Business Continuity Management Framework

Version – v1 – February 2026

Procedure Author – Head of Risk and Resilience

Procedure Owner – Vice Principal (Governance) and University Secretary

Parent Framework Statement – Corporate Governance

Public Access or Staff Only Access – Public

Version – v1 February 2026

Changes and Reason for Changes – New Framework

Glossary

Term	Definition
Activation	The implementation of business continuity procedures, activities and plans in response to a serious Incident, Emergency, Event or Crisis.
Activity	Set of one or more tasks with a defined output.
Assembly Point	The designated area at which employees, visitors and contractors assemble if evacuated from their building/site.
Business Continuity (BC)	The capability of the University to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.
Business Continuity Coordinator	Representative from the school/ department who acts as a single point of contact for BCM issues and is supported by a deputy.
Business Continuity Management (BCM)	A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats if realised might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value creating activities.
Business Continuity Plan (BCP)	documented information that guides an organisation to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.
Business Impact Analysis (BIA)	Process of analysing the impact over time of a disruption on the organisation.
Call Tree	A structured cascade process that enables a list of persons, roles and/or organisations to be contacted as a part of information exchange or plan invocation procedure.
Continual Improvement	A recurring activity to enhance performance.
Crisis	An abnormal, unstable and complex situation that represents a threat to the strategic objectives, reputation or existence of an organisation.
Critical Activities	Those activities which have to be performed to deliver the key products and services, and which enable an organisation to meet the most important and time-sensitive objectives.

Disaster	A physical event which interrupts business processes sufficiently to threaten the viability of the organisation.
Disaster Recovery (DR)	The strategies and plans for recovering and restoring the organisation's technological infra-structure and capabilities after a serious interruption.
Disaster Recovery Planning (DRP)	The activities associated with the continuing availability and restoration of the IT infrastructure.
Disruption	An incident whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives.
Emergency	An event or situation which threatens serious damage to human welfare, the environment or security of a place.
Essential services	A service to which priority must be given following an incident in order to mitigate impacts.
Exercise	Process to train for, assess, practice, and improve performance in an organisation.
Impact	An outcome of a disruption affecting objectives.
Incident	An event that can be, or could lead to, a disruption, loss, emergency or crisis.
Maximum Tolerable Downtime (MTD)	The duration after which an organization's viability will be irrevocably threatened if a product or service delivery cannot be resumed. It is the Maximum Tolerable period of Downtime.
Process	Set of interrelated or interacting activities which transforms inputs into outputs.
Recovery Point Objective (RPO)	Point to which information used by an activity must be restored to enable the activity to operate on resumption.
Recovery Time Objective (RTO)	Period of time following an incident within which an activity must be resumed.
Risk	effect of uncertainty on objectives.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation

Risk Management	Is the process of defining and analysing risks, and the deciding on the appropriate course of action in order to minimise these risks, while still achieving business goals.
Testing	Procedure for evaluation; a means of determining the presence, quality, or veracity of something

Source: ISO 22301:2019

Business Continuity Management Framework

Introduction

ISO22301 defines Business Continuity as an organisation's ability to operate business as usual in the event of a disruption. The University recognises the importance of ensuring as far as possible, the organisation's ability to maintain core functions during and after a disruption or incident. Business Continuity provides reassurance that the University can continue delivering essential services, allowing it to focus on growth, innovation, and strategic development with confidence.

This Framework outlines the principles and objectives to assist the University when preparing for, responding to, and recovering from business interruption with the aim of minimising the impact on students, staff and core University activities. This framework is aligned with the requirements outlined in ISO22301 (Business Continuity Management) which includes stages of planning, implementation, monitoring and reviewing and maintaining key documents to continually improve the University's approach to ensuring business continuity.

Additionally, UWS maintains an overarching Major Incident Plan (MIP) procedure that outlines how the University would respond to and manage a major disruption. The MIP ensures that the local business continuity plans (BCPs) at the school and departmental level are invoked in a coordinated manner for effective response.

Scope

This Framework applies to all Schools, Departments, projects, and activities at the University. It encompasses all potential disruptions, including but not limited to, planned and unplanned disruptions ranging from natural disasters, infrastructure failures, energy disruptions, cyber incidents and pandemics. The Framework outlines the implementation of business continuity management across the University.

