Risk Management Policy

Section 1 - Purpose

(1) The purpose of this policy is to establish the expectations and approach to risk management at Charles Sturt University (the University) as part of the University's governance responsibilities and obligations under Section 19 (1B) of the Charles Sturt University Act 1989 and also the Voluntary Code of Best Practice for the Governance of Australian Universities by Universities Australia.

(2) The objectives of this policy are to:

a. develop an inclusive and risk aware culture while maintaining institutional innovation and agility to identify and realise opportunities;
b. establish a consistent, systematic and demonstrable approach to risk management at the University;
c. incorporate organisational risk management as part of the University's strategic planning and management process;
d. integrate the management of risks into day-to-day management and accountability processes; and
e. define clear roles and responsibilities for managing risks at the University.

Scope

(3) This policy applies to all academic and professional/general staff of the University, controlled entities, partnerships, contractors and adjunct staff.

Section 2 - Glossary

(4) For the purpose of this policy, the University has adopted the following definitions:

a. Academic risks – risk of failure in academic quality or of students not achieving learning outcomes.
b. Controlled risk – residual risk after implementation of risk treatments.
c. Inherent risk – risk exposure prior to the implementation of internal controls.
d. Internal control – measure that maintains and/or modifies risk.
e. Managers – primary or secondary manager or manager, as defined in clause 3 of the Delegations and Authorisations Policy.
f. Other risks – risks that are not classified as a principal or academic risk. Other risks include operational, financial, and compliance risks.
g. Principal risks - risks that are directly linked to the achievement of the University’s strategic objectives.
h. Risk – effect of uncertainty on objectives.
i. Risk appetite – degree of risk, on a broad-based level, that the University is willing to pursue or retain.
j. Risk management – coordinated activities to direct and control an organisation with regard to risk.
k. Risk management process – systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

l. Risk matrix – defined risk likelihood and consequence thresholds aligned to the organisational context and used to determine the inherent and controlled risk ratings.
m. Risk owner – the person accountable for managing a particular risk.
n. Risk rating – level of exposure to a risk based on the likelihood and consequence of the risk occurrence.
o. Risk register – management tool that documents risks identified by the University by describing the characteristics of risks (e.g., risk description, risk category, potential causes or risk factors, risk ratings, risk treatments).
p. Risk treatment – an iterative process to select and implement options for addressing risks that exceed the risk appetite (e.g., enhancing controls).
q. The Standard – International Standard for Risk Management: ISO 31000:2018, Risk Management – Guidelines.
r. University Risk Management System – Charles Sturt University system or tool used to identify, analyse, monitor and report on risks.

Section 3 - Policy

Risk management standard

(5) The University adopts risk management principles and processes in accordance with the International Standard for Risk Management: ISO 31000:2018, Risk Management – Guidelines.

(6) Effective and efficient risk management is based on the eight principles identified in the Standard:

a. Integrated – be an integral part of organisational activities and/or processes;
b. Structured and comprehensive – risk management should be structured and comprehensive to enable consistent and comparable results;
c. Customized – approach and processes are fit for purpose for Charles Sturt University;
d. Inclusive – all relevant stakeholders' knowledge, views and perceptions are to be considered;
e. Dynamic – risk management processes identify, manage and respond to changes and events in an appropriate and timely manner;
f. Best available information – information should be timely, clear and available to relevant stakeholders;
g. Human and cultural factors – considers human behaviour and cultural factors that significantly influence Charles Sturt University's risk management; and
h. Continual improvement – risk management practices and systems are continually improved through learning and experience.

Risk management process

(7) The University has established a risk management process, based on the Standard, to assist responsible parties to effectively manage risks. The Risk Management Procedure provides guidance for implementation of the risk management process.

Scope, context, and criteria

(8) Risk management applies to all enterprise levels of the University responsible for forming and pursuing objectives. For the purposes of this policy, enterprise levels include:

a. whole of organisation (entity-level);
b. portfolio;
c. business unit (faculty, division, centre, office); and

d. unit (school, office, unit, institute or centre),

where the latter two are defined in the Delegations and Authorisations Policy. Risk management also relates to specific-purpose and temporary endeavours within enterprise levels, such as projects and events.

(9) When determining the scope of risk management, consideration will be given to the external and internal context in which the University seeks to define and achieve its objectives.

(10) The amount and category of risk that the University is willing to take in the achievement of its objectives is established by the University Council and documented in the Risk Appetite Statement. Risks are assessed against the risk appetite based on the Risk Management Guidelines.

Risk assessment

(11) Risk assessment is the process of identifying, analysing, and evaluating risk according to the predefined criteria referred to in clause 10.

(12) The purpose of risk identification is to formally document risks that might prevent the achievement of University objectives. Identified risks are documented in the risk register with respect to the enterprise level at which they apply, risk category, responsible officer, and associated controls. Risk identification results in an inherent risk rating based on the likelihood and consequence of their occurrence, as per the Risk Management Guidelines.

(13) Once identified, risks are analysed to determine the level of University exposure to risks, considering the design and implementation, as well as the operating effectiveness, of existing internal controls, processes, and structures. Risk analysis may draw from a range of quantitative and qualitative techniques to generate a controlled risk rating for identified risks.

