University of Dundee

University of Dundee
Business Continuity Management Framework

1. Introduction

1.1. Normal activities can be disrupted unexpectedly at any time. Whilst, in most cases, this can be dealt with quickly and effectively, some situations or incidents may escalate into what we call a major incident or crisis. The impact of such situations could include: the inability to deliver teaching activities, loss of research facilities, financial loss and/or damage to the University's reputation. But there may be other organisational or local impacts.

1.2. In order to mitigate the impact of such situations, the University has an institutional Business Continuity Management Framework. This seeks to minimise disruption and enable the University to resume business as usual as promptly as is possible.

1.3. The Framework assumes a worst-case scenario. The Framework also assumes that fire prevention, security and health & safety standards are being applied consistently throughout the University.

2. Business Continuity Management

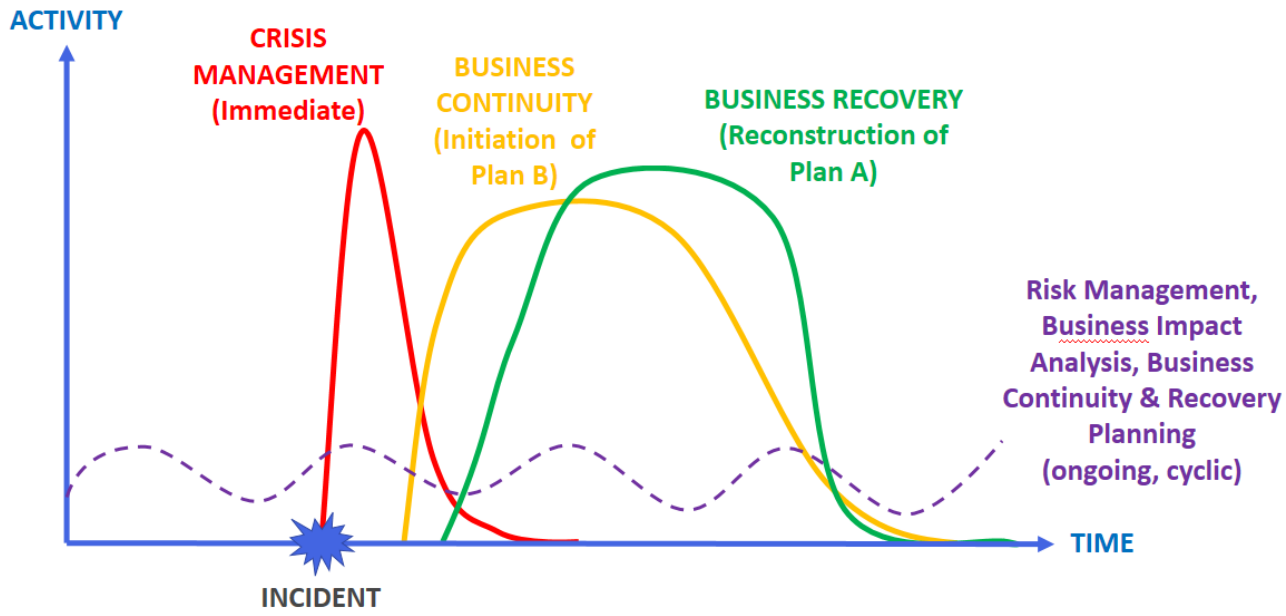
2.1. Business Continuity Management is a proactive approach to identifying potential threats to the organisation and responding to the associated impact on business operations that these threats might cause. Good business continuity management provides a framework for building resilience. It has the following objectives:

- To take into account the key risks facing the institution, as identified in the institutional and local risk registers and through horizon scanning;
- To determine what short, medium and long term measures are required to minimise impact and replicate critical services;
- To ascertain what external stakeholders, if any, need to be informed.

2.2. The key components of Business Continuity Management are summarised below:

Activity	Description
Risk Management	Focused on mitigation: reduce likelihood/ impact of disaster
Crisis Management	Management of incident, supplemented and influenced as appropriate by external stakeholders (i.e. by fire department in the event of a fire)
Business Continuity	'Plan B': how can we continue to operate with loss of facilities/staff/technology etc
Business Recovery	Back to 'Plan A': getting facilities/staff/technology back and returning to business as usual

These components are interrelated as the diagram below depicts:



Not all situations that require business continuity/business recovery plans will start with an incident that results in a 'crisis'; pandemic flu would be an example of this.

