Risk Management Procedure

Section 1 - Purpose

(1) This procedure supports the Risk Management Policy and describes the methodology and processes to guide, direct and support a consistent approach to risk management across Charles Sturt University (the University).

Scope

(2) See the Risk Management Policy.

Section 2 - Policy

(3) This procedure supports the Risk Management Policy.

Section 3 - Procedures

(4) All staff actively engage in risk management in their areas of responsibility with many day-to-day decisions involving an element of risk.

(5) Often, once a risk has been identified, it can be prevented, controlled and managed through business-as-usual operations. In some situations, even though a risk has been identified, no action will be taken and the risk is accepted by the appropriate risk owner in accordance with the University's Risk Appetite Statement.

(6) All relevant stakeholders must be consulted when managing risk. This provides the decision-maker with as much relevant information as is available and facilitates implementation by ensuring that the reasons for the decision taken are understood.

(7) The University's approach to risk management is to identify, assess, treat, monitor and review, and report.

Risk identification

(8) Risks are described as potential uncertain events that could lead to adverse impacts to the University's strategic objectives and reputation, students and staff. Risks can be either threats or opportunities missed.

(9) To analyse and consolidate risk information, risks are classified using the following risk categories (as outlined in the Risk Appetite Statement):

a. Strategy and business improvement
b. Research, development, innovation and entrepreneurship
c. Teaching and learning
d. Financial viability and sustainability
e. Legislative and regulatory compliance
f. Trust and reputation

g. People
h. Technology and cyber security
i. Operational risk

(10) Risk identification occurs at various levels and stages within the University:

a. Strategic planning – risks to the University's strategy objectives are identified as part of the strategic and annual operating planning process. 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. Project risk identification - project risks are generally associated with significant 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 the project is completed, any risks that continue to exist should be incorporated into the appropriate portfolio, faculty and divisional risk register.
c. Event-based or ad-hoc risk identification – risks can be identified by staff when performing their day-to-day roles, continuous improvement activities, organising events, and undertaking risk assessments for new activities not previously executed by the University.
d. Risk control self-assessment (RCSA) – the University performs an RCSA on an annual basis to identify risks relevant to the overall organisation as well as each portfolio, faculty and division. The RCSA process is a structured mechanism for identifying and assessing risk exposures and provides senior management, the Executive Leadership Team, the Audit and Risk Committee and University Council with a view of the University's overall risk profile.

(11) Identified risks must be documented in the relevant portfolio, faculty and divisional RCSA risk register.

(12) The Risk and Compliance Unit is responsible for coordinating the following RCSA risk registers:

a. University-level – the University risk register (risk profile) is endorsed by the Executive Leadership Team and approved by the Audit and Risk Committee.
b. Portfolio-level – portfolio risk registers (key portfolio risks) are approved by the relevant executive lead.
c. Division and faculty-level – risk registers are approved by the relevant division or faculty leader.

(13) The RCSA risk register is an output of the RCSA process that documents the University's current exposure to risks. It includes information such as risk category, description, controls, inherent and residual risk ratings, risk appetite and risk treatments.

Risk assessment

(14) Identified risks are assessed to determine the potential causes and sources in order to analyse the likelihood of the risk event occurring and potential severity of its consequences using the Risk Matrix, defined in the Risk Management Guidelines. This initial assessment provides an inherent risk rating that is the risk exposure prior to the implementation of controls.

(15) Analysis should also consider the design, performance and effectiveness of existing internal controls, processes and governance structures. Risk analysis may draw from a range of quantitative and qualitative techniques to generate a residual risk rating. Residual risk is the exposure after controls have been implemented.

(16) Risks will be evaluated to determine whether or not residual risks are within the University's risk appetite:

a. Residual risks rated equal to or below the risk appetite require no further action.

b. Residual risks that exceed the relevant risk appetite(s) require further treatment to reduce the University's exposure to acceptable levels.

(17) A risk owner will be applied to each risk, with responsibility for managing the risk.

(18) Further guidance on completing the risk assessment process is outlined in the Risk Management Guidelines.

Risk treatment

(19) Risk treatments must be applied for risks that exceed the University's risk appetite for the relevant risk category (see clause 9).

