Risk Register 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 Policy, the University has adopted the following definitions:

a. Risk - means the effect of uncertainty on the achievement of objectives;
b. Risk Management - means coordinated activities to direct and control an organisation with regard to risk;
c. Risk Management Process - means the 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;
d. Inherent Risk - means an assessment of the risk exposure without reference to specific mitigation strategies or actions;
e. Residual Risk - refers to the risk remaining after implementation of risk treatment; and
f. Risk Appetite - refers to the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals.
g. Senior Executive - refers to Deputy Vice-Chancellors, Chief Financial Officer and Executive Director, People and Culture, in accordance with clause 3 of the Delegations and Authorisations Policy.
h. Managers - refers to a Primary Budget Centre Manager or Secondary Budget Centre Manager, as defined in clause 3 of the Delegations and Authorisations Policy.

Section 3 - Policy

(3) Refer to the Risk Management Policy.

Section 4 - Procedures

What is a Risk Register?

(4) A Risk Register is a management tool that documents risks identified by the University by describing the characteristics of each risk in terms of its nature, causes or contributing factors, risk rating and risk mitigations.

(5) Risk Registers are outputs of the risk management processes undertaken at various levels of the University including the Senior Executive team, divisional, projects and functional operations of the University.

Types of Risk Registers and responsible owners

(6) The various types of Risk Registers expected to be completed at the University are listed below along with their responsible owners:

Type of Risk Register	Description of Risk Register	Responsible Owner
Principal Risk Register (PRR)	A University-wide risk register which reflects the University's risk profile. It contains strategic risks and key operational risks consolidated or aggregated from other risk registers.	Vice-Chancellor's Leadership Team
Operational Risk Register (ORR)	A risk register that reflects the key operational risks of a faculty, division, institute, controlled entity or partnership.	Primary Budget Centre Manager / Secondary Budget Centre Manager
Project Risk Registers	Risk registers maintained throughout the lifecycle of individual projects or initiatives, e.g. major capital and IT projects, strategic initiative or transformation projects.	Project Managers
Other specific purpose risk registers	These are risk registers maintained as part of a legislative requirement such as Work, Health and Safety (WHS) and, Research Ethics and Integrity.	Primary Budget Centre Manager / Secondary Budget Centre Manager

(7) The Risk Management unit within the Office of Governance and Corporate Affairs is responsible for maintaining and updating the University's Principal Risk Register through bi- annual Strategic Risk Assessments facilitated with the Vice-Chancellor's Leadership Team.

(8) The owners of operational, project and specific purpose risk registers are responsible for establishing, updating and reviewing their respective risk registers on a regular basis, e.g. as part of a standing agenda item in recurring management meetings or committees. It is the intention that risk management is embedded as part of a business-as-usual management activity instead of a separate process.

(9) The Risk Management unit may be requested to support managers in the establishment of risk registers and to facilitate risk identification and assessment workshops with the respective operational unit or area.

How risk registers across the University work together

(10) Every risk register established across the University contains risks which are unique to their area of operation or similar to other areas. The aggregation and consolidation of risks documented through risk registers will allow managers, Senior Executives and ultimately Council, to understand the University's risk profile. This will also inform whether necessary risk mitigations are undertaken to protect the University from unacceptable adverse impact or to further capitalise on potential opportunities.

(11) An illustration of how risk registers contribute to the University's risk profile and management process is captured in this diagram.

Risk Assessment Process

(12) The risk assessment process adopted by the University is captured in the Risk Management Process diagram.

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 activity;
b. define the internal and external parameters to be considered when managing risk; and
c. identify the relevant stakeholders to communicate and consult with.

(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 are some aspects for consideration:

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 available resources and capabilities; and
    iv. understanding the University's Risk Appetite Statement (including risk tolerances).
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 legislations, rules and compliance standards requirements; and
    ii. 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 material risk events which may impact the achievement of University objectives. An incomplete or not comprehensive list of risks may result in material risks not further analysed in the process.

(16) Risks identified are documented in a risk register. The University has an approved Risk Register template which must be used when developing or revising a risk register. Risk register templates can also be downloaded from the University's Risk Management website/portal.

(17) When identifying and describing a risk, it should be comprehensive and include:

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.

(18) Note: potential consequences should be described in qualitative terms and not described as a process, a failure or lack of controls.

(19) It is preferred that risk identification is conducted through a team-based approach with all members of the group having a good understanding of the tasks and objectives of the area being assessed will help reduce the chance of any risks being overlooked. Other techniques such as desktop risk assessments or management reviews can also be used.

(20) It is important to identify the risk owner who will be responsible for 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.

(21) Questions to ask when identifying potential risks might include:

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 objective?
g. How do we know that we are making the right decisions?

Risk Analysis

(22) 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. The University's Risk Ratings Matrix and Likelihood Ratings Guide is attached at Appendix A.

(23) 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 companies in similar scenarios, available University performance data or audit/independent review observations.