(14) Risk evaluation complements risk analysis to determine whether or not controlled risks reside within the corresponding risk appetite of the University. Controlled risks rated equal or below the risk appetite level may attract no further action. Conversely, controlled risks that exceed the risk appetite require further treatment to reduce the University’s exposure to acceptable levels.

Risk treatment

(15) The purpose of risk treatment is to respond to risks evaluated as falling outside the corresponding risk appetite level established in the Risk Appetite Statement. Risk treatment options are varied and can range from, for example, avoiding the risk by not engaging in a given activity, to sharing the risk through insurance contracts, to changing the risk likelihood and consequences by implementing or enhancing internal controls, through to retaining the risk by informed decision. Selecting appropriate risk treatment options entails balancing benefits and costs, whether tangible or intangible, in relation to the achievement of objectives.

(16) Implementing new and/or improving existing internal controls is a common risk treatment option to reduce exposure to risks. Internal controls, when implemented effectively, may bring the controlled risk rating to a level commensurate with the risk appetite. For documentation purposes, internal controls are to be considered ‘treatments’ until they are fully implemented; after which point they are to be listed as ‘controls’ within the risk register.

(17) Where no viable risk treatment option is available to reduce risk exposure, the Executive Leadership Team and the Vice-Chancellor may propose to the Audit and Risk Committee to retain the risk based on informed decision. The Audit and Risk Committee will consider the proposal and make a recommendation to the University Council to accept the risk at existing levels.

Monitoring and review

(18) The purpose of monitoring and review is to ensure that the risk management process is operating effectively as

external and internal contexts change. Monitoring and review can either be carried out formally or informally, including: management reviews (e.g., risk self-assessments); independent reviews (e.g., internal audit); and continuous informal reviews (e.g., discussing emerging risks in meetings).

Recording and reporting

(19) The University risk register serves as the central repository of risk data and information, including those pertaining inherent and controlled risk ratings derived from risk assessments, risk treatments, and risk management responsibilities and accountabilities.

(20) The risk register is the basis for internal risk reporting to enable decision makers to fulfil their risk management obligations. It does so by communicating risk management activities and outcomes, providing information for decision-making, and ensuring consistency of risk-related information across the University. Internal risk reporting processes are carried out through existing management and governance structures as documented within the University's Risk Appetite Statement.

(21) The risk register also provides data and information for reporting to external stakeholders, such as sector regulators.

Risk management responsibility

University Council

(22) The University Council (Council) has primary responsibility, under Section 19 (1B) of the Charles Sturt University Act 1989, for:

a. overseeing risk management (including risk assessment) across the University and its controlled entities;
b. promoting a culture that supports strategically driven decision making within a framework of public accountability;
c. approving the risk appetite of the University and the University's attitude to risks with respect to particular major issues;
d. approving major policies in relation to risk management; and
e. approving major decisions affecting the University's risk profile or exposure.

(23) The Council is also responsible for:

a. reviewing overall risk mitigation strategy for principal, whole of organisation, and academic risks; and
b. approving the acceptance of risks exceeding the risk appetite, as per the Risk Appetite Statement.

Audit and Risk Committee

(24) The Audit and Risk Committee is responsible, on behalf of the University Council, under the Governance (Audit and Risk Committee) Rule 2022, for oversighting and granting relevant approvals with respect to risk activities. This includes reviewing risk assessments within the University and the internal control systems in place to underpin this assessment, including the University's risk register, Risk Appetite Statement and risk management related policies and procedures in order to make any necessary recommendations to the Council.

(25) The Audit and Risk Committee is also responsible for reviewing treatment plans relating to principal, whole of organisation, and academic risks that exceed the risk appetite, as per the Risk Appetite Statement, or when their corresponding risk ratings increase.

Vice-Chancellor and Executive Leadership Team

(26) The Vice-Chancellor and the Executive Leadership Team is accountable to Council for risk management and is responsible for ensuring the:

a. identification and appropriate management of the Principal risks faced by the University, including the provision of adequate and timely information to the Council, principally through the Audit and Risk Committee;
b. identification and appropriate management of Other risks throughout the University through the implementation of the risk management process and subsequent development and implementation of risk treatments; and
c. reviewing the relevant risk report and establishing or updating the organisational risk treatments for all relevant risks;

(27) The Executive Leadership Team is also responsible for establishing risk mitigation strategies for principal and whole of organisation risks that exceed the risk appetite, as per the Risk Appetite Statement, and also approve the entry of all new risks into the risk register.

Academic Senate

(28) Academic Senate is responsible for the following functions:

a. exercising academic governance of the University on behalf of the University Council through institutional oversight, risk management and reporting to the Council on academic standards compliance, academic risk, quality and outcomes in teaching, learning, research, as well as research training;
b. providing advice and recommendations to the University Council and University management on academic matters, including advice on academic outcomes, policies and practices;
c. requiring the production and submission of reports in relation to academic issues from, or referring academic matters to; management, faculties, other organisational units or committees for consideration and action as required;
d. setting and monitoring institutional benchmarks for academic quality and outcomes, and as necessary initiating action to improve performance against these benchmarks; and
e. reviewing relevant risk reports and organisational risk treatment actions for academic risks, including for those that exceed the risk appetite, as per the Risk Appetite Statement.

