 **Continuity Planning &**

**Department Impact Analysis Toolkit**

**1. Developing BCM Plans**

Many organisations start by developing continuity plans against perceived risks such as loss of IT or a building. This is the traditional disaster recovery approach, and will probably suffice to identify the most obvious risks. However a problem with this approach is that it might overlook critical activities outside of the facilities and services of the department and not meet their actual needs.

The modern Business Continuity Management (BCM) approach is based on ensuring the continuity of critical activities and processes that deliver key research/teaching /services to partners, students and other stakeholders. It aligns with total quality management, which is based on supplier / customer relationships and the processes that serve them.

All departments operate processes with inputs and outputs. All have stakeholders for whom they conduct research, provide teaching or services or interact with in other ways.

**2. Stakeholder Identification**

To begin with departments should identify all their stakeholders. This enables them to consider continuity solutions against stakeholder requirements and perceptions. Some stakeholders are obvious; students, staff, industry partners, suppliers, etc. Additional stakeholders include regulators, funding bodies, insurance companies, professional bodies etc. Some are less obvious; competitor institutions, the community, the environment in which the University operates, the media and protest groups. The last two can have a great influence on the public’s perception of the University.

A technique used to identify stakeholders and their expectations, both under normal and disrupted conditions, is to use a group of senior staff within the department and get them to list the stakeholders and their expectations and then rank them in order of importance for the department.

**3. Departmental Impact Analysis (DIA)**

The next stage is to define the critical activities that enable the department to deliver its services, teaching, research etc. It is essential to identify the key services that, if disrupted for any reason, would have the greatest impact on the department and its stakeholders. It is these services on which BCM must be focussed initially. Once plans have been successfully established to deal with the key services the programme can be extended to other areas of the department at a later date.

In analysing the way services are delivered, an approach must be taken that breaks with the traditional functional view of an organisation. This approach requires an “end to end” view of the department and its activities.

Consideration must be given to any third party’s (suppliers, contractors etc.) role in these activities. (See fig. below)

Input

Customer/Client e.g. Students/ Partnerships

Intermediary

Department Activities

Output

Outsourcer

Supplier

Stakeholders of the department will expect the department to deliver the service regardless of the ability of third parties to maintain their continuity of operations.

The Value Chain Analysis Model (Porter 1998) can provide a useful methodology to assist in the understanding of how a department works. The activities are broken down to determine where value is added. This provides a starting point in understanding how the department works. It is often common for managers to assume that they know exactly how an organisation works, but use of this technique can ensure that nothing is overlooked.

**4. Impact versus Risk**

Traditional risk management would now consider the threats/risks that could disrupt the critical activities and what could be done to prevent them happening.

Business Continuity Management on the other hand, uses an approach based on **impact** and **time**. It looks at the impact on the department if critical activities are interrupted; it is concerned with the effects rather than the causes. The department must consider what the impact would be on itself and its stakeholders if the delivery of key services and their supporting critical activities were disrupted for any reason. This process is known as a ‘Department Impact Analysis’ .

Measures of impact could be:

* Financial loss
* Data loss
* The effect on teaching delivery, examinations or graduation
* Embarrassment or loss of reputation
* Failure to meet statutory or regulatory obligations
* Effect on project/research objectives and schedules

The measures must also take into consideration time: how soon will the impact of the disruption to key services impinge on the department? How long before the department is seriously affected by the disruption? This is referred to as the **Maximum Tolerable Period of Disruption (MTPD),** and is defined as “the duration after which the department’s viability will be irrevocably threatened if service delivery cannot be resumed”. It should be noted that this may be driven by factors external to the department. For example, a department may want an IT failure resolved within two hours. However a catastrophic failure of the IT system my take a full week to completely resolve. Departments must plan their own resilience measures based on the reality of realistic recovery times.

Additionally some services and their supporting activities are more critical at certain times of the year e.g. student enrolment, graduations, key reporting dates, payroll processing, etc. Also there may be key events that have to be delivered on time and, if disrupted, will have serious consequences for the department. As emergency incidents cannot be predicted, it is advisable that departments chart these activities/events against a calendar and take this worst case scenario into account when planning continuity actions.

Consideration must also be given to disruptions that could occur outside the university e.g. UK Fuel shortages are external events for most organisations but the impact is felt internally.

