Risk Management Policy

Section 1 - Purpose

(1) Managing risk is an essential part of everyone's role at Charles Sturt University (the University) and supports the University in delivering its 2030 vision and strategic goals. Effective identification and management of risk protects the University's teaching and research, people (staff, students and community), resources and reputation.

(2) The objective of this policy is to:

a. create a strong risk culture where all staff are encouraged to proactively manage risks in their day-to-day activities
b. promote an environment where informed decisions to identify and manage the University's risks are made in an open and consistent manner, and in accordance with the University's Risk Appetite Statement
c. define responsibilities and governance structures to support risk management and compliance management, and
d. outline the University's approach to continuous improvement and providing assurance on the effectiveness and reliability of controls and other activities designed to manage risk and compliance.

(3) This policy leverages the principles of ISO 31000:2018 Risk Management – Guidelines.

Scope

(4) This policy applies to all staff of the University, students, customers, volunteers, contractors, education partners and third-party service providers of the University and its controlled entities.

Section 2 - Policy

Risk culture

(5) Risk culture refers to the University's attitude to risk management and the norms of behaviour for individuals and groups of staff that influence the ability to identify, understand, openly discuss, escalate, and act on current and future challenges and risks.

(6) All staff actively engage in risk management in their areas of responsibility. Risk is managed both informally through robust day-to-day operations and decision making and also formally through structured risk assessment processes such as the University's delegations and authorisations, strategic and annual operational planning processes, annual risk control self-assessment (RCSA) process and governance reporting.

(7) The University's approach to maintaining an appropriate risk culture is based on the following principles, which support the effectiveness of the risk management framework and allow the University to operate within its Risk Appetite Statement.

a. Governance and leadership – The University's governance structure provides effective oversight and drives effective risk management. The University Council (Council) and Executive Leadership Team set an appropriate ‘tone at the top’ and, through their actions and decisions, role model expectations of our staff.

b. Expectations and accountability – Roles and responsibilities are clearly defined. Staff understand expectations around how they act, solve problems and make decisions. The University focuses on identification, management and reporting of risks. Staff feel safe to escalate issues quickly and confidently.
c. Risk management practices – The University has a clearly articulated and well understood risk management framework and supporting processes to allow timely identification, assessment and management of risks.
d. Capability and performance - University staff are set up for success and are able to identify, and are equipped to, manage risks.

(8) Measurable outcomes that demonstrate how certain aspects of risk culture are performing are reported to the Council and Executive Leadership Team on a regular basis.

Risk governance

(9) The Council has ultimate accountability for risk management, overseeing the development of the University's risk management framework and instilling a strong risk culture.

(10) Governance oversight of risk management at the University is predominantly effected by means of:

a. a formal Council and committee structure with appropriate terms of reference and clear roles and responsibilities
b. a Council approved Risk Appetite Statement in addition to a broader suite of University policies and procedures, including documented delegations and authorisations
c. Council and Council committee oversight of risk and compliance obligations, including through the RCSA process and annual attestation of key legislative obligations defined in the Legislative Compliance Guide, and
d. clear ownership, management and oversight of risks to ensure that risk-taking activities are aligned with the University's strategic objectives.

(11) The University employs a ‘three lines’ model to support the monitoring, oversight and escalation of risks and to provide assurance over the management of risk:

a. First line – includes all staff and management directly involved in day-to-day academic, corporate, and research activities, who are responsible for identifying, assessing and mitigating risks as an integral part of their roles. Quality assurance and continuous improvement functions are also considered first line role responsibilities.
b. Second line – specialist functions that establish frameworks and provide expert advice, support, monitoring and continuous improvement that monitors, tests and challenges the effectiveness of first line assurance mechanisms (e.g. risk and compliance, academic quality and standards, work health and safety, IT security, etc.).
c. Third line – independent functions that objectively review the effectiveness of the first and second lines. At the University, third line activities are conducted by the internal audit function in accordance with the Internal Audit Charter.

Risk management process

(12) The University’s approach to risk management is to identify, assess, treat, monitor and report risk. This applies to all University day-to-day activities, project management, strategic planning and decision making:

a. Identify – risks are identified through staff escalation, consultation with key stakeholders as part of the strategic planning and the annual RCSA process. Risks must also be considered as part of any proposed significant change to the University's operations, academic and research activities.
b. Assess - the likelihood of the risk is assessed and the consequences of the risks are evaluated should the risk

materialise in accordance with the Risk Matrix outlined in the Risk Management Guidelines.

c. Treat – appropriate strategies to avoid, reduce or accept the risk are implemented. Strategies include implementing policies, procedures and controls to ensure risks are within the University's risk appetite. There may be occasions where the University wishes to accept risk outside the relevant risk appetite level for strategic or other reasons. Any such exceptions must be approved by the Council following review by the Audit and Risk Committee in accordance with the University's Risk Appetite Statement.
d. Monitor and report – risks are reviewed and reported to Council and management committees on an ongoing basis. Outcomes from assurance activities on the effectiveness of controls from first, second and third lines are also reported on a regular basis.

