Risk Management Procedure

Section 1 - Purpose

(1) This procedure is developed in support of the University's Risk Management Policy to provide detailed procedural steps and guidance to implement effective and demonstrable risk management practices across Charles Sturt University (the University). Through this procedure, the University aims to achieve consistent application of risk management principles and maintenance of risk registers across the institution.

Section 2 - Glossary

(2) For the purpose of this procedure, the University has outlined a number of definitions in the Risk Management Policy.

Section 3 - Policy

(3) Refer to the Risk Management Policy.

Section 4 - Procedures

Enterprise levels and risk owners

(4) Enterprise levels refer to the hierarchical management structure of the University at which risks are managed. Enterprise levels also include specific-purpose endeavours, such as projects and events. For the purpose of risk management, enterprise levels are classified according to tiers.

(5) Risk owners are accountable for ensuring that risks within the management structure for which they are responsible are managed in accordance with acceptable appetite levels, as per University's Risk Appetite Statement. This entails carrying out or overseeing the identification, analysis, evaluation of risks, as well as the design, implementation, and monitoring of any risk treatments.

(6) The risk owners for each enterprise level are listed below:

Enterprise level	Management structure	Risk owner
Tier 1	Whole of organisation	Vice-Chancellor
Tier 2	Portfolio	Executive Leadership Team portfolio leaders
Tier 3	Business unit (e.g., faculty, division, centre, office)	Executive directors, executive deans, pro vice-chancellors
Tier 4	Unit (e.g., school, office, unit, institute or centre)	Directors, deans, heads of school, managers
Tier 5	Specific-purpose endeavours (e.g., projects, events)	Project managers, event managers

Risk register

(7) A risk register is an output of the risk management processes that documents the University's current exposure to risks. It includes such information as: enterprise level, risk description, risk factors or causes, controls, inherent and controlled risk ratings, risk appetite, and risk treatments.

Risk register maintenance

(8) The Risk and Compliance Unit is responsible for maintaining the University's risk register through periodic risk assessments facilitated with the support of the Audit and Risk Committee and the Executive Leadership Team (ELT).

(9) Each risk owner is responsible for establishing, updating and reviewing their respective risks on a periodic basis to be included in the University risk reporting process outlined in the Risk Appetite Statement. It is the intention that risk management is embedded as part of a business-as-usual management activity, instead of a separate process.

Updating the risk register

(10) When entering new risks into the risk register, the following process applies:

a. All newly identified risks should be approved by the ELT; and
b. Once a new risk is approved, the Risk and Compliance Unit will vet the appropriateness of the risk terminology and provide final approval, prior to being entered into the University risk register.

(11) Once risks are incorporated into the risk register, any updates should be approved by the corresponding portfolio leader or the Vice-Chancellor.

Risk management process

(12) The risk assessment process adopted by the University is based on the Standard.

Establishing the context

(13) Prior to undertaking the risk assessment process, it is important to define the context against which risks will be assessed. This will help to:

a. clarify the scope and purpose of the risk assessment;
b. define the internal and external parameters to be considered when managing risk; and
c. identify the relevant stakeholders with whom to communicate and consult.

(14) It is important to understand the internal and external environments that the University operates in that may influence or impact the function or process being assessed. The following should be considered:

a. Internal context - the environment in which the University operating model is designed and based upon, including but not limited to:
    i. understanding the University's strategy, objectives, values and policies to identify areas of priority and alignment with operational business plans and drivers;
    ii. considering the University's governance, structure, roles and accountabilities;
    iii. considering the University's contractual relationships and commitments;
    iv. considering available resources and capabilities; and
    v. understanding the University's Risk Appetite Statement (including acceptable risk appetite levels).
b. External context - the environment in which the University operates and the impact of this on achievement of the University's objectives, including:

i. key legislation, rules and compliance standards requirements;
ii. external stakeholder relationships, perceptions, values, needs and expectations; and
iii. social, cultural, political, economic and market conditions.

Risk identification

(15) The risk identification process is a critical step to ensure that risks captured reflect a list of risk events that may impact the achievement of University objectives. An incomplete list of risks may result in material risks not being analysed to the required detail and, in turn, exposing the University to an inappropriate degree of risk. Risks identified are documented in the risk register.

(16) Identified risks should be described in a comprehensive fashion, with reference to the following:

a. the source of risk;
b. the areas affected;
c. causes/potential triggers that may results in the risk event occurring;
d. potential consequences to the University should this risk event occur; and
e. any existing controls which are in place to mitigate the influence of the risk.

Note: Potential consequences should be described according to the Risk Management Guidelines, rather than a process, a failure or lack of controls.

(17) It is preferred that risk identification be conducted through a team-based approach with all members of the group having a good understanding of the tasks, objectives of the area being assessed and how the risks impact the University's objectives. Other techniques such as desktop (i.e., offsite) risk assessments or management reviews can also be used.

(18) It is important to identify the risk owner who will be responsible for managing the risk. This is critical to ensure that the risk is regularly monitored and appropriately addressed through mitigation strategies further down the risk management process.

(19) Questions to ask when identifying potential risks might include, but are not limited to the following:

a. What needs to go right to achieve a specific objective?
b. What are our top priorities?
c. What could go wrong that will derail us from achieving our objectives?
d. Where and how could this happen?
e. Where are our vulnerabilities?
f. How do we know if we are achieving our objectives?
g. How do we know that we are making the right decisions?

Risk analysis

(20) This stage is undertaken to better understand the risks identified in the previous step. This involves measuring the likelihood of the risk event occurring and extent of the consequences if the risk were to occur.

