Business Continuity Management Policy

Section 1 - Definitions

(1) For the purpose of this Policy:

a. "Disaster" - An unexpected disruption to normal business of sufficient duration to cause unacceptable loss to the organisation necessitating disaster recovery procedures to be activated.
b. "Disaster Recovery" - Activities and procedures designed to return the organisation to an acceptable condition following a disaster.
c. "Business Continuity" - The uninterrupted availability of all key resources supporting essential business functions.
d. "Business Continuity Management" - Provides for the availability of processes and resources in order to ensure the continued achievement of critical objectives.
e. "Business Continuity Planning" - A process developed to ensure continuation of essential business operations at an acceptable level during and following a disaster.
f. "Maximum Acceptable Outage" (MAO), also "Maximum Tolerable Outage" (MTO) and "Maximum Downtime" (MD) - The maximum period of time that critical business processes can operate before the loss of critical resources affects their operations.

Section 2 - Policy Statement

Part A - Policy Declaration

(2) This Business Continuity Policy forms part of the Risk Management Framework at Southern Cross University. Business Continuity Planning sits alongside crisis management and disaster recovery planning and is part of the organisation's overall risk management procedures.

(3) By the adoption of Business Continuity Management best practices the University endeavours to ensure that business critical teaching and research outcomes are not compromised by a major disruptive event.

(4) Under this Policy the University shall, in the event of a disaster:

a. act to ensure that critical business processes can be continued;
b. use its best endeavours to meet the needs of staff, students, the wider community and other key stakeholders; and
c. safeguard its reputation and public image.

Part B - Policy Description

Objectives

(5) This Policy:

a. defines the University's Business Continuity Management (BCM) process and allocates responsibility for the BCM and Business Continuity Planning (BCP) processes on a University-wide basis.
b. outlines the structures the University has developed in order to provide timely availability of all key resources necessary to re-establish the critical business processes to a level of operation that is acceptable to management.

Scope

(6) This Policy is applicable to all staff (including casual staff) of the University including those of the University's controlled entities and any entities that are derived from the University's legal status.

Part C - Content and Implementation

(7) Business continuity management is an integral part of the University's overall risk management, corporate governance and quality management framework. This Policy is complementary to the University's Risk Management Policy.

(8) Using a risk management approach, the University's key business interruption risks are to be identified and assessed so as to ensure the uninterrupted availability of all key business resources required to support essential or critical business activities.

(9) All unacceptably high business interruption risks will be subject to risk mitigation treatment in line with the University's overall risk management plans. The effectiveness of the business continuity management program is to be constantly monitored and regularly reviewed.

Institutional Context

(10) The University has an obligation to its stakeholders (students, staff and wider community) to ensure that its operations can continue to a pre-determined minimum level in the event of a major disruptive incident.

(11) Through the adoption of Business Continuity Management best practices the University will achieve its business continuity objectives of:

a. providing timely availability of key resources necessary to operate the critical business processes at a level of operation that is acceptable to management
b. maintenance of staff, student, client and other stakeholder contact and confidence
c. fulfilment of regulatory requirements
d. safeguarding our reputation and public image
e. controlling extraordinary expenditure caused by the event
f. controlling risk in priority areas.

(12) All organisations have potential risk areas. Some of the most common, in the university context, with associated preventative requirements (controls), are:

a. Information Systems (including academic and other records): ensuring security is maintained; ensuring the physical assets are protected against damage/loss and records are controlled and secure.
b. Financial Systems and Procedures: ensuring systems cannot be misused; ensuring appropriate accountability for expenditure of funding; ensuring security of financial assets.
c. Buildings, Infrastructure and other Assets: ensuring the organisation's resources are protected against damage/loss; ensuring University material assets are available to support key business activities.

Section 3 - Responsibilities

Part D - Responsibilities and Approvals

Audit and Risk Management Committee

(13) Business Continuity Management is a component of the overall risk management function of the University, overseen at a strategic level by the Audit and Risk Management Committee of University Council.