3. Risk Management

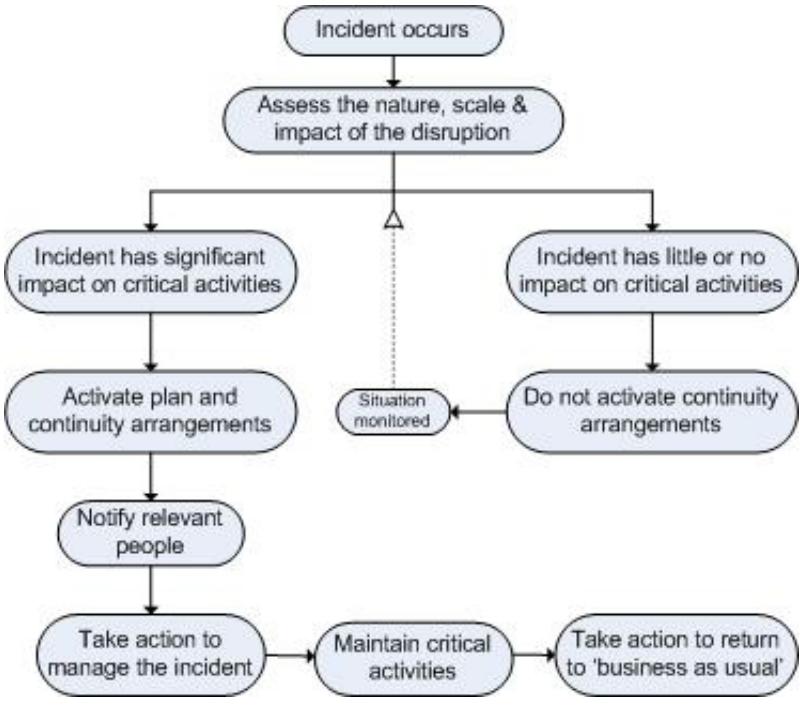
3.1. The process for Risk Management at the University of Dundee is through local risk registers and the institutional risk register. As stipulated in the Risk Management Policy[1], all Schools and Directorates are expected to own a risk register. These are to be revised on a regular basis and are reviewed by the Risk Management Oversight Group annually.

The Risk Management Oversight Group monitors the institution's performance in identifying, assessing, prioritising and mitigating key risks related to all aspects of the University's activities and provides guidance in relation to the management of risks. This includes identifying trends amongst local risks registers and escalating up to an institutional level if required.

The Risk Management Oversight Group report to the Audit & Risk Committee to provide assurance on risk management at a local level. The Audit & Risk Committee review the institutional risk register twice a year and report to the Court.

[1] Risk Management Policy

4. Process for Incident/Crisis Management, Business Continuity & Recovery



4.1 The purpose of Incident/Crisis Management is to:

- Protect the safety of staff, visitors and the wider community
- Protect vital assets e.g. equipment, data, reputation, etc.
- Ensure necessary communication takes place
- Support the Business Continuity phase
- Support the Business Recovery phase

4.2. The University has the below means to categorise incidents to provide guidance in the event of an incident:

Bronze Level Incident	**Silver Level Incident**	**Gold Level Incident**		**External Incident Gold/Silver/Bronze**
Internal to University; can be managed at a School/Directorate level	*Internal to University*	*Internal to University but may have external impact*		*An incident off campus tha impacts on the University*
Minor/local incident causing no serious physical threat to people, infrastructure or activities	Incident poses a potentially serious threat to people, infrastructure or operations	Major incidents that threaten people, infrastructure or operations		Could impact on operations due to aid being offered or loss of staff
Response can be managed within resources/may require minor emergency services assistance	May require **Incident Response Team** to assemble	Requires interaction with emergency responders, local resilience officer, press etc. Requires **Incident Management Team**.		May require interaction with emergency responders, local resilience officer etc.
May attract social media attention	May require emergency assistance	Incidents which could impact wider community/		Likely to impact wider community and have a knock-on effect on University

		Incidents which could escalate		
No risk to reputation, compliance (legal) or operations	Risk to reputation, compliance or integrity of institution	Serious risk to reputation, compliance or integrity of institution		Could risk reputation, depending on nature of incident
e.g. isolated evacuation of a building resulting in limited disruption, individual in hospital with minor injuries	**e.g.** loss of use of part of a building, unnatural death of a student/member of staff, individual in hospital with serious or critical injury to individual on campus	**e.g.** death of an individual on campus, individuals in hospital, outbreak of disease, terrorist activity, multi casualty incident		**e.g.** extreme weather conditions threatening the closure of a campus, incident in Dundee City, incident that requires aid etc.
e.g. loss of network services in an entire building, failure of an enterprise application or cloud service	**e.g.** loss of network services across campus, failure of significant infrastructure component affecting multiple enterprise applications, prolonged loss of cloud service	**e.g.** total loss of data centre facility, failure of entire infrastructure component or cloud service affecting many services necessitating extended recovery period.		**e.g.** cyber-attack impacting local provider, partner or supplier

The full process for incident response, crisis management and the utilisation of the Gold, Silver and Bronze teams is enclosed as **Annex 1** (this includes an example of how this would work, using a fire in the library scenario). The membership of these teams is provided in **Annex 2**.

4.3. Crisis/Incident Management Process

Actions to Protect the Safety and Welfare of Staff, Visitors and The Public

ACTION
Evacuate the building, if necessary, using normal evacuation procedures for the building
Ensure all staff report to the Assembly Point
Call emergency services (as appropriate)
Check that all staff, contractors and any visitors have been evacuated from the building and are present. Consider safety of all staff, contactors and visitors as a priority
Ensure log of incident is started and maintained throughout the incident phase
Record names and details of any staff, contractors or visitors who may have been injured or distressed in the incident.
Forward details of any fatalities or injuries in the incident to HR (depending on scale of incident) and agree action that will be taken.
Assess impact of the incident to agree response / next steps
Log details of all items lost by staff, visitors, etc. as a result of the incident

Consider whether the involvement of other teams, services or organisations are required to support the management of the incident. Depending on the incident the following may be approached to assist with incident management: • Estates and Campus Services • Human Resources • Health and Safety • Legal • Occupational Health • IT • Schools & Directorate Staff

Communication Actions

In the event of an incident and this plan being activated, the following people should be contacted. Nature of contact will depend on the incident type and time it has occurred. See **Annex 2** describing the staff to be involved in the communications actions dependent on the scale of the incident.