(13) Timely escalation and reporting of risks and issues to Council and management committees also underpin the University's approach to risk management. All staff are responsible for ensuring risks and issues are escalated to senior management and the Risk and Compliance Unit in a timely manner.

Compliance management process

(14) Compliance is managed through reference to the University's policies and procedures, staff awareness and training and the University's Legislative Compliance Guide. All staff are expected to manage compliance with the University's mandatory and voluntary compliance obligations in line with the Compliance Management Procedure.

(15) Compliance is also managed through the Legislative Compliance Guide, which identifies the University's key legislative obligations and assigns management and oversight accountability for each obligation to relevant staff. Staff to whom obligations are assigned in the Legislative Compliance Guide:

a. are accountable for their obligations and for ensuring that controls within their area of responsibility are regularly monitored and reviewed so that compliance is maintained
b. must monitor for changes and advise the Risk and Compliance Unit of any changes to legislative obligations as they arise, and
c. must complete an annual attestation of compliance with their legislative obligations.

(16) All actual or potential compliance breaches must be reported to the Risk and Compliance Unit in a timely manner, in addition to senior management for assessment in line with the Compliance Management Procedure. The Risk and Compliance Unit, in consultation with the Vice-Chancellor and University Secretary, will report compliance breaches to the Council and relevant Council committees, and report to external regulators where required.

(17) Outcomes from assurance activities on the effectiveness of compliance controls from first, second and third lines are performed and reported on a regular basis.

(18) Compulsory training courses must be completed by all relevant staff and students in relation to key legislative instruments.

Roles and responsibilities

University Council

(19) The University Council is ultimately accountable for risk management under section 19(1B) of the Charles Sturt University Act 1989. The Council:

a. oversees risk management (including risk assessment) across the University and its controlled entities
b. oversees systems of control and accountability for the University and its controlled entities, including establishing policies and procedures consistent with the University's legislative obligations
c. promotes a culture that supports strategically driven decision making within a framework of public

accountability

d. approves the risk appetite of the University and the University's attitude to risks with respect to particular major issues, including the acceptance of risks exceeding the risk appetite as per the Risk Appetite Statement, and
e. approves major decisions affecting the University's risk profile or exposure.

Audit and Risk Committee

(20) The Audit and Risk Committee is responsible, on behalf of the University Council, under the Governance (Audit and Risk Committee) Rule 2022, for oversight of the University's risk governance processes, risk management and control frameworks, risk reporting and its external accountability obligations.

(21) The Audit and Risk Committee reviews the Risk Appetite Statement on an annual basis. In addition, outcomes from the University's risk control self-ssessment process, and significant changes to the University's risk profile are also reported to the Audit and Risk Committee to faciliate the annual review, in order to make any necessary recommendations to the Council. The Audit and Risk Committee approves risk management related policies on behalf of the Council.

(22) The Audit and Risk Committee reviews the effectiveness of systems to monitor the University's compliance with its obligations, significant changes to those obligations and the annual legislative attestation process, in order to make any necessary recommendations to Council. The Audit and Risk Committee approves compliance related policies on behalf of the Council.

(23) Risk acceptances outside of the relevant risk appetite must be approved by the University Council following review by the Audit and Risk Committee.

(24) The Audit and Risk Committee is also responsible for ensuring adequate assurance is performed across the three lines to support and evidence the operating effectiveness of risk management processes. In particular, the Audit and Risk Committee approves the annual internal audit program, monitors its scope and progress, ensures alignment with risk management activities and approves any significant changes to the program in line with the Internal Audit Charter.

Vice-Chancellor

(25) The Vice-Chancellor is accountable to the Council for risk management and is responsible for:

a. establishing, implementing and maintaining the University's risk and compliance management frameworks that align with the University's strategic objectives and risk appetite
b. leading the University's risk culture and ensuring accountability for identifying, assessing, treating, monitoring and reporting of risks is clearly understood across the organisation. The Executive Leadership Team supports the Vice-Chancellor by embedding and reinforcing risk culture and accountability for managing risk within the organisation.
c. Allocating adequate resources to enable effective risk and compliance management, and continuous improvement across the University.

Executive Leadership Team members

(26) Executive Leadership Team members are responsible for:

a. managing the University's activities within the boundaries set out in the Risk Appetite Statement
b. owning and managing risks in their area(s) of responsibility, including routinely identifying, assessing, treating, monitoring and reporting risks
c. ensuring operational systems, processes and activities meet with the University's compliance obligations

d. routinely reporting to the Council and Council committees on the progress towards the achievement of objectives and the management of material risks outlined in the Risk Appetite Statement
e. reporting all actual or potential breaches of compliance obligations, and the Risk Appetite Statement, to the Risk and Compliance Unit, and
f. promoting a culture of risk management, continuous improvement and quality enhancement that emphasises the University's requirement for ethical conduct and personal accountability.

