Risk Management - Procedures

1. Purpose of procedures

1.1 In accordance with the Enterprise Risk Management Framework – Governing Policy, these procedures describe the University's standard process for risk management, including:

(a) risk identification;

(b) risk analysis;

(c) risk evaluation; and

(d) risk mitigation and control (including risk treatment).

1.2 A standard approach to risk management allows risks to be correctly prioritised across all of the University's operations. Resultingly, effective controls can be put in place to ensure the University is able to manage its operations effectively, now and into the future.

1.3 These procedures apply to all activities undertaken in the course of University business, whether on University campuses or other locations.

1.4 These procedures must be read in conjunction with the Enterprise Risk Management - Governing Policy.

2. Scope and application

2.1 These procedures apply to all staff and members of the University decision-making or advisory bodies.

3. Definitions

3.1 Refer to the University's Glossary of Terms for definitions as they specifically relate to policy documents.

Risk management refers to the set of coordinated activities to direct and control an organisation with regard to risk.

Risk is the effect of uncertainty upon the University's objectives. Risk may have a positive or negative impact.

Likelihood measures the expected frequency of a risk occurring. Typically, it is a subjective judgement based on past experience and the insights of persons familiar with the activity.

Consequence measures the expected level of impact on the University and its objectives, should the risk occur.

Risk owner is an individual within the University with primary responsibility for managing a particular risk.

Risk Event is an occurrence or change of particular circumstances.

Control is a measure that maintains and/or modifies risk.

Risk Source is an element which, alone or in combination, has the potential to give rise to risk.

Risk Appetite conveys the degree of risk the University is prepared to accept in pursuit of its business objectives and strategic plan.

Risk Appetite Framework is the overall approach, including policies, processes, controls and systems through which appetite is established, communicated and monitored.

Risk Management Framework is the totality of systems, structures, policies, processes and people that identify, measure, monitor and mitigate risk.

Inherent Risk is an assessment of the likelihood and consequence if the risk being realised. It is the level of risk if the risk is to be realised with no controls in place.

APPROVAL AUTHORITY

Vice-Chancellor and President

RESPONSIBLE EXECUTIVE MEMBER

Vice-Chancellor and President

DESIGNATED OFFICER

Director, Governance and Risk Management

FIRST APPROVED

27 April 2006

LAST AMENDED

30 October 2023

REVIEW DATE

30 October 2024

STATUS

Active

Residual Risk is an assessment of the likelihood and consequence once controls have been implemented to manage, monitor and/or mitigate the risk. The residual risk is generally lower than the inherent risk and should fall within the University's risk appetite.

4. Principles

4.1 In accordance with the University's Enterprise Risk Management – Governing Policy and adapted from the standard ISO 31000: 2018 Risk Management – Guidelines, the following principles have been identified:

(a) Integrated: Risk management is an integral part of all organisational activities.

(i) Risk management applies to all areas of the University and as such, is an integral part of the University's organisational processes. This includes strategic planning, operational planning, project management and change management. The intention is for risk to be used to inform decision making and is the responsibility of all staff.

(b) Structured and comprehensive: A structured and comprehensive approach to risk management contributes to consistent and comparable results.

(i) The approach to risk management across the University is consistent. All areas of the University are required to identify and assess risks and identify controls using consistent processes with reference to the University Risk Tables.

(c) Customised: The risk management framework and processes are customised and proportionate to the organisation's external and internal context related to its objectives.

(i) Risk management is tailored to the University. The tools and processes for managing risks are aligned with the strategic and business planning process and are reviewed on a regular basis. The Risk Management Framework is dynamic and is updated to reflect changes to the internal or external environments.

(d) Inclusive: Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

(i) The University takes a collaborative approach to risk management. Risks and controls are discussed with each area, the risk profile is circulated for feedback and at the Risk Management Committees and forums, there is open dialogue on risk management, including emerging risk issues.

(e) Dynamic: Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

(i) The University's approach to risk management is dynamic. When internal or external changes occur, they are considered as part of the updates to affected business unit risk profiles, and the Risk Management Strategy. Those changes are also considered within relevant policy, processes and procedures supporting risk management.

(f) Best available information: The inputs to risk management are based on historical and current information, as well as on future expectations.

(i) Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

(ii)The University's risk management practices are forward looking and include both leading and lagging indicators of risk.