Actions to Support Business Continuity

ACTION
Recover vital assets/equipment to enable delivery of critical activities if it is safe to do so
Assess the key priorities for the remainder of the working day and take relevant action. Consider sending staff home, or to alternate location, etc.
Inform staff what is required of them,
Publicise the interim arrangements for delivery of critical activities. Ensure all stakeholders are kept informed of contingency arrangements as appropriate

Actions to Support Business Recovery

ACTION
Take any salvage/asset recovery actions that are appropriate. Remove any equipment, furniture, records etc. that are at risk of damage.
Continue to log all expenditure incurred as a result of the incident. Use a financial expenditure log to record costs incurred as a result of responding to the incident
Seek specific advice/ inform University Insurance Company

5. Business Continuity

The purpose of the business continuity phase of response is to ensure that critical activities are resumed as quickly as possible and/or continue to be delivered during the disruption. The University's approach to business Continuity focuses on three areas: loss of people, loss of building and loss of technology. The strategy for each of these will follow the below business capability priorities, as approved by the University Executive Group (see **Annex 3**). The overall set of business continuity actions will be as follows.

ACTION	FUTHER INFO/DETAILS
Identify any other staff required to be involved in the BC response	Depending on the incident, the Business Continuity Team may need additional/specific input in order to drive the recovery of critical activities
Evaluate the impact of the incident	Use an incident impact assessment form to understand the impact of the incident on 'business as usual' working activities.
Plan how critical activities will be maintained.	Consider: ▪ Immediate priorities ▪ Communication strategies ▪ Deployment of resources ▪ Finance ▪ Monitoring the situation ▪ Reporting

ACTION	FUTHER INFO/DETAILS
Log all decisions and actions, including what is decided not to action and include rationale	Use decision and action log to do this
Log all financial expenditure incurred	Use financial expenditure log to do this
Allocate specific roles as necessary	Roles allocated will depend on the incident and availability of staff
Secure resources to enable critical activities to continue/be recovered	Consider requirements such as the staffing, premises, equipment. Refer to Local BCP / BIA for more detailed information on resource needs.
Deliver appropriate communication actions as required	Ensure methods of communication and key messages are developed as appropriate to the needs of your key stakeholders e.g. students, suppliers, staff, University Executive Group, Senate, Court, Scottish Funding Council, Scottish Government, etc.

5.1 Business Continuity Strategy for Loss of People

The loss people on campus could have a significant impact on the University's ability to meet its strategic objectives. This may be due to one key member of staff being absent for a prolonged period, several staff being away (due to snow, illness, industrial action etc.) or even a pandemic situation which requires the University to close.

Responsibilities:

1. Senior members of staff (Deans, Directors and School Managers) should, where possible, respond to incidents out of hours where required. All Schools and Directorates should maintain an up-to-date list of out-of-hours contact details for key/relevant staff and this must be shared with Security.

2. All University managers should have a named deputy who is aware that it is their responsibility to deputise in the event of their being unavailable during a crisis/period of disruption.

3. Local Business Continuity & Recovery plans will depict how loss of staff will be managed at a local level.

4. It is the responsibility of Deans, Directors and School Managers to ensure that Local Business Continuity & Recovery Plans contain a list of key staff and a plan to mitigate the loss of key staff.

Loss of staff:

1. In the event of a large number of staff being absent in one area, the Director of Human Resources & Organisational Development will organise members of the HR team to support arrangements for secondment where possible.

2. In the event of a large number of staff being absent across the institution, the HR team will seek reciprocal arrangements with fellow universities to ensure adequate HR support is in place.

3. The University Executive Group will determine if the University should close.

Loss of Senior Management:

1. With regard to the absence of a Dean for a prolonged period of time, the University Executive Group should be consulted to agree on interim arrangements.

2. With regard to the absence of a Director, the University Secretary will determine if interim arrangements are required.

3. In the event that a School Manager is absent, the Deputy University Secretary & Director of Academic & Corporate Governance will determine if interim arrangements are required.

4. Directors and Deputy Directors must ensure that their annual leave arrangements do not result in there being a lack of leadership in the event of a crisis/period of disruption.

5. The Court Resilience Plan outlines actions if there is a loss of leadership within the University Executive Group.

Loss of Governance:

1. In the event of a crisis situation it may be necessary to make emergency purchases. The Schedule of Delegation stipulates that the Director of Finance can approve individual purchases between £25k and £1.25m and the University Executive Group and University Secretary can approve individual purchases between £1.25m and £3m. Purchases over £3m require approval from the Finance & Policy Committee.