(14) This Committee:

a. ensures that the University maintains effective risk management practices across all areas of its activities;
b. oversees the development of a systematic and coordinated risk management framework;
c. monitors the external risk environment;
d. ensures appropriate assessment of the impact of any changes to the University's risk profile.

Vice Chancellor

(15) The Vice Chancellor plays a pivotal role in providing leadership consistent with the University's commitment to meet stakeholder expectations of the highest standards of operational efficiency at all times.

Business Units

Vice President (Engagement)

(16) The Vice President (Engagement) is responsible for overseeing the functions of the University's public relations activities, including crisis management communications.

Internal Auditor

The University's Internal Auditor shall consider coverage and review of this Policy during the course of the annual audit program.

Section 4 - Procedures

(17) Under this Policy, it is incumbent upon all University managers to ensure that the key functions for which they have responsibility are able to continue following major disruptive events and that arrangements are in place to achieve this.

(18) This requires the proactive development, maintenance and devolution of business continuity planning within their areas.

(19) Managers are expected to encourage and facilitate the active participation of staff in business continuity issues and must ensure that key personnel are able to perform competently during a major disruptive event.

Part E - Developing the Business Continuity Plan (BCP)

a. The critical business objectives that still must be achieved during and after a major disruption.
b. Stakeholder expectations of acceptable service delivery.
c. The likely scenarios that may result in disruption to the business.
d. What is important to protect, provide or operate during a disruption i.e. the critical business functions and

processes.

e. The people, infrastructure and data resources required to maintain a minimal acceptable level of operations.
f. Communications requirements and the methods and channels of dissemination.

The Process

(20) Identify the critical business functions and processes that support achievement of key business objectives. This involves the identification of core business objectives, critical business functions that support these objectives and their critical success factors.

(21) The maximum period of time (Maximum Acceptable Outage) that each of the University's key functions and processes can operate before the loss of critical resources affects overall operations needs to be defined at this time.

(22) Identify the types of disruptions (risks) that are likely to occur and that will need to be catered for. The actual events do not necessarily have to be considered individually, but the impact of losing key resources, facilities, processes etc. as a result of a disastrous event must be.

(23) These impacts will probably be similar across the operations of the University but each business unit will need to consider such impacts on its own operations. The vulnerability of business processes and interdependencies should be considered as part of this analysis.

(24) Any Business Continuity Plan (BCP) should allow the University to respond flexibly to a wide variety of potential disruption scenarios.

(25) Each business unit will then need to identify its business cycles, because the severity of a disruption will depend upon where each area is within its business cycle.

(26) While this, in the University context, will be similar for many areas and units, it will not necessarily be the same for all. During some stages of a business cycle (academic year, for example), a limited resource outage can be more disruptive than at other stages. At these times, decisions in relation to implementing emergency alternative procedures to cater for the outage/loss will need to be made more quickly.

(27) Conduct a business impact analysis to identify the effect of the different types of outages/losses on the key business functions/processes at each phase of the business cycle. Often there will need to be alternative approaches to cater for disruptions to or losses of different resources, facilities etc. at various times of the year. The loss of a work space, for example, will require different contingency procedures to the loss of computing resources, even at the same point in the business cycle.

(28) Identify and document existing workarounds and continuity arrangements. The development of alternative procedures to be implemented in the event of a major disruption can become part of the area's business improvement plan.

(29) Identify the resources required to ensure speedy restoration of a minimum acceptable level of the area's key operations.

a. These might include people (specialist and support); IT infrastructure; information and data (hardcopy and electronic); office and specialist equipment; facilities and accommodation; internal dependencies and/or interfaces (e.g. other business units); external dependencies and/or interfaces (e.g. suppliers, contractors, customers, competitors and regulators etc.), and current stock holdings, among others.
b. The resource requirements for business continuity can be considered in relation to other business requirements and included in budget proposals.

