Critical Incident & Business Continuity Policy

Version	v1.1
Author	University Secretary
Approving Body	UEB, endorsed by Audit Committee
Approval Date	19th September 2024
Review Date	3 years after approval
Accessibility Checked	
Equality Impact Assessment	N/A

Contents

1. Policy Statement

1.1 The University of Worcester is committed to the development and implementation of critical incident and business continuity plans and processes, appropriate to the scale, nature, complexity and geography of the University, and the relevant environments in which it operates. We believe that the way in which we plan, prepare, respond to, and learn from, incidents is key to our overall effective recovery. Business Continuity Management plays a critical part in the University's overall control environment.

1.2 Aims & Objectives

Critical Incident and Business Continuity Management (BCM) is concerned with improving the resilience of the University. This means developing the University's ability to detect, prevent, minimise, and where necessary, deal with the impact of disruptive events or critical incidents. In the aftermath of an incident, business continuity enables the urgent and priority activities of the University to continue. In the longer term it will help the University to recover and return to "business as usual" as soon as possible while diminishing possible disruption.

1.3 The Critical Incident and Business Continuity Management Framework has the following key objectives:

- To raise the profile of BCM within the University. This will include arrangements to make staff aware of plans, their roles in them and ensure they are trained appropriately.
- To identify urgent or priority (time critical) activities across the University and develop suitable business continuity arrangements for them.
- To establish defined structure to plan for and respond to incidents.
- To have on-going BCM arrangements at all levels and in all areas of the University that are subject to regular review, audits, and exercises.
- To develop and review the Framework for continuous improvement, with reference to best practice across the sector.
- To embed Business Continuity into the culture of the University so it becomes an integral part of decision making at all levels.

2. Scope

2.1 The scope of the Critical Incident & Business Continuity Management (BCM) Framework will operate across the University, covering all academic departments, professional services, subsidiary companies, and research units. The IT Department will remain responsible for specific IT Disaster Recovery arrangements relating cybersecurity and to the recovery of IT servers/applications and corporate systems.

2.2 The University works with a number of partner institutions and organisations to deliver its services and a risk-based approach will be adopted in terms of the University's expectations on these organisations, focusing on those for which the University has primary responsibility for the building and would be considered the greatest risk.

2.3 The BCM Framework is focussed on protecting and recovering the priority activities of the University. This means being able to deliver its teaching, research, supporting the student experience, and meeting its financial obligations. A priority activity is identified based on how quickly it needs to be resumed and the impact if it is not available – on the safety of people, on the reputation of the University, its finances, and community.

2.4 The University has defined three types of critical incident and business continuity situation, please also see the Decision Tree (Appendix 1) :

2.4.1 Critical Incidents require the implementation of the University's Critical Incident Plan, when they meet the plan's criteria for causing serious harm to staff, students, the University community, property, or its reputation. These situations may include, but are not limited to:

- Cyber security attack
- Fire
- Terrorist attack
- Significant property damage from flooding or other weather event
- Critical field trip incident or similar
- Mass casualty event either on campus or directly involving University community

The Critical Incident Plan is focused on the incident management phase and covers larger scale events posing immediate risk to individuals or property e.g. a national emergency, a power cut affecting the whole campus, etc. Under the Critical Incident Plan the University's response is lead by the Gold Team, supported in the first instance by Immediate Response Teams for example IT, Communications and Estates and Facilities as the event dictates. After the initial response the Gold Team establish the Silver Team to deliver the longer-term response. The Immediate Response Teams will be stood down or subsumed into the Silver Team.

If you believe there is a Critical Incident happening, you should call one of the following numbers:

IT Service Desk for potential Cyber Security/IT related matters during normal working hours	01905 857500
Security for all other Critical Incidents and IT outside of normal working hours	01905 855000

UEB, with advice from the University Secretary, will decide if the situation is a 'reportable event' to the Office for Students (OfS).

2.4.2 Major Business Continuity Situations require escalation to the Vice Chancellor and University Executive Board (UEB). These situations are likely to involve the management of a range of significant situations which would not be identified as Critical Incidents (2.4.1) but do need to be managed and overseen at the highest level. These situations maybe identified as Major Business Continuity Situations due to their impact on:

- a significant cohort of students and/or staff;
- the academic provision of a course or school;
- wider student experience;
- day to day management of the University;
- financial sustainability and/or
- reputation of the University.