(29) While being accountable to the University Council, Academic Senate may delegate its academic risk oversight responsibilities to its sub-committees.

Portfolio leaders

(30) Members of the Executive Leadership Team are responsible for ensuring that risk management processes are implemented in their respective areas of responsibility. This includes:

a. ensuring key principal, academic, and other risks within their areas of responsibility are identified and documented as required in this policy and associated documents;
b. accepting ownership of the risks identified and be satisfied that the appropriate risk treatments are in place to manage risks to acceptable levels;
c. escalating and reporting on significant risks;
d. ensuring the inclusion of risk management responsibilities in duty statements, induction, professional development and performance management processes for all staff within their areas of responsibility; and
e. updating their respective risks in the risk register.

Managers

(31) Managers of the University are responsible for incorporating risk management into their standard management practices by:

a. understanding the University's risk management process and fostering a risk aware culture within their areas of responsibility;
b. identifying and determining appropriate actions to address risks within their area of responsibility in accordance with University policies and procedures;
c. documenting their risk management processes;
d. upward reporting of emerging risks; and
e. ensuring the inclusion of risk management responsibilities in duty statements, induction, professional development and performance management processes for all staff within their area of responsibility.

Project managers

(32) Project managers of the University are responsible for incorporating organisational risk management into their project management methodology and practices by:

a. understanding and employing the University's risk management framework and methodologies in the delivery of projects;
b. identifying appropriate risk treatment actions to manage risks to an acceptable level; and
c. upward escalation (where required) and reporting of significant emerging risks to the Project Sponsor or Control Group.

Risk and Compliance Unit

(33) The role of the Risk and Compliance Unit is to facilitate and provide advice on the implementation of the elements of the University's Risk Management Policy and continuously improve the University's risk management framework. This includes:

a. establishing supporting processes, tools and advice to facilitate effective risk management;
b. facilitating periodic principal, academic, and other risk assessments for the identification, analysis, evaluation, and reporting of the University's risk profile to the Executive Leadership Team, Audit and Risk Committee, Academic Senate, and Council;
c. preparing, developing and presenting all relevant periodic risk reports;
d. operating and maintaining the University's risk management system;
e. reviewing risk registers prepared and maintained by University portfolio leaders for completeness, accuracy, clarity and quality of risk information;
f. working with staff members across the University to assist with the embedding of risk management processes into operational, management and strategic processes; and
g. establishing a capability development framework to support the University's risk management practices.

Internal Audit function

(34) The role of the Internal Audit function is to provide independent advice through the conduct of internal audit activities on the effectiveness of the mitigation controls or strategies for managing risk in the University.

(35) Internal Audit will also independently assess the effectiveness of risk management practices across the University against the Risk Management Policy and Procedure and related processes.

All academic and professional/general staff members

(36) Staff members (including contractors and adjunct staff) are required to be aware of the University's risk management activities and contribute towards building a strong risk management culture. This includes:

a. undertaking responsibility to perform tasks and duties diligently and effectively, contributing to effective operational risk management; and
b. bringing to the attention of their managers/supervisors:
    i. risks within their areas of operation which may not be well mitigated and may affect the performance and reputation of the University; and
    ii. risks that should be escalated according to the Risk Management Guidelines.

Directors of controlled entities, centres and institutes

(37) Directors of controlled entities, research centres and institutes are responsible for overseeing the risk management practices in their organisations in accordance with this policy.

Performance

(38) The University Council, through the Audit and Risk Committee will monitor and evaluate the University's performance in relation to risk management. This will be informed by a periodic assessment facilitated by Internal Audit (or an external independent assessor if necessary) covering:

a. the effectiveness of the implementation of the risk management framework across the University and its controlled entities;
b. the awareness of managers and staff of their responsibilities, including appropriate professional development and performance management in relation to risk management;
c. the existence of risk assessments for all major activities, including all commercial activities;
d. the identification of risk management responsibilities in duty statements, induction, professional development and performance management processes for all staff of the University and its controlled entities; and
e. the currency of the principal and portfolio risk assessments, including the effectiveness of controls and the completion and effectiveness of the additional risk treatments.

Authority

(39) The University Council is the only authority that may approve this policy and other policies relating to risk management. (Refer to the Delegations and Authorisations Policy and Delegation Schedule A - Governance and Legal.)

Review

(40) This policy will be reviewed periodically.

Section 4 - Procedure

(41) Refer to the Risk Management Procedure.

Section 5 - Guidelines

(42) Nil.

Status and Details

Status	Current
Effective Date	22nd June 2020
Review Date	29th February 2024
Approval Authority	University Council
Approval Date	22nd June 2020
Expiry Date	Not Applicable
Unit Head	Dugald Hope Director, Risk and Compliance
Author	Marcos Tabacow
Enquiries Contact	Risk and Compliance Unit