2. Additionally the Resilience Plan outlines the University's plan in the event of a vacancy in the Office of the Principal or failure of the University Court or any of its members.

In addition, following a technology or estates incident, additional HR support may be required to support the incident team and affected members of staff. Mutual aid from a fellow institution (potentially involving the secondment of staff) may be required to ensure the HR team is equipped to do this whilst maintaining business as usual.

Business Recovery Strategy for Loss of People

This will normally entail back to work interviews and may involve meetings with occupational health if required and phased returns arranged. This may put added pressure onto HR team, and additional HR support may be required for a period of time (i.e. mutual aid from fellow institution). Managers are expected to check in with staff who have returned to work to ensure that they are adequately supported.

5.2. Business Continuity Strategy for Loss of Building

The loss of space on campus may be temporary and short term (e.g. access issue, minor security issue, false alarm fire evacuation, severe weather disruption), medium term (e.g. loss of access to a specific building area or room due to localised fire, loss essential services like gas or water within a building, or localised flooding), or long term (e.g. total loss of an essential infrastructure system like the Energy Centre, or a total loss of a building through fire).

1. Prioritise site security and containment of any dangerous areas to enable and assist fire brigade investigation and loss adjuster assessments. Schools / Directorates to instigate early phases of Business Continuity Plans.

   The Estates and Campus Services team have a Disaster Recovery Plan which is designed to serve the needs of the University in the event of a catastrophic failure which would prevent the use of parts

or the whole of a building or campus. The Plan includes all contact details for relevant key staff members, critical roles and identifies key actions to be taken to contain an incident.

This strategy relies on incident management and requires Schools and Directorates to have their own Business Continuity plans which will enable them to initially deal with the immediate problems posed by a loss of space or access to key facilities on campus whilst the Estates and Campus Services teams work to contain the issue and make the area / property safe by bringing the incident to a defined conclusion.

2. Appoint operational team to work with affected schools / directorates to instigate medium term Business Continuity Plans leading to temporary accommodation solution (instigate Plan B solution)

   Estates and Campus Services have a temporary accommodation solution for situations where a medium-term plan is required in the event of significant disruption on the City Campus. This would entail the procurement of a temporary building to be located on the Tennis Courts. Not all building users could be occupied in such a premises for example, highly technical areas are more challenging to provide and there is a limitation on capacity which will prevent us from accommodating all users from larger buildings.

3. Appoint project team to oversee the development of refurbishment works / new build project to return operations to original business operations long term via long term actions in school / directorates Business Continuity Plans (return to Plan A).

   Estates and Campus Services will work with the affected School / Directorate to reinstate their operations. This activity may require minor adjustments (e.g. working with IT to relaunch door security), may be a medium term activity (e.g. a refurbishment following a flood), it might be a substantial undertaking (e.g. new build replacement property).

5.3. Business Continuity Strategy for Loss of Technology

The outcome of the Business Impact Analysis process has been to identify the following service portfolios as critical:

Priority	IT Service Portfolio	Service Description
1.	Infrastructure	Enterprise-level hardware, software, systems, and network infrastructure that provide underlying support for institutional activities. Includes data centers, network backbone, wireless, central storage and system backup solutions, server virtualization, and systems management and operations.
2.	Security	Infrastructure and services that provide security, data integrity, and compliance for institutional activities. Includes security services such as virus protection, encryption, privacy impact assessments, information risk management, emergency preparedness, data security, identity management solutions, access controls (i.e., passwords, accounts, and authentication), audit and monitoring systems and services, and data access and stewardship.

3.	Communication and Collaboration	IT services that facilitate institutional communication and collaboration needs. Includes e-mail, calendaring, telephony/VoIP, video/web conferencing, unified communications, web content management system, web application development and hosting, and media development.
4.	End-Point Computing - My IT	Services that enable community members to do their day-to-day work, including providing access to enterprise services. Includes network access, user file storage, end-point computing backup solutions, desktop virtualization, computer labs, and printing.

The following services will be recovered in line with the University agreed Business Capability priorities and will vary depending on the time within the University calendar:

Priority	IT Service Portfolio	Service Description
5.	Teaching and Learning	Instructional technology, tools, and resources directly supporting teaching and learning. Includes learning management systems, in-class and online course development, learning analytics, course evaluation, lecture capture, webinars, and other academic tools for faculty and students.
6.	Administrative and Business	Enterprise and local services that support the administrative and business functions of an institution. Includes analytics, business intelligence, reporting, finance, human resources, student information systems, timetabling advancement, research administration, and conference and event management.
7.	Research	Services supporting the institution's research activities, including specialized storage and computation, high-performance computing (HPC), visualization, and lab-management systems.

All project activities and the following services are non-critical and consideration will be given to:

- Not recovering these activities until critical activities have been resumed
- Suspending these activities and diverting their resources to support the critical ones

IT Service Portfolio	Service Description
IT Professional Services	Services that are consultative in nature, in contrast to the other categories, which tend to be technology based; these may be a combination of customer-facing and non-customer-facing services. Includes IT training, consulting/advisory services, business continuity/disaster recovery, enterprise architecture, portfolio/project management, and ITSM.