These situations may include, but are not limited to:

- Epidemic or pandemic
- Notification of inspection by a regulator as a result of matters of concern having been raised with them
- Notification of legal action being taken against the University
- Accumulation of a number of smaller concerns/issues in one particular area leading to the development of a larger cause for concern
- Infrastructure problems including cyber-infrastructure affecting more than one area of the University
- Supply chain significant delays or failure affecting more than one area of the University or with a large impact to a key service, including potential major IT/Cyber issues affecting suppliers

The Vice Chancellor and UEB will oversee the management of the situation, ensuring that an appropriate action plan is in place and actioned and sufficient resources allocated. UEB will receive regular reports from the designated officer(s) managing the situation and ensure that an appropriate audit trail and record is maintained. UEB, with advice from the University Secretary, will decide if the situation is a 'reportable event' to the OfS.

If you believe that a Major Business Continuity Situation has arisen please advise your Head of School or Professional Department who will escalate the matter to their line manager on UEB. They will consult with the Vice Chancellor, and relevant colleagues on UEB, to decide if a Major Business Continuity Plan needs to be implemented.

Please also advise the University Secretary or Business Continuity Officer (businesscontinuity@worc.ac.uk)

2.4.3 Minor business continuity situations are interruptions/disruptions that are often localised but are sufficiently disruptive to require the implementation of business continuity arrangements. They can often be addressed by a departmental response including using local business continuity plans. They are smaller scale events, affecting one or a small number of academic schools (or departments within) or professional departments. These situations may include but are not limited to:

- a localised computer virus
- a minor power cut for a short period
- adverse weather impacting travel
- significant staff absence
- supply chain delays to one area of the University

- noticeable drop in staff/student recruitment or retainment in a specific area

If the incident relates to an IT matter please contact IT Service Desk – 01905 857500 (select 1 for cyber incidents).

If you believe that a Minor Business Continuity Situation has arisen or is emerging, please advise your line manager and/or Head of School or Professional Service.

Please note that the Business Continuity Officer (businesscontinuity@worc.ac.uk*)* should be made aware as sometimes minor incidents can become major incidents.

2.4.4 Please refer to the Business Continuity Decision Tree (Appendix 1) to assist in identifying the type of situation you are managing and how to escalate it appropriately.

3. Roles and Responsibilities

3.1 Structure

The overall ownership and accountability for Critical Incident and Business Continuity Management rests with the Vice Chancellor and the University Executive Board (UEB). The Vice Chancellor is accountable to the Board of Governors for the "organisation, direction and management of the University and leadership of the staff" (Articles 4.1.2)

Business continuity roles are separated into **Planning** (i.e. pre-situation) roles and **Response** (during situation) roles. The organisational structure for Critical Incident and Business Continuity operates at the Strategic, Tactical and Operational Levels.

In the event of a Critical Incident the management of that incident is in accordance with the Critical Incident Plan, recovery from the Critical Incident is managed by the Gold level group identified in this Policy.

3.2 Planning Responsibilities

3.2.1 Audit Committee

The Audit Committee, on behalf of the Board of Governors, has a responsibility for ensuring that satisfactory arrangements are in place to ensure material adverse events, or reportable events, are managed appropriately.

3.2.2 Vice Chancellor and University Executive Board

As the senior decision-making group the UEB is responsible for:

- Oversight of the Critical Incident & Business Continuity Management Framework, including the regular testing of the Critical Incident Plan.
- Oversight of the Critical Incident & Business Continuity Management Policy.

- Oversight of post-incident/situation reviews, ensuring that lessons learnt during the incident/situation are taken forward appropriately and processes/systems improved.

3.2.3 University Secretary (Critical Incident & Business Continuity Lead)

The University Secretary is the lead for Critical Incident & Business Continuity across the University. This involves:

- Ensuring that the profile of business continuity is raised at a strategic level.
- Ensuring that the Critical Incident & Business Continuity Management Policy is kept up to date and communicated to the University community.
- Ensuring that the Critical Incident Plan and Business Continuity Management Framework are tested on a regular basis, areas for improvement identified and addressed
- Ensuring that post incident/situation reviews are undertaken by UEB (see Section 4).
- Reporting on the Critical Incident & Business Continuity Management Framework and the state of readiness to UEB.
- Ensuring that any business continuity situations which are classed by the OfS as reportable events are reported to the OfS within the required time frame and records kept.
- Line management of the Business Continuity Officer.