The best approach to Department Impact Analysis is to use the department management team, to consider the department as a whole and to provide a ranking for key services and the point at which MTPD occurs. This team also need to set the timescales for service resumption within the MTPD. This is known as the **Recovery Time Objective (RTO)** and specifies the minimum levels at which key services must be resumed and the point in time by when full resumption must be achieved. E.g. 20% within half a day, 50 % within 1 day 100% within a week.

The output is then used to determine the critical activities and resources required across the department that are needed to deliver these services at the agreed levels. This approach provides the quickest route to establishing the first round of BCM implementation.

**5. Process Mapping**

Once the department’s management team have identified their **key services**, the next stage is to identify the **critical activities** that support these services. Work processes, some formal some informal, that have been established over time will support these critical activities. They all draw upon the resources of the department and of third parties. The next step is to identify these processes and the resources they use.

Process mapping should be applied to the critical activities. The benefit of using this technique is that it will identify what actually happens in the department in order to deliver the key services. It is dangerous for managers to assume they know how things are done. It is vital that they understand what exactly happens in order to replicate this at the time of any disruption in order to provide a seamless continuity of operations.

Process mapping should start with the high level operations e.g. Estates Services have to deal with complaints from departments regarding infrastructure. The high level mapping for this process could look something like:

Department Informed of Outcome

Department Calls Helpdesk

Helpdesk Log Complaint Details

Investigation

Resolution

The next level down is then mapped, for example:

Fault Forwarded To Trades Staff

Department Advised Of Reference Number etc.

Details of Fault Entered

New Fault Form Opened In Database

There may be further levels of processes below these that also need to be recorded. Staff who operate the processes should be involved in helping to map the way they work and the resources they use. As people work in different ways and informal processes develop over time it is useful to work with several people who are involved in operating the same process in order to ensure that all key information is captured.

The process mapping exercise gives an opportunity for those delivering the service to highlight areas where they experience difficulties. Input at this level can identify continuity solutions that already exist but which may not be documented along with areas where the department can be made more resilient by reducing vulnerabilities.

**5.1 A Process Mapping Tool**

A simple form of process mapping is based on the use of adhesive notes.

* The person who operates the process is interviewed about the job they do.
* The interviewer writes each stage of the process on a separate adhesive note, which is then attached to a flip chart. The use of adhesive notes allows missed steps to be added without having to redraw the diagram. Often those being interviewed will miss out steps as they assume the interviewer knows what happens next.
* The next stage is to use different coloured adhesive notes to chart resources used against steps in the process. The key resources used to support processes may be people, IT resources, facilities and suppliers. The numbers, location, skills, roles and responsibilities of the people required should also be noted. The systems that support them must be logged e.g. computer hardware, software, communications and information (data). It should be noted what facilities in terms of premises, plant, machinery and materials are required. Very often third parties have a major role to play in critical activities as suppliers of goods and services, as outsourcers or as intermediaries between the university and its stakeholders. Their part in the process must also be recorded.

It is recommended that a separate line and colour of adhesive note is used for information and resources. (See below) When the mapping exercise is complete the output should be permanently recorded.

 Process Information Resource

 Input

 Simple Process Mapping

When mapping has been completed for all processes that support the critical activities necessary for delivery of key services, it is now possible to identify all the resources that are required to support these activities.

The inputs and outputs are recorded together with the timescales and the resources used to complete the task.

**6. Threats and Risk Assessment**

It is now possible to undertake risk assessments against the resources identified from the process mapping. Traditional risk assessment techniques are used, (See Safety Services Principles & Practice Of Risk Assessment Training Course for further detail if required) and using the process mapping data it is easy to identify which processes and which activities will be affected by a single point of failure e.g. loss of a key member of staff, building or supplier. Internal and external threats, liabilities and exposures are identified, together with the likelihood of the threat occurring.

Best practice guidance recommends that threats to service delivery from five key scenarios are considered:

* Denial of access to the premises
* Shortage of staff
* Failure of technology services.
* Failure of key suppliers or partners.
* Failure of utility services

The results must be recorded. A department risk register exists within the University as part of the University Risk Management Framework. The BCM risks identified should be incorporated into this register.

The results of the Department Impact Analysis and risk analysis are now used to create a risk matrix for the critical activities as shown below:

**LIKELIHOOD**

Rare

Highly Probable

**IMPACT**

Insignificant

Very Significant

Manage

Contain

Prevent

Reduce

Accept

Plan

The department management team should agree the assignment of risk to the critical activities. They should also understand the level of risk they are prepared to accept: their risk appetite. This will determine the level of resilience required and the amount of delay that is acceptable before continuity of operations is achieved.