(30) Senior management will need to consider the business impact analysis of each area to determine what additional

resources are required across the University. The approach to meeting these requirements, including the sequence in which they should be provided, is to be determined.

(31) The BCP should be documented in such a way that it is of practical use in a disaster and that it fulfils business, regulatory, training and audit requirements.

(32) A BCP communications strategy should be developed which should include identification of who needs information, what information is needed, how that information can be provided, what constraints on its provision might exist and who has the authority to approve the communications.

(33) The strategy should also define the means by which different types of messages will be promulgated to each of the stakeholders.

(34) There should be BCP testing and training, a verification process to ensure that staff are familiar with the business continuity measures to be implemented and that the various components of the plan function properly. At this stage, plan inadequacies are identified and corrected.

(35) BCP reviews and updates should occur on a regular basis to ensure its currency.

(36) Any changes to business functions and activities, key dependencies, facilities and supporting infrastructure etc. must be reflected in the plan.

(37) The above process is to be overseen by the Manager, Insurance and Risk.

Appendix A

The Risk Management Process

(38) In order to prepare Business Continuity Plans it is necessary to understand how to evaluate the level of risk and what level of risk is acceptable to the University. Reference should be made to the University's Risk Management Policyand Procedure, in particular Annexure A, the University's Risk Management Approach and Methodology.

(39) The main elements of the Risk Management Process outlined in the above Policy are:

a. Communicate and Consult.
    i. Appropriate communication and consultation with internal and external stakeholders should occur at each stage of the Risk Management Process as well as on the process as a whole.
b. Establish a context.
    i. By establishing the context, the organisation articulates its objectives, defines the external and internal parameters to be taken into account when managing Risk, and sets the scope and risk criteria for the remaining process.
c. Define the criteria
    i. Criteria against which Risk will be evaluated should be established and the structure of the analysis defined. The criteria should reflect the organisation's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and/or other requirements to which the organisation subscribes.
d. Risk Assessment
    i. Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.
e. Identify Risks.
    i. The organisation should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences.

f. Analyse Risk.
    i. This is the determination of existing controls and the analysis of Risks in terms of consequence and likelihood in the context of those controls. This analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood may be combined to produce an estimated level of Risk.

g. Evaluate Risks.
    i. This is a comparison of estimated Risk levels against pre-established criteria. This enables Risks to be ranked to identify management priorities which will be influenced by the organisation's attitude to Risk. If the level of the Risk established is low, then Risk may fall into an acceptable category and further treatment may not be required.

h. Treat Risks.
    i. Risk treatment involves selecting one or more options for modifying Risks, and implementing those options. Lower priority Risks may be accepted and monitored. For other Risks, the University is required to develop and implement a specific Risk Management plan including funding considerations.

i. Monitor and Review.
    i. Both monitoring and review should be a planned part of the Risk Management Process and involve regular checking or surveillance. It can be periodic or ad hoc. Responsibilities for monitoring and review should be clearly defined.

Appendix B

(40) The business continuity plans of operational units need to include information relating to:

a. the risk(s) identified;
b. the likelihood of the risk eventuating;
c. the business impact (consequence) of each risk;
d. any variation in impact due to the timing (in the business cycle) of the risk eventuating;
e. the level of risk in the light of existing controls (the residual risk);
f. the maximum tolerable (or acceptable) outage;
g. the controls or strategies in place to avoid the risks or mitigate the impact if the risk eventuates;
h. the time it will take to restore functions to an acceptable level by implementing current control strategies;
i. the further control strategies required (if any) to reduce the level of risk to an acceptable level;
j. the resources required to restore operations to an acceptable level; and
k. the officer responsible for managing each risk.

(41) To assist with this process the attached Business Continuity Plan template has been developed.

Status and Details

Status	Historic
Effective Date	9th August 2012
Review Date	31st March 2020
Approval Authority	University Council
Approval Date	20th July 2012
Expiry Date	23rd March 2021
Head of Work Unit	Mark Dixon Director, Governance Services
Enquiries Contact	Governance Services