Infrastructure Service Portfolio Resilience

Data Centre, Power & Cooling Infrastructure

The University operates two data centres, in Springfield and JBC. These datacentres provide resilient power and cooling backed by generators and modular UPS supplies. In the event of a catastrophic loss of a data centre, additional equipment can be installed into the secondary data centre to provide additional capacity.

Storage, Backup and Archiving Infrastructure

All storage is provided using modular storage arrays preventing the loss of data from individual component failure. The storage platforms are configured to provide instant snapshots to preserve data within the storage layer for 7 days. Further resilience is provided by two tape libraries for Backup and Archiving, geographically located 5km apart. All backup data is replicated between these two libraries and it is possible to restore from each location independently in the event of a disaster. In the event of a catastrophic failure, data and applications will be restored from the tape frames however it should be noted that the data volumes involved mean that this will be a significant undertaking lasting months during which alternate provision will be necessary for some activities. During this time the University will be required to use Office 365 to provide alternate storage capability.

Core & Data Centre Network Infrastructure

The Core, Distribution and Data Centre networks are fully resilient with no single point of failure. Fibre optic cable paths are, wherever possible, independently routed to prevent a single incident affecting service provision. The network is monitored and supported by an external supplier to provide additional reassurance to the service provision.

Server & Hypervisor Infrastructure

The underpinning server infrastructure is constructed using modular servers with resilience for storage, network and power. These are aggregated into a resource pools via a hypervisor enabling virtual machines to be restarted on alternate hardware in the event of an incident. Currently capacity limits the resilience of failure to 1/16th of the overall capacity. In addition to the virtual environment some services such as High-Performance Computing are provisioned using physical hardware. Wherever possible these are built using multiple nodes rather than single systems however single node systems do exist. Whenever possible, these systems are converted from physical assets to either running on the virtual infrastructure or are subsumed into the resilient High-Performance Computing cluster.

Security

The University operates independent, resilient firewalls pairs at the perimeter and the datacentre. These are configured with default deny inbound rules. Remote access to the university network is currently provided by a single VPN device. Client devices are configured with anti-malware and application whitelisting to minimise the likelihood of malicious software invading the environment. Staff and Student Office 365 accounts are protected by Multi Factor Authentication. In the event of a failure of security on server / storage infrastructure restoration of data from either storage snapshots or backup and archiving solutions will be necessary.

Endpoint/Client Computing

Most staff are now issued with laptops enabling staff to work from alternate locations. Staff are expected not to store primary data on local devices or portable storage media and thus in the event of a catastrophic loss, client endpoints will be either re-imaged to a baseline state or purchased afresh with a standard configuration.

Communications & Collaboration

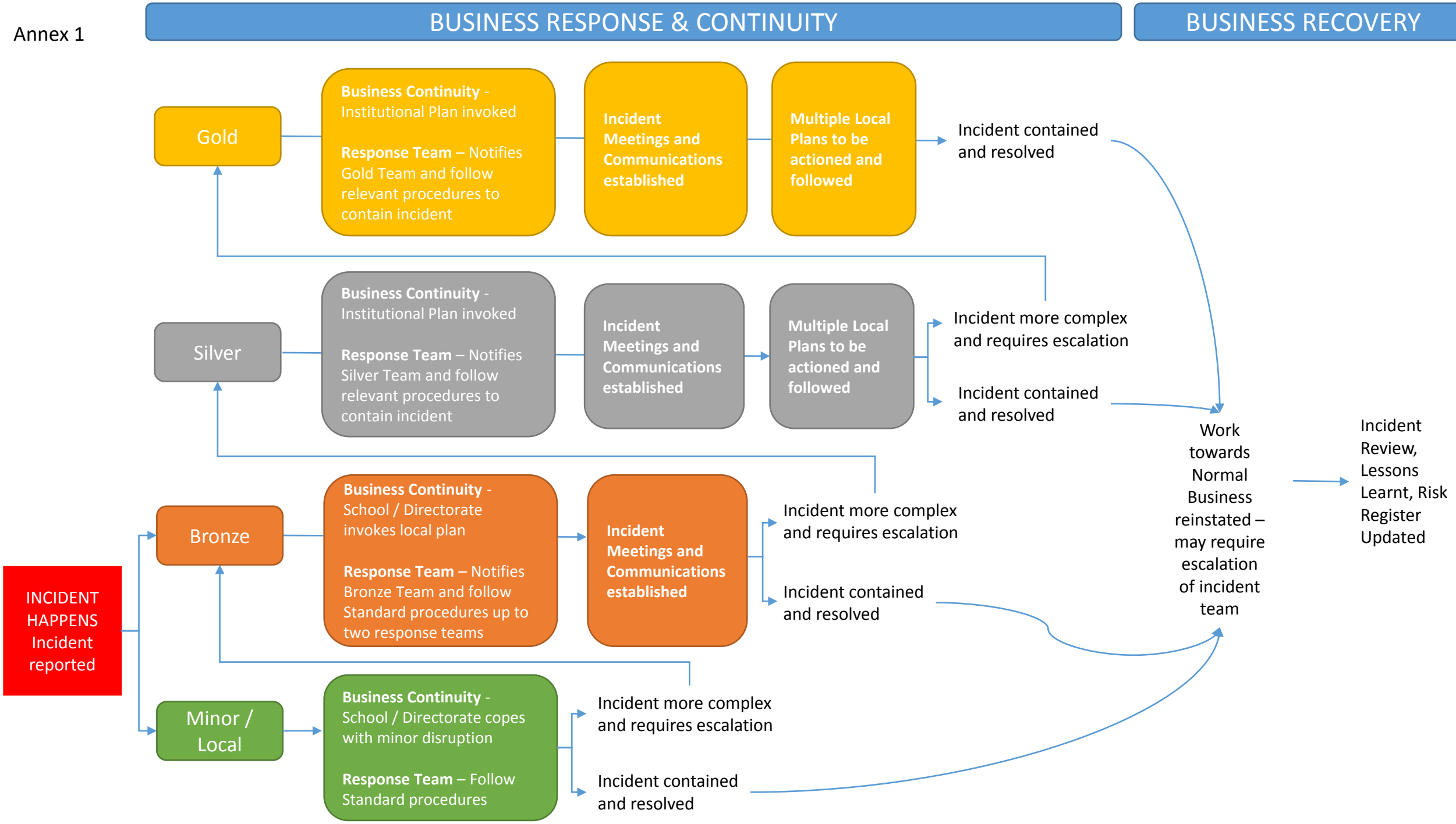
The university operates an on-premise telephony system with resilient services provided from both data centres. In addition, Office 365 provides a globally available communication and collaboration platform including email, instant messaging, voice and video calling, file storage and sharing.