3.2.3 Business Continuity Officer (BCO)

The role of Business Continuity Officer (BCO) is undertaken by the University's Risk Management & Business Continuity Officer. They are responsible for co-ordinating the Critical Incident & Business Continuity Management Framework. This involves:

- Raising the profile of Business Continuity across the University and ensuring that information is available to staff, with the aim of embedding BCM into the activities of the University.
- Providing advice and assistance throughout the BCM process.
- Developing appropriate templates for the University to detail its arrangements, ensuring consistency in the Framework with flexibility to recognise the differences across schools and professional departments.
- Supporting academic schools and professional departments in developing plans for specific provision when necessary
- Assisting in the development of overarching arrangements to support academic schools and professional departmental plans.
- Ensuring that the University's arrangements are regularly reviewed and tested.
- Monitoring the level of Critical Incident & Business Continuity planning in the institution and reporting to the University Secretary, and in turn UEB, on this.
- Reviewing the BCM Framework to ensure it remains fit for purpose and to continuously improve the arrangements in place.
- Ensuring that all BCM arrangements work in tandem with the risk management framework.

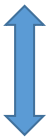
3.2.4 Staff

It is important that everyone at the University is aware of the Critical Incident & Business Continuity Management Framework. Staff should be aware of any arrangements in their department's critical incident and business continuity plans including how they will be contacted/notified of an incident, whether or not they will be expected to work remotely, and where to access key information and updates.

3.3. Response Responsibilities

In the event of an incident where a business continuity response is required the following will apply:

RESPONSE ORGANISATION (Post-Incident if the incident is classed as a Critical Incident)

GOLD LEVEL Vice Chancellor & UEB		**Role: Strategic** - Consider wider issues - Give direction - High level liaison - Media facing - Communication and updates staff and students - Assign priority to restoring core critical functions in alignment with University Strategy
SILVER LEVEL Specific Group(s) identified by Vice Chancellor & UEB to lead on day to day management Membership of the group(s) will be agreed by UEB dependent upon the nature of the incident e.g. health & safety issue, cyber security attack, academic matters		**Role: Tactical** - Report to UEB - Assess impact - Co-ordinate recovery - Handle logistics
BRONZE LEVEL Heads and Deputy Heads of Schools and Professional Services		**Role: Operational** - Focus on core activities - Handle work in progress - Liaise with key clients - Ensure staff and students within their remit understand the information being provided by the University - Raise specific issues to the Silver level group(s)

3.3.1 In the event of the University responding to a critical incident or some major business continuity situations the Board of Governors will convene its Board Business Continuity Group to provide a forum for accountability to the Vice Chancellor and UEB.

4. Post incident review

4.1 If there is a formalised response to a critical incident or business continuity situation at the University then a post-disruption review will be undertaken by the Gold Team, with input from the Silver level group(s) and supported by the Business Continuity Officer, to ensure all lessons learnt from managing the business continuity situation are captured.

Commented [HJ1]: But it might be the wider UEB?

4.2 The Business Continuity Officer is responsible for documenting post incident reviews and working with the University Secretary to implement any identified improvements, reporting to UEB accordingly.

5. Link to other Areas

5.1 Risk Management

Business Continuity Management and Risk Management work closely together, as both are concerned with good governance and raising awareness about risks. However, the focus of the two areas is different; Business Continuity Management is only concerned with managing those threats or vulnerabilities that could cause a disruption to the University's operations, whereas Risk Management has a wider remit. The Risk Management and Business Continuity Officer works across both areas to ensure all risks and threats are identified and responded to accordingly.

Business Continuity Management may be used as a treatment of some risks identified in risk registers and is noted on the University's Strategic Risk Register. When developing business continuity arrangements, priority should be given to treating threats or vulnerabilities identified as most likely and having the greatest impact.

5.2 Internal Audit

As part of the review and monitoring of the Framework Internal Audit has an important role in ensuring that the Business Continuity Management Framework achieves its objectives as set out in this document.