(20) Risk treatment options include:

a. avoiding the risk by discontinuing or not commencing the activity
b. removing the source of the risk
c. taking action to change the likelihood of the risk
d. taking action to change the impact of the risk
e. sharing the risk with another party (e.g. contracting or insurance), and
f. accepting the risk through informed decision (the acceptance of risk outside the relevant risk appetite is subject to Council approval).

(21) Selecting appropriate risk treatment actions must balance benefit and cost and should bring the residual risk rating in line with the risk appetite when implemented effectively.

(22) Risk treatment actions must be documented and agreed upon with the relevant risk owner.

a. Actions are documented in portfolio and division/faculty RCSA risk registers and included in the enterprise action register for monitoring, validation and reporting to the Executive Leadership Team and Audit and Risk Committee.
b. Project risk treatment actions must be documented, monitored and reported as part of the project's governance framework.

(23) Where no viable risk treatment option is available to reduce risk exposure, the Vice-Chancellor may propose to the Council, via the Audit and Risk Committee, that the risk be accepted.

(24) Risk appetite exceptions submitted to Council must include:

a. a business case endorsed by the relevant Executive Leadership Team member accountable for the risk, and
b. a risk analysis and evaluation of the controls in place to manage the risk.

(25) Further guidance on the risk treatment process at the University is outlined in the Risk Management Guidelines.

Risk monitoring and review

(26) Risk monitoring and review ensure that the risk management process is operating effectively. Monitoring and review can be formal or informal, and include the risk control self-assessment process, independent reviews (e.g. internal audit) and continuous informal reviews (e.g. discussing emerging risks in meetings).

(27) Portfolio and division/faculty senior leaders review a summary of their RCSA risk registers at least quarterly.

Risk reporting

(28) All staff must identify and assess risks before commencing new activities and report risk upwards to their supervisor as part of day-to-day operational activities.

(29) Where risks rated medium, high or very high using the Risk Matrix have been realised (the risk occurs and is now an issue) or where a risk breaches the University's Risk Appetite Statement, staff must also report the risk to the Risk and Compliance Unit. Examples of risks to be escalated include but are not limited to:

a. overpayments or financial loss greater than $50,000
b. matters received from, or that may require reporting to a regulator
c. inadequate performance or actions taken by third parties
d. systemic process and/or control failures, or deviations from University policies and procedures
e. business disruption resulting in business continuity plans being activated
f. matters that have the potential to damage the University's brand, and
g. breaches of the University's Risk Appetite Statement.

(30) RCSA risk registers act as central repositories of risk data, including context, risk ratings, treatments and risk management responsibilities and accountabilities. The Risk and Compliance Unit will maintain RCSA risk registers at the University level, portfolio level and individual division/faculty level.

(31) By consistent application of the RCSA process, the self-assessments act as the basis for internal risk reporting to enable decision makers to meet their risk management obligations. Risk control self-assessments also provide data and information for reporting to external stakeholders, where applicable (such as regulators or external auditors).

(32) In line with the Risk Appetite Statement, the Risk and Compliance Unit will monitor and report to the Executive Leadership Team and Audit and Risk Committee on:

a. compliance with the relevant risk appetite levels
b. any actual or potential breaches of the University's Risk Appetite Statement
c. progress of treatment actions captured and monitored via the enterprise actions register
d. changes to the University's risk profile, and
e. emerging and realised material risks.

Risk owners

(33) Risk owners are accountable for ensuring that risks within their management structure are managed in accordance with the University's Risk Appetite Statement.

(34) A guide to risk ownership is outlined below:

a. Whole of organisation risks – Vice-Chancellor
b. Portfolio risks – relevant Executive Leadership Team member
c. Business unit risks (e.g. faculty, division, centre, office) – Executive Directors, Executive Deans, Pro Vice-Chancellors
d. Unit risks (e.g. school, office, unit, institute or centre) – Directors, Deans, Heads of School, Managers
e. Specific purpose endeavours (e.g. project, events, research activities) – project managers, event managers, research supervisors.

(35) Each risk owner is responsible for:

a. establishing, updating and reviewing their risks periodically, to be included in the University risk reporting process
b. understanding and monitoring the key internal controls in place to mitigate risk, to ensure they remain effective
c. integrating risk and assurance as part of a business-as-usual management activity, and
d. identifying and monitoring against risk tolerance measures within the University's risk appetite, and reporting any triggers against tolerance measures to the Risk and Compliance Unit.