(g) Human and cultural factors: Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

(i) The University aims to promote a culture which encourages strong risk management. This is reinforced through the University's risk appetite and by training and communications.

(h) Continual improvement: Risk management is continually improved through learning and experience.

(i) The University's approach to risk management is continually improved to reflect best practice.

5. Risk management process

5.1 Process Overview

5.1.1 The Enterprise Risk Management - Governing Policy identifies that the risk management process and procedures will be consistent with ISO 31000:2018 Risk Management – Guidelines. The table below is adopted from this standard.

Figure 1: ISO 31000:2018 risk management process

5.2 Scope, Context, Criteria

5.2.1 By establishing the scope, context and criteria, the University will be able to articulate its objectives and define the external and internal parameters to be considered when managing risk, as well as set the scope and risk criteria for the remaining process.

5.3 Risk Identification

5.3.1 Risk identification requires reasonably foreseeable risks that have the potential to have a meaningful impact on the University to be identified. A risk is any event or action that has an uncertain effect that may impact on the University's objectives. Risks arise as much from the possibility that opportunities will not be realised as they do from the possibility that threats will materialise, errors made, or damage or injury to occur. The University also commits to , and where appropriate, undertaking scenario plan testing for 'black swan' risk events which are 'unpredictable events that are beyond what is normally expected of a situation and has potentially severe consequences.'

5.3.2 Within the University, risk identification occurs at various levels:

(a) Strategic risk identification: Strategic risks are identified as part of the strategic planning process. They are documented in the University's Strategic Risk Register. Identification at this level is aimed to inform strategic decision making to allow the University to improve outcomes while minimising adverse impacts on the University's goals and objectives.

(b) Organisational or Operational risk identification: Organisational or Operational risks are identified on an ongoing basis and are documented in the Organisational or Operational Risk Register (note that Organisational or Operational risks are sometimes referred to as the 'corporate risks' of the University).

(c) Departmental or School risk identification: Risks associated with Departments, Schools and Research Centres and Institutes are identified on an ongoing basis and are required to be documented in the Departmental or School Risk Registers. These risks are the risks at the local level of the University. Risk registers are reviewed on a quarterly basis to ensure that the identification and treatment of risks is managed on a timely basis.

(d) Project risk identification: These risks are generally associated with significant change or project activities. They are normally identified at the commencement of a new project and updated over the life of the project. Project Managers are responsible for documenting these risks within Project Risk Registers, with mitigating actions in place to manage the project risks. When operationalised, any remaining residual risks should be incorporated into the appropriate Department or School Risk Registers.

(e) Ad-hoc or activity-based risk identification: Risks can be identified by staff during their normal University work. A risk assessment is required to be undertaken for all relevant University activities. This risk assessment is completed by the relevant business unit in consultation with relevant stakeholders involved in undertaking the activity. This includes representatives from work, health and safety and governance and risk management.

(f) Targeted Risk identification: Targeted risk registers will be developed for specific areas of focus that may cross multiple business units (e.g., Cyber, Fraud or Health and Safety). The need for these items will be identified by Executive members and delegated to relevant business owners throughout the organisation.

5.3.3 All identified risks are to be entered in the relevant Risk Register or completed as part of a Risk Assessment. Risks are owned by each relevant business unit. As a minimum, the following information must be included:

(a) a description of the risk;

(b) the causes and implications of the risk; and

(c) the assigned risk owner.

5.3.4 In addition, the following information, if known, is to be included:

(a) details of the existing controls in place to manage/mitigate the risk;

(b) the inherent risk rating as determined by the assessment of the potential consequences and likelihood for the risk;

(c) details of any additional controls, including a due date for implementation; and

(d) the residual risk rating, as determined by the assessment of the consequences and likelihood, after the implementation of controls.

5.4 Risk Analysis

5.4.1 Risk analysis involves developing an understanding of the risk and provides an input to risk evaluation and to decisions on whether risks need to be treated, and if so, on the most appropriate risk treatment methods. This analysis can also provide input into the options to address risks and inform the decision making required across different types and levels of risk.

5.4.2 Risk analysis should seek to identify potential causes and sources of risk in order to analyse their consequence and the likelihood that the consequence will occur.