(21) Measuring the likelihood and consequence of a risk event is not strictly a statistical or quantitative measure. It requires management's judgement which can be informed by previous experiences of such risk event, experience of other Universities or organisations in similar scenarios, available University performance data or audit/independent review observations.

(22) The following steps should be followed in assigning risk rating to each risk event and should be rated from a

whole-of-institution perspective:

a. assign inherent risk rating - i.e., determine the likelihood and consequence of the risk event if it were to occur without reference to specific mitigation strategies or actions;
b. identify existing controls - i.e., what activities are already in place to address or mitigate the risk identified? Are they well designed and are they operating as intended? and
c. analyse the controlled risk rating - i.e., determine the likelihood and consequence of the risk event once the influence and effectiveness of existing controls has been considered.

(23) When completing the risk register the inherent and controlled risk ratings are calculated based on the University's Risk Management Guidelines.

Risk evaluation

(24) Once the controlled risk ratings are determined, each risk is evaluated to determine whether it is acceptable or unacceptable based on the University's Risk Appetite Statement or acceptable risk levels determined by risk owners. The University's acceptable risk appetite levels can change over time, depending on its strategy and the environment it operates in.

(25) Evaluation of each identified risk may result in the following scenarios:

a. the controlled risk rating is beyond acceptable risk appetite level:
    i. further risk treatment actions are expected to be formulated to reduce the risk to acceptable levels; or
    ii. if no further treatment is identified, the acceptance of this risk will be referred to the University Council.
b. the controlled risk rating is below acceptable risk appetite level:
    i. no further action is required; or
    ii. consider reducing the level of controls currently in place to reallocate resources to areas of greater need.

(26) Although many risks may be rated within the acceptable risk appetite level from a University perspective, these may be unacceptable to the risk owner and should be flagged as such. The risk register can in this way identify risks that warrant priority attention both at a University level and/or an operational level.

(27) The acceptance of risks lying outside the Risk Appetite Statement is subject to University Council approval. This may be the case, when, for example:

a. there are no appropriate risk treatment actions available;
b. the cost of the treatment outweighs the benefit;
c. the benefits and opportunities outweigh the potential consequences of the risk; or
d. the risk is being taken to pursue an opportunity in line with the University's strategy and objectives.

Risk treatment selection

(28) If further risk treatment actions are required for a specific risk, risk owners are accountable for implementing appropriate measures to reduce the risk to an acceptable level.

(29) Risk treatment actions to reduce the risk level include:

a. avoiding the risk by discontinuing or not commencing the activity;
b. removing the source of the risk;
c. changing the likelihood of the risk;

d. changing the consequences of the risk; and
e. sharing the risk with another party (e.g. contracting or insurance).

(30) The following principles should be considered when identifying risk treatment actions:

a. identify and assess a range of treatment actions before selecting one or more of these options to be implemented (e.g., implementing new controls, obtaining insurance);
b. a cost/benefit analysis may be useful in determining the most appropriate risk treatment action; and
c. treating a risk may have implications elsewhere and impact on other activities. Consequential impacts, correlations and dependencies should also be considered to ensure that in managing one risk, an unacceptable situation is not created elsewhere.

Risk treatment implementation

(31) Once a risk treatment action is identified, it should outline the:

a. risk treatment to be implemented;
b. person responsible for implementation;
c. any potential constraints; and
d. timeframes for completion and resources required.

(32) Examples of possible mitigation strategies include:

a. re-designing or enhancing existing processes, structures, and controls;
b. introducing new processes, structures, and controls; and
c. further monitoring of existing controls.

(33) In most cases, treatments to reduce exposure to risk will entail modifications to the University's internal control environment, such as by implementing new or enhancing existing controls.

Risk monitoring

Risk owners

(34) Risk owners are accountable overall for ensuring risks, internal controls and any risk treatments documented in the risk register within their area of responsibility are regularly monitored and reviewed.

(35) Monitoring and review processes are used to ensure that:

a. risks and controls are still relevant;
b. assumptions remain valid;
c. expected results are being achieved;
d. risk appetite levels are respected;
e. implementation of risk treatments is completed and effective; and
f. emerging risks and new information are integrated into the risk management process.

(36) To assist in risk monitoring, it is recommended that governance and management bodies include risk management as a standing agenda item and as part of their annual work plans for periodic review.

Risk and Compliance Unit

(37) The Risk and Compliance Unit will review risks to ensure that the following risk management functions are undertaken in accordance with the University's Risk Management Policy:

a. facilitate the periodic review of existing and emerging risks;
b. prepare, develop and present relevant risk reports, as well as operate and maintain the University Risk System; and
c. review the management of identified risks and proposed risk changes prior to these being entered into the University Risk System to ensure completeness, accuracy, clarity and quality of risk information, and to prevent duplication.

Internal audit function

(38) The internal audit function is responsible for independently assessing the adequacy and effectiveness of internal controls of the University on a risk-based approach. The results of Internal Audit's work will inform how well the controls identified in risk registers are operating and may affect the controlled risk ratings for associated risks.

(39) Internal Audit will periodically review the completeness and effectiveness of the University's Risk Management Framework and refer the findings to the University Council (via the Audit and Risk Committee).

Related documentation

(40) The Risk Management Policy is published in the University's policy library and referenced on the Risk and Compliance website/portal. All associated guides, templates and information on the University's risk management framework is available from the Risk and Compliance website/portal.

Risk Reporting Structure

(41) Refer to the Charles Sturt University's Risk Appetite Statement which outlines the University's risk reporting structure.

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