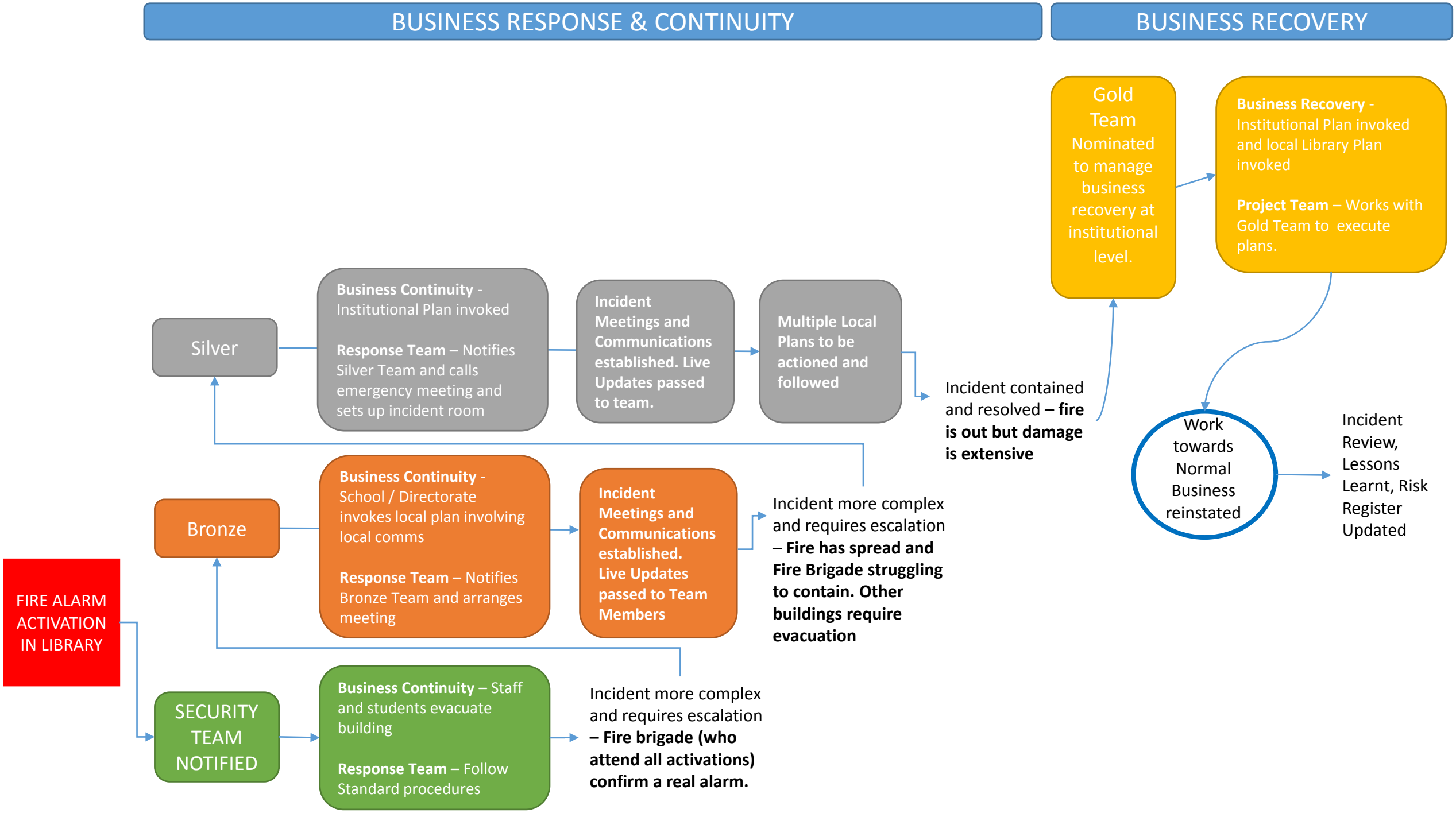
6. Business Recovery Plan

The purpose of the recovery phase is to resume normal working practices. Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g. from a different building or using a different, replacement technology.