**6.1 Risk Treatments**

From the risk assessment matrix, it can be seen that there are a number of options that can be applied to the critical activities: **accept, manage or contain, prevent** **or reduce**, or **plan**. An appropriate risk treatment may be to implement one or a combination of these:

Accept

Where the impact is insignificant and the likelihood of failure is rare, the management team may decide to accept the risk and do nothing. This option will be driven by the risk appetite of the department.

Mitigate

Where the risk level is high but the impact on the critical activity is low the best option is to mitigate the risk, i.e. manage or contain the risk. E.g. if the risk of power failure is high then the provision of a standby generator or uninterrupted power supply will minimise the impact on critical activities.

Prevent or Reduce

Where the likelihood of failure is very high and the impact would be considerable on the department, urgent action will be needed. If it is not possible to reduce the risk then a decision may be needed to cease the activity. This may not be possible if it is a statutory requirement. In such circumstances alternative strategies are to change or re-engineer the processes that support the activities.

Plan for Continuity.

Where the risk of failure is low, but the impact would be high it is essential that departments develop continuity and incident management plans that would deal with such a situation if it should arise.

The outcome of the risk assessments should be a set of risk treatments that are designed to reduce the likelihood of disruption, shorten the period of disruption if it should happen and limit the impact of any disruption on the department’s key services.

Both Department Impact Analysis and Risk Assessment documents must be reviewed at planned intervals and when significant changes occur to the department or the environment in which it operates.

 **7. Department Impact Analysis & Risk Assessment Process Summary**

Identify Department Stakeholders

Yes

No

Update department Risk register to capture the outcome of the DIA process

Record DIA & Risk Assessment Information and keep under appropriate periodic review

Develop and rehearse plans for process continuity

Implement appropriate management strategy to control risk

Plan for continuity

Cease activity or re-engineer process to reduce risk.

Manage or mitigate risk

Accept risk

Evaluate risk and determine appropriate risk treatment

Assess likelihood of the risk occurring

Assess severity if risk occurs

Assess risk controls including confidence therein relative to threats

Define (map) the process and conduct hazard analysis

Does the RTO reflect any process seasonality?

How long can department cope without the service (RTO)

Define Maximum Tolerable Period of Disruption for tasks or services.

Define critical tasks or services to be analysed

**8. Developing a Business Continuity Strategy**

When developing a strategy for maintaining service delivery during emergency incidents, the following points could be considered, collated for all critical activities and used in the preparation of appropriate continuity plans.

**8.1 People**

Key Staff:

* Can staff be contacted out of hours? Key department management staff should be aware of each other’s contact details.
* Could extra capacity be built into your staffing to assist you in coping during an incident?
* All key staff should be aware of the business continuity arrangements for their Department/University; the critical activities and be familiar with the proposed action.
* In the absence of the Head of Department, a deputy should always be identified.
* Ensure all deputies (teaching, research, management) are prepared for their roles.
* Key roles in the department (e.g. Academic Co-ordinator, Academic selector) could have additional members of staff appointed as “shadows” in the event of illness.

Skills/Expertise/Training:

* Could staff be trained in other roles?
* Could other members of staff undertake non-specialist roles in the event of an incident?

Minimum Staffing Levels:

* What is the minimum staffing level required to continue to deliver your critical activities at an acceptable level?
* What measures could be taken to minimise the impact of staff shortfalls? (Cut back on non-essential work, temporarily increase working hours).

**8.2 Premises**

Buildings

* Could you operate from more than one building/location?
* Could you relocate operations in the event of a premise being lost or if access to the premise was denied?
* Could staff work from home?

Facilities

* Are any of your facilities multipurpose?
* Are alternative facilities available in the event of an incident?

Equipment/Resources

* Is there an asset register or other central record of all equipment required?
* Could alternative equipment/resources be acquired in the event of an incident/disruption?
* Is equipment “off the shelf” or specialised and if so what is the lead-times on critical equipment?

**8.3 Processes**

IT

* Is data backed up and are back-ups kept off site?
* Do you have any disaster recovery arrangements in place?
* What IT equipment is required?

Documentation:

* Is essential documentation stored securely (e.g. fire proof safe, backed –up)?
* Do you keep copies of essential documentation elsewhere?