Third-party risks

(36) Managing risks associated with partners is a key part of the University's risk management framework to mitigate operational, financial, reputational and information security risks that may arise from engagements with vendors, third-party education arrangements and partners.

(37) The University's risk management process (of identifying, assessing, treating, monitoring and reviewing risks) applies to the University's engagement with third parties and supports the University's resilience against disruptions, maintains compliance with regulatory requirements and protects the integrity of operations in line with the University's risk appetite.

(38) Managing third-party risk involves due diligence during onboarding, ongoing monitoring, contractual safeguards, and incident response planning tailored to the risk associated with the relationship.

(39) Responsibility for managing third-party risk is aligned with the portfolio engaging with the third party.

(40) Risk mitigation activities during onboarding, ongoing and offboarding of third parties, coupled with regular reporting and oversight, ensure that third-party risks are systematically addressed and align with the University's risk appetite.

Assurance management process

(41) In line with the Risk Management Policy and the 'three lines' model of risk governance, the first, second and third lines must obtain adequate assurance that key controls highlighted during the RCSA process are effective, to ensure that:

a. risks are identified and managed, and risk treatments are completed in a timely manner
b. controls are designed and operating effectively to mitigate risk
c. compliance obligations are being managed and controls effectively highlight actual or potential compliance breaches for reporting and remediation, and
d. all expected quality standards are met.

(42) The Risk and Compliance Unit will prepare an annual assurance plan in consultation with members of the Executive Leadership Team and approved by the Audit and Risk Committee. The annual assurance plan will include targeted assurance reviews, internal audits and known assurance activities conducted by external parties, and will be informed by:

a. emerging risks
b. key controls identified through the RCSA process
c. the introduction of new products, services or processes
d. outcomes of reviews of actual or potential compliance breaches conducted through the Compliance Management Procedure
e. on a risk basis, requests from Executive Leadership Team members, Council committees and/or the University Council, and

f. the Internal Audit Charter for internal audit activities.

(43) Each compliance assurance review should include the following stages:

a. Scope – the objectives and scope of the assurance review will be defined and shared with management of the relevant business unit(s) that may be impacted by the review.
b. Controls analysis – testing the design and effectiveness of key controls to determine whether the controls meet control objectives and work as intended.
c. Reporting – a report will be prepared and issued to relevant management, including details of any risks identified that have not been effectively treated and recommendations for improvements to further control the risks.

(44) Following the issue of a compliance assurance review report, management will identify risk treatment actions to address recommendations made within the report, where applicable. Treatments will be captured by the Risk and Compliance Unit and included in the enterprise actions register.

(45) The Risk and Compliance Unit will report the progress against the annual assurance plan to the Executive Leadership Team and Council committees.

Internal audit

(46) Internal audit activities will be conducted to support third line assurance. Internal audits will be conducted and reported in line with the Internal Audit Charter and Internal Audit Manual.

Enterprise actions register

(47) The University maintains an enterprise actions register (EAR) to record and monitor the remediation of risk-related actions. Actions represent existing instances of non-compliance, gaps or improvement opportunities in operational controls and processes, and proactive measures required to reduce the likelihood/impact of risks in accordance with the University's risk appetite.

(48) Each action recorded on the EAR will be assigned an action owner by senior management, responsible for the timely completion of agreed actions to mitigate the identified risk.

(49) The Risk and Compliance Unit manages the EAR and provides status reporting to action owners, Executive Leadership Team and Council committees.

(50) Reporting on actions is crucial from a risk accountability perspective. When actions taken to address risk are documented and reported, it provides a clear record of the steps that have been taken to manage and mitigate actual and potential issues. This accountability ensures that staff members or teams are held accountable for their roles in risk management, facilitates communication about the progress of risk treatment efforts, and supports the overall risk culture of the University.

Education and training

(51) The University supports education and training as an essential mechanism in developing and maturing its risk and compliance culture.

(52) The University implements education and training programs to increase awareness of risk and compliance and the responsibilities of managers and staff to understand and fulfill their obligations.

Section 4 - Guidelines and supporting documents

(53) See the:

a. Risk Appetite Statement
b. Risk Management Guidelines (including the Risk Matrix)
c. associated templates and information on the Risk and Compliance website/portal.

Section 5 - Glossary

(54) This procedure uses terms defined in the Risk Management Policy.

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	University Secretary
Approval Date	2nd 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