	ACTION	FUTHER INFO/DETAILS
1.	Agree and plan the actions required to enable recovery and resumption of normal working practises	Agreed actions will be detailed in an action plan and set against timescales with responsibility for completion clearly indicated.
2.	Continue to log all expenditure incurred as a result of the incident	Use a financial expenditure log to do this
3.	Respond to any long terms support needs of staff	Depending on the nature of the incident, the Business Continuity Team may need to consider the use of Counselling Services e.g. internal Occupational Health involvement or appropriate External Agencies
4.	Carry out a 'debrief' of the incident and complete an Incident Report to document opportunities for improvement and any lessons identified	Use an Incident Report Form to do this. This should be reviewed by all members of the Business Continuity Team to ensure key actions resulting from the incident are implemented within designated timescales
5.	Review this Continuity Plan in light of lessons learned from incident and the response to it	Implement recommendations for improvement and update this Plan. Ensure a revised version of the Plan is read by all members of the Business Continuity Team
6.	Publicise that there is now 'business as usual'.	

Annex 1


BUSINESS RESPONSE & CONTINUITY
BUSINESS RECOVERY
INCIDENT HAPPENS Incident reported
Gold
Business Continuity - Institutional Plan invoked
Response Team – Notifies Gold Team and follow relevant procedures to contain incident
Incident Meetings and Communications established
Multiple Local Plans to be actioned and followed
Incident contained and resolved
Silver
Business Continuity - Institutional Plan invoked
Response Team – Notifies Silver Team and follow relevant procedures to contain incident
Incident Meetings and Communications established
Multiple Local Plans to be actioned and followed
Incident more complex and requires escalation
Incident contained and resolved
Bronze
Business Continuity - School / Directorate invokes local plan
Response Team – Notifies Bronze Team and follow Standard procedures up to two response teams
Incident Meetings and Communications established
Incident more complex and requires escalation
Incident contained and resolved
Minor / Local
Business Continuity - School / Directorate copes with minor disruption
Response Team – Follow Standard procedures
Incident more complex and requires escalation
Incident contained and resolved
Work towards Normal Business reinstated – may require escalation of incident team
Incident Review, Lessons Learnt, Risk Register Updated


BUSINESS RESPONSE & CONTINUITY
BUSINESS RECOVERY
FIRE ALARM ACTIVATION IN LIBRARY
SECURITY TEAM NOTIFIED
Business Continuity – Staff and students evacuate building
Response Team – Follow Standard procedures
Incident more complex and requires escalation – Fire brigade (who attend all activations) confirm a real alarm.
Bronze
Business Continuity - School / Directorate invokes local plan involving local comms
Response Team – Notifies Bronze Team and arranges meeting
Incident Meetings and Communications established. Live Updates passed to Team Members
Incident more complex and requires escalation – Fire has spread and Fire Brigade struggling to contain. Other buildings require evacuation
Silver
Business Continuity - Institutional Plan invoked
Response Team – Notifies Silver Team and calls emergency meeting and sets up incident room
Incident Meetings and Communications established. Live Updates passed to team.
Multiple Local Plans to be actioned and followed
Incident contained and resolved – fire is out but damage is extensive
Gold Team Nominated to manage business recovery at institutional level.
Business Recovery - Institutional Plan invoked and local Library Plan invoked
Project Team – Works with Gold Team to execute plans.
Work towards Normal Business reinstated
Incident Review, Lessons Learnt, Risk Register Updated

Annex 2: Leadership in the event that the Strategy is enacted

Gold Team: Strategic Leadership

Membership of the Gold team will comprise the University Executive Group or a sub-set of this Group as deemed appropriate.

Role:

- Strategy. Outline strategy (inclusive of press)
- Communicate strategy
- Be contactable and remain available to the Silver convener(s)
- Must retain strategic oversight.

Silver team: Tactical decision-making

There may require to be multiple conveners of the Silver Team, at the University Secretary's discretion. The members of the Silver Team shall usually be:

- The University Secretary
- Director of Estates & Campus Services
- Director of UoD IT
- Director of Academic & Corporate Governance
- Head of Corporate Communications
- All Directors/Deans/School Managers as required and subject to invitation from the Silver Team Convener(s).

Silver role:

- Tactical/operational
- Appoint Bronze convener as appropriate
- Communicate tactical plan

Bronze Team: Operational

The Convener of the Bronze team will depend on the nature of the incident. The following members would be expected to be in attendance:

- Head of Precinct Services
- Head of Safety Services
- HR Officer
- Student Services Officer
- DUSA Representative

Bronze role:

- Support implementation of strategy and tactical response to incident

All decisions and discussions must be logged.