Communications:

* Are your systems flexible?
* Do you have alternative systems in place (manual processes)?
* What alternative means of communication exist?
* Department administrators should ensure they have contact details for all staff and students.
* Department administrators should keep staff & students informed of any operational changes necessitated.
* Global email addresses should be available to all key staff to enable them to alert students and staff.
* Voice mail messages and out of office email notifications used to provide contact details for urgent business to be taken care of.

**8.4 Providers**

Reciprocal Arrangements:

* Do you have agreements with other organisations regarding staffing, use of facilities, etc., in the event of an incident?

Contractors/External Providers:

* Do you know of alternative contractors or are you reliant on a single contractor?
* Do your contractors have contingency plans in place?
* Could contractors be contacted in the event of an incident?

Suppliers:

* Are you reliant on a single supplier?
* Do you know of suitable alternative suppliers?
* Could key suppliers be contacted in an emergency?

**8.5 Profile (Brand)**

Reputation:

* How could reputational damage to your department be reduced?
* How could you provide information to staff and stakeholders in an emergency?
* Legal Considerations:
* Do you have systems to log decisions, actions and costs, in the event of an incident?

Vulnerable Groups:

* How could vulnerable groups be contacted /accommodated in the event of an incident?

**8.6 Teaching**

* Directors of teaching could review the impact on course delivery and seek timetable alterations or where possible alternate teaching staff or methods.
* Directors of teaching could in extreme cases prepare to extend the teaching period and delay exams.
* Academic staff could be required to review and modify assessment requirements, rationalise assignments/continuous assessment.

**9. Recommended Elements of Business Continuity Plans**

The following are the recommended elements of business continuity plans:

**9.1 Purpose & Scope**: these should be identified.

**9.2 Roles & responsibilities**: the plan should identify the roles and responsibilities of staff who will be involved in delivering the plan. It will identify the team leader, key team members and their deputies required at the time of invocation. It will set out their levels of authority and to whom they must report their actions. The plan will also set out the point at which the responsibility for incident management must pass to a higher level.

**9.3 Invoking the plan**: the plan must indicate the circumstances under which it is to be invoked and who can authorise its invocation. It must also include details of how to manage a disruption and its impact on the department. It is important that any invocation is flagged to senior management so that they are aware that an incident exists and can consider its wider implications for the University. Instructions to that affect should be written into the plan.

**9.4 Call out lists**: should be included along with details of where the team should meet to manage the disruption along with a suitable backup. These areas should be equipped with the appropriate level of communications and other facilities to allow the incident to be managed.

**9.5 Contact details**: the plan should include full details for key internal and external contacts. These could include:-

* Key senior management
* Key operational staff
* Regulators and other compliance bodies.
* Suppliers
* Key partners
* It may be appropriate to include details of contracts, insurance policies, regulatory requirements etc. These documents may be stored separately to the plans but should be readily accessible.

**9.6 Priorities**: details of the priority order for continuity and recovery of key services and their critical activities must be available together with their Recovery Time Objectives and recovery levels.

**9.7 Vital documents and resources**: a list of vital documents and resources needed for continuity and recovery for each critical activity must be included along with details of where these are located. Vital documents may include records of who is authorised to retrieve materials as well as security arrangements, e.g. passwords that will be required. Vital materials may include stationary, spare parts, specialist machinery and tools etc.

**9.8 Checklists**: and audit trails: a simple checklist or action card may be included to ensure the team completes mandatory tasks and provides a tracking process for task completion. Meeting agendas can be included so that all key elements of the plan are covered when the team meets.

**9.9 Incident log**: with any emergency there is a requirement for post incident review and audit. Consequently it is of vital importance that a record is maintained of what actions were taken, why they were taken, when they were taken and by whom. This is best done by maintaining and incident log.

**9:10 People issues**: special consideration should be given to the needs of staff, contractors and visitors who may have been evacuated from the premises without time to collect their personal belongings e.g. money, credit cards, keys etc.

**9.11 Salvage**: if the incident results in damage to buildings e.g. fire, it is important that arrangement is made to recover important documents and equipment, when safe to do so. Documents and equipment that are damaged by water or other contaminants will need to be cleaned and restored by specialist contractors. This would be coordinated centrally, however as time is of the essence it will assist recovery if departments develop their own mechanisms to identify items requiring salvage, e.g. equipment lists or asset registers.