Objectives

The purpose of this Business Continuity Management Framework and Procedure is to establish a proactive and resilient approach to managing disruptions that may affect UWS operations. The objectives of this Framework are to:

- Implement a Business Continuity Management framework that is informed by the requirements outlined in ISO22301 (Business Continuity Management)
- Reduce the disruption to organisational activities including but not limited to learning and teaching, research and operational functions.
- Embed Business Continuity within the University so that decision making is supported by risk management and business continuity
- Identify and prioritise the University's critical business activities through the use of a coherent Business Impact Analysis (BIA) process
- Establish robust business continuity plans that are fit for purpose and kept up to date as business processes evolve

- Increase awareness and promote business continuity across the organisation by embedding business continuity management into normal business activities

Roles and Responsibilities

Vice-Principal (Governance) and University Secretary	• Owner of the University's Major Incident Plan procedure and Business Continuity Framework. • Ensures that the Court/ Audit and Risk Committee is informed of business continuity developments, risks, and recovery progress as the executive owner. • Oversees the implementation of the BCM programme
Vice Chancellor's Executive	• Provides strategic leadership and oversight for the University's BCM programme. • Ensures that Business Continuity is embedded within their respective portfolios, with direct accountability for the effectiveness and implementation of the BCM Framework across all business areas under their remit. • Ensures that the BIA and response plans are understood, reviewed, and fit for purpose within their area of responsibility, and that appropriate assurance is provided to the University on business continuity preparedness. • Receives regular reports and recommendations from the Risk Group and Risk and Resilience, endorsing or requesting improvements as required, and ensuring that key risks and BCPs are subject to periodic scrutiny and review.
Risk Group	• Oversee business continuity planning and agree updates to business continuity framework and procedures. • Analyse findings from the BIA to evaluate whether existing recovery strategies are sufficient and, if necessary, recommend improvements to align continuity planning with the University's strategic objectives. • Oversee BCM activities such as BIA, BCP reviews and training and awareness activities

Major Incident Team	• Decides on what the University response to any referred incident will be and coordinates the implementation of that response • Communicates with internal and external stakeholders, including government agencies, emergency services, and the media, as needed. • Ensures local BCPs are activated and that relevant departments take appropriate action. • Ensures lessons learned sessions are conducted and protocols are updated following major incidents
Head of Risk and Resilience	• Responsible for ensuring the implementation of the business continuity management programme and framework within the University • Provides oversight to business impact analysis (BIA) and risk assessments and ensures their findings are integrated into University-wide risk management and strategic planning • Ensures the University is prepared for disruptions through training, awareness raising, and regular testing of business continuity plans • Maintain protocols/playbooks to address predictable disruption such as severe weather and utilities disruptions. • Reports to the Risk Group and Vice-Principal (Governance) and University Secretary on business continuity risks, incidents, and recovery performance
Deans of Schools and Directors/ Heads of Department	• Supporters of the Business Continuity Framework and responsible for the overseeing BCM in their respective areas and further embedding business continuity across the University • Ensure that BIAs and BCPs are developed, updated, tested, and effectively implemented for their respective Schools and Departments. • Sign off of their School/Department's Business Continuity Plan and ensures this is kept up to date • Ensure that key personnel within their Schools and Departments receive appropriate business continuity training. • Report on the status and testing of BCPs to Risk and Resilience as part of the assurance cycle.
All Members of Staff	• Contribute to the business continuity planning process by providing input on risks, critical functions, and mitigation strategies.

	• Ensure business continuity plans are in place for their respective activities • Follow business continuity procedures during disruptions and support recovery efforts • Participate in training, awareness programs, and business continuity exercises to enhance preparedness. • Report potential risks or vulnerabilities that could impact business continuity
Risk and Resilience Team	• Manages the business continuity management programme • Support Schools and Departments to carry out business impact analysis to identify critical operations and dependencies • Works with Schools and Departments to ensure effective BCPs are in place and that they are tested • Facilitates business continuity training, simulation exercises, and scenario testing to assess readiness and improve organisational response • Maintains incident logs, post-incident reviews, and performance assessments to drive continuous improvement in resilience strategies • Liaises with external stakeholders, such as local authorities, emergency services, and partner organisations, to align continuity planning with wider community and sector resilience strategies

Relationship with Risk Management

Business continuity management and risk management are closely connected, each serving distinct but complementary roles within risk and resilience. Risk management at UWS, guided by ISO 31000:2018, focuses on identifying and reducing risks before they occur, addressing a wide spectrum of potential impacts (financial, reputational risks legal and compliance risks etc) that may affect the University's objectives. In contrast, business continuity management, as outlined by ISO 22301:2019, ensures that if risks materialise despite preventive efforts, there are effective plans in place to maintain or rapidly restore critical services. In this sense, risk management aims to prevent disruptions, while BCM prepares the University to respond and recover when prevention is not possible. Risk owners remain responsible for prevention and reduction of risks, while plan owners are accountable for preparedness and continuity.

