6.2.1e Corporate Monitoring and Accountability, 6.3.2d Academic Governance

(24) Outcome Standards for NVR Registered Training Organisations 2025: Standard 1.8 Facilities, Equipment and Resources; 4.3 Risk Management.

Section 6 - Definitions

(25) Accountability: Responsibility for ensuring that risk is appropriately managed including the implementation of treatment plans and monitoring the effectiveness of controls.

(26) Contributing Factors: Factors internal and external that contribute to the risk existing or could result in the risk materialising.

(27) Controls: The existing actions, activities or mitigation strategies in place to prevent the risk from materialising.

(28) Consequences: The outcome of a risk event or situation, being a loss, injury, disadvantage or gain.

- a. An event can lead to a range of consequences.
- b. A consequence can be certain or uncertain and can have positive or negative effects on objectives.
- c. Consequences can be expressed qualitatively or quantitatively.
- d. Initial consequences can escalate through knock-on effects.

(29) Likelihood: The chance or probability of a risk materialising.

(30) Risk: The effect of uncertainty on objectives:

- a. A deviation from the expected – positive or negative and can result in opportunities or threats.
- b. Objectives will have different aspects such as financial, academic, people, service delivery, reputation, legal and regulatory, cybercrime and data security and will be managed at different levels such as strategic, enterprise or operational.
- c. Risk is often categorised by reference to sources of risk or potential events, consequences and their likelihood of occurrence.

(31) Risk Appetite: The amount and type of risk that the University is willing to take in order to meet its strategic objectives.

(32) Risk Categories: Broad categories of risk that the University uses to identify and group risks.

- (33) Risk Management: The coordinated management of activities to direct and control the University with regard to risk.
- (34) Risk Tolerance: The acceptable range of risk rating within which the University will seek to maintain each risk.
- (35) Treatment Plan: Actions that will be taken to reduce the likelihood or consequence of a risk occurring.

Status and Details

Status	Current
Effective Date	4th June 2026
Review Date	4th June 2029
Approval Authority	University Council
Approval Date	4th June 2026
Expiry Date	Not Applicable
Accountable Officer	Matthew Walsh Chief Financial Officer officeofCFO@vu.edu.au
Responsible Officer	Anne Siegers Chief Risk Officer anne.siegers@vu.edu.au
Enquiries Contact	Adam Mills Manager, Risk +61 3 9919 4280