! yŷŜĖ o

Priority 1	Managing Facilities and Property	All activities aimed at ensuring that organisational facilities and properties are fit for purpose, future-proofed and maintained to the appropriate standards, including security and health and safety.
	Managing ICT	All activities aimed at the efficient and effective development, delivery and management of ICT resources and access to those resources.
	Managing Student Support & Wellbeing	All activities aimed at ensuring students receive adequate support and advice throughout their time at organisation.
	Providing Legal Services	All activities aimed at ensuring the availability of effective legal services.
	Government, Public & Stakeholder Relationships	All activities aimed at ensuring a continuous level of engagement is maintained between the organisation and its customers, stakeholders & other interested parties.
	Managing People	All activities aimed at the management and organisation of staff and their contribution to the institution.
	Managing Research Infrastructure	What the organisation does to manage its specialist research infrastructure.
	Managing Finance	All activities aimed at the efficient and effective management of money (funds) in such a manner as to allow the organisation to accomplish its objectives.
Priority 2 (Dependant on Time of Year)	Managing Accommodation	All activities aimed at the provision of accommodation to students, and potentially other people when not occupied by students.
	Managing Student Admission	All activities aimed at managing student applications, placement offers and quotas.
	Matriculating Students	All activities aimed at ensuring that students are fully enrolled at the programme and module level and inducted into the organisation community.
	Assessing Students	All activities aimed at assessing whether a student has achieved the learning outcomes of the curriculum.
	Completing and Graduating Students	All activities aimed at conferring degrees (and other awards) to students who have qualified appropriately and hence become graduates.
	Delivering Learning and Teaching	All activities aimed at delivering a learning experience to students of the organisation and enabling them to engage with learning in the subjects as described in the curriculum. This includes the delivery of teaching activities as well as other activities that support a meaningful learning environment.
Priority 3	Managing Research Funding	All activities aimed at obtaining and managing funds to undertake research projects.
	Delivering Research	All activities aimed at undertaking and delivering the research itself.
	Attracting and Recruiting Students	All activities aimed at planning and delivering campaigns and events that aim to recruit and convert undergraduate and postgraduate students to the organisation.
	Administrating Students	All activities aimed at maintaining accurate records of students and their administrative and academic statuses during their time at organisation, and managing the change of records and statuses.
	Managing Library Services	All activities related to the management of library resources and access to those resources. This does not include the physical library environment.
	Academic Administration	All activities aimed at managing academic policies, regulations, scheduling and related customer feedback.
	Managing Curriculum	All activities aimed at educators and administrators collaborating on the creation, development, design, review, approval, assessment, and refinement of curriculum content to achieve desired student outcomes.
	Publishing Research	All activities aimed at publishing research findings and reporting outputs.
	Research Impact	All activities aimed at maximising and promoting the impacts of research undertaken at the organisation.
	Managing Research Compliance	What the organisation does to manage and ensure compliance with research rules and regulations, including ethics.
	Training Researchers	All activities aimed at training and developing the organisation's researchers, including both staff and post-graduate research students.
	Planning and Managing Research Opportunities	All activities aimed at determining and defining the research programmes and projects that will be undertaken at the organisation.
	Improving Research	All activities aimed at the continuous improvement of research quality and performance.
Priority 4	Commercial Sourcing	All activities aimed at ensuring that the organisation can effectively identify and assess commercial opportunities.
	Commercial Engagement	All activities aimed at managing the organisations relationship with commercial partners.
	Commercial Delivery	All activities aimed at the successful fulfilment of the organisations commercial activity commitments.
	Commercial Monitoring	All activities aimed at scrutinising the effectiveness and performance of all commercial endeavours within the organisation.
	Managing Marketing & Promotions	All activities aimed at the promotion of the institution to prospective and current students, businesses and the general public.
	Corporate Governance	All activities aimed at ensuring compliance with external regulations and internal policies, including management of risk.
	Engaging with Alumni	All activities aimed at Alumni engagement ensuring the organisations alumni is fully involved in the life of the institution as valued supporters, advocates, and lifelong learners who contribute to, and benefit from, connections to each other and to the organisation.
	Managing Strategy	All activities aimed at ensuring that the organisation has a coherent, integrated and sustainable vision, mission and strategy.

Strategy & Governance

- Corporate Governance
- Managing Strategy

Teaching & Learning

- Managing Curriculum
- Attracting & Recruiting Students
- Managing Student Admission
- Matriculating Students
- Delivering Teaching & Learning
- Assessing Students
- Completing & Graduating Students
- Engaging with Alumni
- Academic Administration
- Administrating Students
- Managing Student Support & Wellbeing

Research

- Planning & Managing Opportunities
- Managing Research Funding
- Delivering Research
- Training Researchers
- Publishing Research
- Research Impact
- Improving Research
- Administering Research

Enabling Capabilities

- Managing Facilities & Property
- Managing ICT
- Providing Legal Services
- Government, Public & Stakeholder Relationships
- Managing Finance
- Managing People
- Managing Information
- Providing Supporting Services
- Managing Library Services
- Managing Accommodation
- Managing Promotions