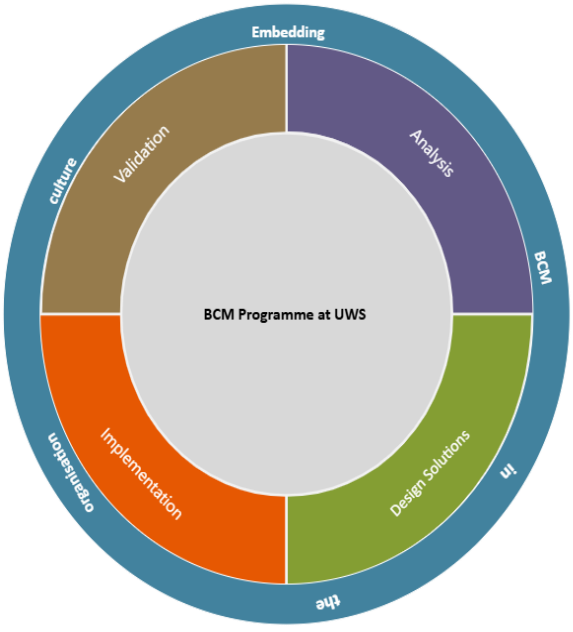
The risk assessment undertaken as part of the BCM process is not independent from, but rather complementary to, the University's broader Risk Management Framework. The BCM risk assessment specifically identifies threats to critical operations, particularly those revealed through the BIA process.

To ensure integration and traceability between these processes, major and serious risks identified during BIA exercises will be reconciled against the operational risk registers. Where a risk identified in the BIA does not require a specific BCP response, plan owners must document and justify this decision. This clear linkage between BIA/BCP outcomes and the operational risk register provides assurance that risks are managed comprehensively.

Business Continuity Management Process

The Business Continuity Management (BCM) Process at UWS is structured to embed resilience across all areas of the University to ensure continuous improvement, alignment with best practices. The Business Continuity Management Process has been developed as part of UWS' ongoing efforts to ensure BCPs are in place, communicated and periodically tested. The University adopts the Plan-Do-Check-Act (PDCA) model, recommended by the Business Continuity Institute (BCI) and aligned with ISO 22301, to drive continuous improvement in business continuity management. The University's approach reflects the Business Continuity lifecycle as documented in BCI Good Practice Guidelines 7.0 (2023) and the programme will be an 18month cycle managed by the Risk and Resilience Department. The department will be responsible for determining the scope and UWS approach to BCM including the establishing and implementation of the BCM process highlighted below:

ISO 22301:2019 BC Management Systems



BCI Good Practice Guidelines 7.0 (2023)

Analysis

Business Impact Analysis (BIA)

The BIA exercise is designed to identify and assess key critical activities, dependencies, and the potential impact of disruptions on University operations. The BIA ensures that UWS can continue to operate at an acceptable level following an incident by prioritising recovery efforts and aligning resource allocation with institutional needs.

Each School and Department is required to conduct a BIA review at least once every 18 months to maintain an up-to-date understanding of critical functions and their resilience requirements. These reviews help to identify key activities that must be restored immediately or within a predefined timeframe, assess the impact of disruptions on the University's core functions, and determine the necessary resources and recovery strategies to restore operations efficiently.

The Risk and Resilience Team will facilitate the BIA process by supporting areas to update their BIA template and providing guidance to ensure consistency and thoroughness across all Schools and Departments. A standardised BIA questionnaire template will be developed and used to systematically evaluate and document key aspects of each school/ department's critical functions which include:

- Critical activities
- Recovery Time Objectives (RTO)- which define the maximum acceptable downtime before a function's failure significantly impacts the University's operations and/or the student experience
- Recovery Point Objectives (RPOs) – maximum acceptable data loss measured in time, ensuring that the University's disaster recovery plans align with University requirements
- The alternative operational processes for key functions/ processes allowing for temporary workarounds if primary methods are unavailable e.g. remote learning platforms, alternative campuses, or manual processes where necessary
- Recovery resource requirements including workspaces, IT infrastructure, essential services, and emergency facilities, to ensure continuity of critical University operations.

The Risk Group will analyse findings from the BIA to evaluate whether existing recovery strategies are sufficient and, if necessary, recommend improvements to align continuity planning with the University's strategic objectives. This will ensure that Schools and Departments implement updated recovery measures to enhance resilience against evolving risks. The BIA process will also be subject to continuous improvement and validation, with regular updates to reflect changes in University operations, technological advancements, or newly emerging threats.