(24) 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 residual risk rating - i.e. determine the likelihood and consequences of the risk event occurring under the current control environment.

(25) When completing a Risk Register the Inherent and Residual Risk Ratings are automatically calculated based on the Likelihood and Consequence ratings and the Risk Matrix (refer Appendix A).

(26) A Risk Consequence Matrix is also included in Appendix A. The consequence scale definitions included in the matrix provide a general description of each impact level as defined against seven broad risk categories relevant to the key operations of the University to assist risk owners in rating risk events, the categories include:

a. Academic Quality;
b. Research Performance;
c. Community Engagement and Brand Reputation;
d. Financial and Commercial;
e. Service Delivery and Infrastructure;
f. Health, Safety and Environment; and
g. Culture, Legal and Compliance.

(27) These categories provide a framework to consider potential risks during the analysis phase. A risk may fall in, or impact on, multiple categories. Therefore, multiple categories may need to be considered.

Risk Evaluation

(28) Once the residual 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 target risk levels determined by Senior Executive risk owners. The University's risk appetite and tolerance is likely to change over time, depending on its strategy and environment it operates in.

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

a. the residual risk rating is beyond acceptable or tolerable level:
    i. further mitigation strategies or treatment 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 made at the Senior Executive level.
b. the residual risk rating is below acceptable or tolerable 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.

(30) Although many risks may be rated low or medium from a University perspective, these may be unacceptable to the responsible manager 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.

(31) Risks beyond the tolerable level may be accepted in some circumstances without further mitigation (i.e. other than maintaining existing controls) if, for example:

a. there is no appropriate risk treatment 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

(32) If further risk treatment is required for a specific risk, the risk owner(s) is responsible for identifying and implementing appropriate measures to reduce the risk to an acceptable level.

(33) Risk treatment strategies 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; or
e. sharing the risk with another party (e.g. contracting or insurance).

(34) The following principles should be considered when identifying risk treatments:

a. identify and assess a range of treatment options before selecting one or more of these options to be implemented;
b. a cost/benefit analysis may be useful in determining the most appropriate mitigation option; 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.

(35) Once a risk treatment plan is identified, it should outline the:

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

(36) Examples of possible mitigation strategies include: re-designing or enhancing existing controls; introducing new controls; further monitoring of existing controls; or, in cases where a control has been assessed as ineffective,

removing the existing control.

Monitoring and Review

(37) Risks are monitored and reviewed through a number of ways, including parties such as risk owners, the Risk Management unit, Internal Audit, the Senior Executive and Council committees. However, the primary responsibility resides with the risk register owners, i.e. Primary Budget Centre Managers or Secondary Budget Centre Managers and Project Managers.

Risk / Risk Register Owners

(38) Managers are responsible for ensuring risks and mitigation plans documented in risk registers within their area of responsibility are regularly monitored and reviewed. It is the intention that risk management is embedded as part of a business-as-usual management activity instead of a separate process. 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 tolerance reflect current levels;
e. implementation of risk treatments are completed and effective; and
f. emerging risks and new information are integrated into the risk management process.

Risk Management unit

(39) The Risk Management unit will review Operational Risk Registers with outcomes of monitoring and review processes used to inform ongoing reporting at various levels, including to the Vice-Chancellor's Leadership Team and the Finance, Audit and Risk Committee.

Internal Audit

(40) Internal Audit is responsible for 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 working and may affect the residual risk ratings for associated risks.

(41) 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 Finance, Audit and Risk Committee).

Risk Reporting Process

(42) The responsible manager will review their area's Operational Risk Register on a quarterly basis and update as required/appropriate. Once completed, if the risk register is revised it must be submitted to the Risk Management unit for consolidation, alternatively if there are no changes this must also be communicated to the Risk Management unit.

(43) Quarterly review of Operational Risk Registers will inform the University wide Principal Risk Register which will be reported quarterly to the Vice-Chancellor's Leadership Team and the Finance, Audit and Risk Committee. This will include:

a. strategic risks of the University;
b. key operational risks which are rated 'Very High' or 'High'; and
c. risks which are beyond acceptable or tolerance level.

(44) The University's Principal Risk Register will be reported to the University Council via the Finance, Audit and Risk Committee on an annual basis or as determined.

Related Documentation

(45) The Risk Management Policy and Risk Register Procedure is published in the CSU Policy Library and referenced on the Risk Management website/portal. All associated guides, templates and information on the University's risk management framework is available from the Risk Management website/portal.

Section 5 - Guidelines

(46) Nil.

Status and Details

Status	Current
Effective Date	23rd December 2016
Review Date	23rd March 2018
Approval Authority	Vice-Chancellor
Approval Date	23rd December 2016
Expiry Date	Not Applicable
Unit Head	Cassandra Webeck University Secretary +61 2 6338 4258
Author	Linda Breen University Secretary and Director, Governance and Corporate Affairs
Enquiries Contact	Office of Governance and Corporate Affairs +61 2 63384207