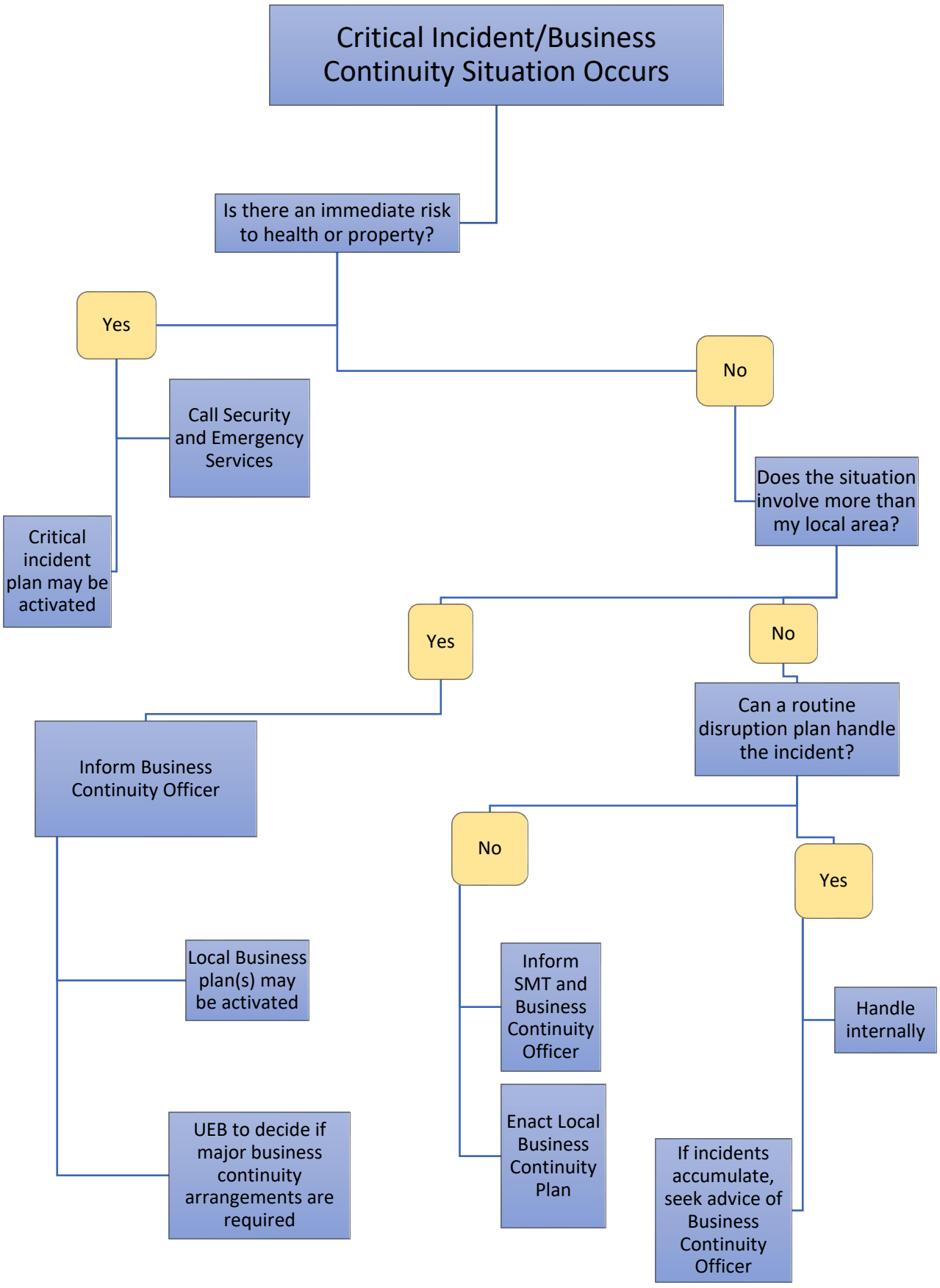
5.3 Information Security

Information security covers the protection of all forms of information and is concerned with ensuring its confidentiality, availability, and integrity. A key part of the Business Continuity process focusses on protecting against a potential loss of resources, including essential information, thereby ensuring it is stored appropriately and remains available after a disruption.

Information Security should be considered when developing alternative arrangements to store/access key information. The loss of university information – either by a loss of access to it or by someone else being able to access it – could have serious implications and dependent on the severity, would be classed as an incident at departmental level and also potentially for the University.

5.4 IT Disaster Recovery

IT Disaster Recovery is a subset of Business Continuity Management and is the ability of the IT elements of an organisation to support its critical business functions to an acceptable level within a predetermined period of time following a disruption. The University's IT Services department has established an IT Service Continuity Management policy that provides a framework for setting Disaster Recovery objectives. The IT Disaster Recovery plan identifies key IT services/systems that would be recovered when a disruption occurs and the operational procedures to enable this recovery.


Critical Incident/Business Continuity Situation Occurs
Is there an immediate risk to health or property?
Yes
No
Call Security and Emergency Services
Critical incident plan may be activated
Does the situation involve more than my local area?
Yes
No
Inform Business Continuity Officer
Can a routine disruption plan handle the incident?
Local Business plan(s) may be activated
UEB to decide if major business continuity arrangements are required
No
Yes
Inform SMT and Business Continuity Officer
Enact Local Business Continuity Plan
Handle internally
If incidents accumulate, seek advice of Business Continuity Officer