Risk Assessment

As part of the BIA exercise, Schools and Departments, supported by Risk and Resilience, will conduct targeted risk assessments to identify specific risks that may adversely impact their critical activities. The findings from this risk assessment will directly inform the development and refinement of BCPs and the overall Business Continuity Programme.

While the BCM risk assessment focuses specifically on risks that could disrupt day-to-day operations and continuity, it is closely aligned with the University's overarching risk management process. Operational, strategic, and compliance risks are often the root causes of disruption therefore must be considered in continuity planning. Risks identified as serious and major through the BIA process will be reviewed and reconciled with the relevant entries in operational risk registers, ensuring traceability and integration between risk management and business continuity planning.

The Risk Group will conduct an annual review of key risks identified through departmental assessments and University-wide risk monitoring efforts. This review will ensure that appropriate mitigation measures have been considered and implemented where feasible. If new or emerging risks are identified as critical to business continuity, the Risk Group will assess whether additional preventive or response strategies should be integrated into the University's BCM Programme or plans. Where necessary, further measures will be taken to reduce the likelihood of a risk occurring and/or to minimise its impact should it materialise.

Further detail on the integration between risk management and business continuity can be found in the "Relationship with Risk Management" section of this framework.

Design Strategy and Solutions (drafting BCPs)

Based on the BIA and risk assessment, this phase involves selecting and implementing appropriate recovery strategies and mitigation measures to ensure that UWS can maintain key services during a disruption. The strategies developed during this stage will be documented in the BCP in the implementation phase, tested, and continuously improved to ensure resilience and adaptability to various scenarios.

The design phase allows the University to establish and document structured Business Continuity strategies to be adopted within BCPs. This includes developing risk mitigation measures aimed at reducing the likelihood of disruptions and minimising their impact if they occur. For example, strategies may involve identifying third-party dependencies and establishing contingency agreements or securing backup sources for critical materials and infrastructure.

A structured recovery response will be developed to provide clear steps on how and when the University will adjust its response to a disruption. This response will be proportionate to the risk/threat level and will include predefined trigger points for activating alternative operating arrangements. These may include remote teaching and learning platforms, temporary relocation for students and staff, and continuity

measures for administrative and research activities. The strategy will also specify the Recovery Time Objective (RTO) for resuming operations, ensuring a clear and actionable timeline for incident response, recovery, and full operational resumption is noted in the BCP.

Additionally, resource allocation will be assessed and planned for all critical business functions identified in the BIA. This will ensure that essential operations have the required personnel, infrastructure, and technological support necessary to effectively respond to and recover from incidents. Resource planning will also consider emergency funding, alternative workspaces, backup IT infrastructure, and stakeholder communication requirements to maintain continuity across the University and recognising the multi-campus structures.

Implementation

The strategies developed in the design phase will be documented in Business Continuity Plans (BCPs) and other supporting documents, ensuring that all Schools, Departments, and critical functions within UWS are prepared to respond effectively to disruptions. These plans will outline recovery procedures, alternative operational arrangements by each individual area within schools/departments, and communication strategies that will be followed during a disruptive period or major incident. These will include strategies for short term and long-term disruption as stated in the BCP.

A University-wide Major Incident Plan (MIP) is maintained by the Risk and Resilience Team and outlines how the University would respond to a major incident. However, each School and Department is required to maintain their own Business Continuity Plan (BCP) that outlines how their specific operations will continue during a disruption. The BCP must also be approved and signed off by the Departmental Heads/ Deans before being shared with Risk and Resilience.

An important component of business continuity at UWS is IT Disaster Recovery (DR), which forms an integral part of the University's overall BCM programme. IT DR plans are developed, managed, reviewed, and monitored by the IT Department, ensuring that critical IT services and data infrastructure remain resilient, secure, and recoverable. While IT DR plans will align with the broader Business Continuity framework, they do not require the same elements as BCPs for physical operations. Instead, IT DR plans will focus on data integrity, system redundancy, and restoring access to critical digital platforms within acceptable recovery timelines.

Incident Management

UWS has established Incident Management Procedures, which are documented in the University's Major Incident Plan (MIP). These procedures provide a structured response framework for handling disruptions, ensuring that incidents are managed efficiently and effectively.

All minor incidents are logged on Awaken, the University's incident management system, to track, monitor, and analyse operational disruptions. However, incidents that have the potential to cause significant disruptions to University-wide services will

be escalated and managed in accordance with the MIP. The MIP outlines the roles and responsibilities that must be followed to coordinate an effective incident response.