5.4.3 All risks within the University are assessed using a common scale that considers:

(a) the potential consequences if the risk were to occur; and

(b) the likelihood of the University being impacted in that way.

5.4.4 The consequence and likelihood are then used to rank the risk in accordance with the following four categories:

(a) Extreme;

(b) High;

(c) Medium; and

(d) Low.

5.4.5 This analysis which is undertaken based on the existing status of the risk, with consideration of the controls that may already be in place, identifies the inherent risk (i.e. the risk prior to the implementation of any controls) and the residual risk (the risk rating after the application of controls in the below sections). This common approach to risk rating is necessary to ensure that the most significant risks to the University can be readily identified and prioritised in a way that has the greatest overall benefit to the University.

5.5 Risk Evaluation

5.5.1 The purpose of risk evaluation is to assist in making decisions, based on the outcome of risk analysis, about which risks need treatment and the priority for treatment implementation.

5.5.2 Decisions should take account of the wider context of the risk and include consideration of the University's risk appetite and tolerances across categories of University activity as well as the actual and perceived consequences to external and internal stakeholders. Legal, regulatory and other requirements may also impact on the evaluation.

5.5.3 The rating of a risk, together with the categories of University activity and the related risk appetite as identified within the UniSC Risk Appetite Statement, are used to determine:

(a) the urgency with which action should be undertaken;

(b) the nature of the action that is required;

(c) the reporting requirements for the risk; and

(d) how the risk is to be monitored.

5.5.4 That is, this risk evaluation identifies risks where the inherent risk is greater than risk tolerances and therefore also identifies where risk treatment is required to further manage the risk.

5.6 Risk Treatment

5.6.1 Controls and mitigating actions are required for all risks to ensure they are within the University's risk appetite. Where a risk is outside appetite, a risk treatment is required. This involves selecting one or more options for modifying the risk and implementing those options. Risk treatment is required when the residual risks remain unacceptably high, or where there is a desire to bring this risk down, with regard to the University's risk appetite. Once implemented, treatments provide or modify the controls.

5.6.2 Risk treatment involves an iterative process of:

(a) formulating and selecting risk treatment options;

(b) planning and implementing risk treatment;

(c) assessing the effectiveness of that treatment;

(d) deciding whether the remaining risk is acceptable; and

(e) if not acceptable, taking further treatment.

5.6.3 Risk treatment options are not necessarily mutually exclusive. Nor may they be appropriate in all circumstances when due consideration is given of the current risk appetite. The purpose of this step is to put in place one or more options (controls) to reduce the level of residual risk to a level that is considered acceptable by the University.

5.6.4 Selection of the most appropriate treatment options involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.

5.6.5 Treatment options include:

(a) Avoid the risk: by deciding not to proceed or continue with the activity or choosing an alternative approach to achieve the same outcome. The aim is risk management, not aversion.

(b) Mitigate: Reduce the likelihood by improving management controls and procedures. Reduce the consequence by putting in place strategies to minimise adverse consequences.

(c) Transfer the risk: Shifting responsibility for a risk to another party by contract or insurance. It can be transferred as a whole or shared.

(d) Accept the risk: Controls are deemed appropriate. These must be monitored and contingency plans developed where appropriate.

5.6.6 A common approach to risk rating is necessary to ensure that the highest rated risks to the University can readily be identified and management of risks can be prioritised in a way that has the greatest overall benefit to the University. Further guidance on risk rating including assigning a consequence and likelihood can be obtained within the Risk Tables.

6. Recording and Reporting

6.1 The risk management process and its outcomes are reported to the Executive Committee and the Audit and Risk Management Committee. Outcomes are also made available to staff where appropriate. This assists with decision making, improving risk management and transparency and the monitoring of risks against the University's stated risk appetite.

END

RELATED DOCUMENTS

- Audit and Assurance Framework - Governing Policy
- Compliance Management Framework - Governing Policy
- Fraud and Corruption Control - Governing Policy
- Fraud and Corruption Control - Procedures
- Risk Management - Governing Policy

LINKED DOCUMENTS

- Risk Management - Governing Policy

RELATED LEGISLATION / STANDARDS

- University of the Sunshine Coast Act 1998 (Qld)
- Financial Accountability Act 2009 (Qld)
- ISO 31000:2018 Risk Management Guidelines