Managers

(27) Managers are responsible for incorporating risk and assurance activities into their day-to-day management practices by:

a. owning and managing risks in their area(s) of responsibility, including routinely identifying, assessing, treating, monitoring and reporting risks
b. complying with obligations, including annual attestations of obligations in the Legislative Compliance Guide
c. implementing quality assurance programs within their areas of responsibility and routinely reviewing the effectiveness of those plans
d. advising and training staff in their day-to-day risk management, compliance obligations, continuous improvement and quality assurance responsibilities, and ensuring staff and students within their areas of responsibilities have completed compulsory training in a timely manner, and
e. upward reporting of risk, compliance and assurance issues to their respective Executive Leadership Team member and the Risk and Compliance Unit.

Project managers

(28) Project managers are responsible for:

a. incorporating risk management into project management methodology
b. identifying, assessing, treating, monitoring and reporting project risks, and
c. escalating significant and emerging risks in line with project governance arrangements.

All staff

(29) All staff (including academic, professional/general staff members, contractors and adjunct staff) are responsible for:

a. assessing risk within their area(s) of responsibility, and performing tasks and duties in line with the University's risk and compliance obligations
b. completing compulsory training in a timely manner, and
c. bringing risk and compliance issues to the attention of their supervisors and the Risk and Compliance Unit.

The Risk and Compliance Unit

(30) The Risk and Compliance Unit is responsible for:

a. reviewing and maintaining the University's risk management framework
b. facilitating the annual risk control self-assessments across portfolios and faculties
c. maintaining the Legislative Compliance Guide and coordinating the annual attestation process
d. maintaining the enterprise actions register and coordinating quarterly monitoring and validation of actions
e. assessing risks and compliance issues and where relevant, determining whether compliance issues are reportable to external agencies and making recommendations to the University Secretary

f. reporting on the University's risk profile and risk culture insights to the Executive Leadership Team, Council and Council committees, and
g. providing information, education and training to staff on risk management processes.

Internal audit

(31) In line with the Internal Audit Charter, the internal audit function is responsible for independently evaluating the effectiveness of first line and second line assurance, and reporting audit findings to the Council through the Audit and Risk Committee.

Section 3 - Procedures

(32) Risk Management Procedure and Compliance Management Procedure.

Section 4 - Guidelines

(33) Risk Management Guidelines

Section 5 - Glossary

(34) For the purpose of this policy, the following terms are used:

a. Action (treat/treatment) – means activities designed to rectify identified issues and/or risks and reduce the likelihood of issues re-occurring and/or risks eventuating.
b. Assurance – means the degree of confidence or certainty that the University's risk management processes and controls are designed and operating effectively.
c. Compliance obligation – means legislative obligations that the University must comply with and voluntary obligations that the University elects to comply with.
d. Control – means any measure or mechanism that is put in place to reduce the impact or likelihood of identified risks and to manage compliance.
e. Issue – means a specific problem or concern that has already occurred or is imminent. Unlike risks, issues are events that need immediate attention because they are currently affecting the University's ability to meet its strategic objectives, its students, and staff.
f. Legislative obligation – means a legislative, regulatory or other requirement that the University must comply with.
g. Risk – means the potential for uncertain events that could impact on the University's strategic objectives and reputation, students and staff. Risk exposure encompasses both the likelihood of an event occurring and the potential severity of its consequences. Risks can be either threats or opportunities missed. Inherent risk is the risk exposure prior to the implementation of controls whereas residual risk is the exposure after controls have been implemented.
h. Risk appetite – means the amount and type of risk the University is willing to accept in the pursuit of its strategic objectives.
i. Risk control self-assessment (RCSA) process – is a standardised approach that management leverages to identify risks and corresponding controls. Risks and controls are summarised at a University-wide basis to support reporting to senior management and the University Council (‘top down’) and also for each divisional/faculty level (‘bottom-up’).
j. Risk culture - refers to an organisation’s attitude to risk management.

k. Risk management framework – means the totality of systems, governance structures, policies, procedures and people that identify, assess, mitigate, and report on risks relevant to the University.

Section 6 - Document context

Compliance drivers	NA
Review requirements	As per Policy Framework Policy
Document class	Governance

Status and Details

Status	Current
Effective Date	3rd April 2024
Review Date	3rd April 2029
Approval Authority	Audit and Risk Committee
Approval Date	3rd April 2024
Expiry Date	Not Applicable
Unit Head	Dugald Hope Director, Risk and Compliance
Author	Julie Watkins Risk and Compliance Adviser
Enquiries Contact	Risk and Compliance Unit