Validation

Regular Business Continuity testing and validation are critical to ensure that BCPs remain effective, fit for purpose and aligned with University objectives. The purpose of validation is to confirm that the Business Continuity approach is relevant and accurate with ongoing efforts to improve organisational resilience and identify any gaps within the current approach. This stage also ensures that colleagues are trained and prepared to respond effectively during an incident or disruption.

Testing, Training, and Exercising

Regular testing, training, and exercising form a core part of the BCM programme which validates the effectiveness of BCPs and ensures that appropriate response to disruption is in place. Testing and exercising activities will be conducted using different approaches to ensure comprehensive coverage, including live drills, tabletop exercises, technical recovery simulations, and call tree tests.

Types of BC Testing and Exercising:

- **Call Tree Testing**: A test will be done for key contacts callout to confirm the effectiveness of emergency communication protocols. This will be conducted annually to verify that contact details are up-to-date and that communication cascades effectively during a disruption.
- **Scenario-Based Workshops**: A scenario-based workshop exercise for the Vice-Chancellor's Executive (VCE) and Risk Group will be conducted at least once every 18 months. These workshops will simulate realistic business continuity scenarios to evaluate leadership decision-making, crisis response coordination, and framework effectiveness.
- **Recovery Testing**: This includes IT Disaster Recovery (DR) simulations and user exercises to test the effectiveness of IT continuity and resilience measures. This will ensure that critical IT services, data backups, and recovery solutions can be restored within the agreed Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- **Emergency Response Testing**: While not part of business continuity exercising itself, fire drills, evacuation exercises, and emergency response training remain critical to the University's overall resilience. These are conducted in accordance with the UWS Fire Safety Plan and the Emergency Evacuation of People with Disabilities Procedure and serve as a transition into business continuity and recovery phases when necessary.

All BCPs and related arrangements must be reviewed, tested, and exercised at least once every 18 months by their respective plan owners, using a variety of appropriate scenarios and formats. Additionally, each area is required to review its BCP on an

annual basis to ensure plans remain current and aligned with the University's BCM objectives. UWS's BC exercise programme will include cross-University participation, involving colleagues from all levels of the organisation. Exercise planning will also ensure the involvement of individuals with direct BC responsibilities as well as colleagues from their area.

Risk and Resilience will provide guidance, templates, and periodic sample testing, as well as maintaining oversight and a register of reviews and exercises. However, responsibility for direct testing, exercising, and ongoing assurance remains with individual plan owners. Plan owners must demonstrate annually to Risk and Resilience that their BCPs have been reviewed and tested as required. Summaries of exercise outcomes and test reports will be submitted to Risk and Resilience, with key updates provided to the Risk Group for further discussion and continuous improvement.

Training and Awareness

To ensure that all University staff understand their roles in business continuity, UWS will implement a planned and strategic communications approach to deliver training and awareness of business continuity. The approach will aim to proactively engage all areas of the University and will be coordinated by Risk and Resilience. The Risk and Resilience Team will also be responsible for creating e-learning modules and resource materials for business continuity awareness training.

These training modules will highlight staff responsibilities during disruptions, incidents, and major emergencies. Departmental training sessions will be conducted as needed to reinforce specific recovery processes related to their area of operation.

Management Review and Continuous Improvement

As part of the Business Continuity Management programme, UWS ensures that regular reviews and continuous improvements are conducted to keep its Business Continuity approach relevant and effective. The Risk Group will provide an initial level of scrutiny and advice to Risk and Resilience, making recommendations to the VCE as required. The Risk Group will support this process through periodic review of performance and assurance reporting, making recommendations for improvements.

A summary report will then be compiled and submitted to the Audit and Risk Committee (ARC) on the effectiveness and appropriateness of the Business Continuity Framework. Additionally, at the beginning of each year, the BCM Programme will be reviewed to set targets, objectives, and Key Performance Indicators (KPIs) for business continuity performance. The VCE is ultimately responsible for agreeing targets, objectives, and KPIs for the BCM programme, ensuring alignment with University strategy and priorities and adjust planning efforts based on:

- University strategy and operational priorities.
- Emerging risks and regulatory changes.
- Technological advancements that impact continuity planning.

Communication

Effective communication is critical during a disruption for ensuring continuity of the University's activities and operations. The availability of multiple communication channels is critical to relay information to staff, students and key stakeholders during an incident or disruption. A communication plan will be reviewed and updated in line with the Business Continuity Framework.

Equality Impact Assessment

An Equality Impact Assessment was completed on 4th April 2025.

Further Advice and Guidance

For further information and guidance on business continuity please contact riskandresilience@uws.ac.uk