Emergency Planning and Business Continuity

Paul Mac Court

What is ER/BC about?

2. Emergency/Incident response

3. Business Continuity Management

4. Business Recovery Management

Incident
Critical disruption to essential services

1. ER/BC Preparation

Time to restore business as usual

The ability to respond to and recover from a business critical incident

ER/BC Preparation
Emergency Response

- What are our risks and vulnerabilities
- What are the internal and external threats to the safety of people and the preservation of the estate
- How can we reduce the risk of disruption
  - Reduce our vulnerabilities
  - Improve our resilience
- How will we respond to the emergencies that could occur
  - what are the priorities?
  - What resources will we need?
  - How do we manage decisions?

Examples of Critical Incidents

- Fire/flood/explosion causing the loss of use of facilities or equipment
- An outbreak of a communicable disease on the campus
- It systems failure causing data loss or loss of use
- Failure of a critical supplier
- The sudden loss of a critical member of faculty
- Failure of a critical piece of equipment
- Civil unrest/breach of security
- Failure to maintain a permit/license

ER/BC Preparation
Business Continuity

- What are our core business functions
- What are our essential needs to achieve our core objectives
  - People (staff, students, contractors, consultants)
  - Facilities (Land, buildings, rooms,)
  - Equipment (routine, specialist, unique)
  - Processes (communications, administration, procurement)
  - Supplies (utilities, fuel, stock, consumables, spares)
- How would we cope if one or more of the above were disrupted – and for how long
- Those that jeopardise our core objectives are our critical dependencies

ER/BC Preparation
Business Continuity

- What vulnerabilities did we identify at the emergency response planning stage and how could we ensure they do not stop us achieving our core objectives?

- What plans (contingencies) can we put in place to achieve our objectives if we experience disuption to one or more of our critical dependencies – either short-term or long term?

- How do we ensure our plans are effective and fit-for-purpose?

Identifying hazards and vulnerabilities/single points of failure

Hazard	✘✔
Hazardous chemical substances	
Hazardous biological substances	
Flammable or explosive substances	
Sealed/unsealed radioactive sources	
X-ray equipment	
High energy electrical equipment	
Compressed gas cylinders	
Pressure vessels	
Lasers	
Electromagnetic radiation equipment	
Lifting equipment	
Vehicles	

Identifying hazards and vulnerabilities/single points of failure

Vulnerability	✗✓
Children	
Patients	
People with disabilities/impairments	
Visitors (including visiting workers)	
Animals	
Rare or unique artefacts or collections	
Irreplaceable research samples	
High dependency on utilities	
High dependency on contractors/suppliers	
Staff/students working off Campus	
Highly specialised equipment	
Highly specialised staff	

Prevent and protect

Issue	Detail and preventative/protective measures in place	Frequency of checks/updates
Measures in place to prevent an emergency, eg.		
Housekeeping standards		
Security systems		
Maintenance needs		
Specific hazard controls		
Contingency arrangements		
Emergency equipment		
Emergency procedures		
Training		
Staff list		
Contact details		
Succession planning		

Emergency Response Planning
School Responsibilities

- Become familiar with emergency response and business continuity policy

- Appoint a ERP coordinator

- Identify local incident management team and develop call out procedures

- Identify partners/stakeholders and key suppliers

- Use emergency planning and response guidance to develop an ERP

Business Continuity & Business Recovery
School Responsibilities

- Become familiar with the emergency response and business continuity policy

- Appoint a BCRP coordinator

- Identify a BC/BR team (same as ER team?)

- Use the business continuity planning guidance to develop BCRP

Business Continuity & Business Recovery

- Identify core functions and the impact of their interruption or loss (ensure you have captured your vulnerabilities / Single Point Failure)
- Identify risk of interruption and contingencies
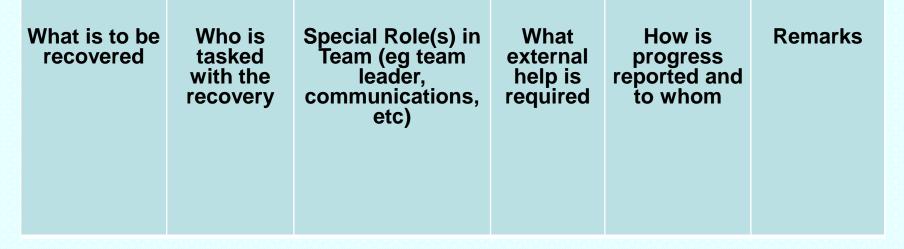- Develop recovery plans

Business Impact Analysis

- Consider critical dependencies – what is the impact of disruption for:
  - Up to 1 day
  - Up to one week
  - Up to one month
  - More than one month
- What is the maximum tolerable period of disruption

Risks and Contingencies

- For each core activity, evaluate the risk level for disruption to each essential need (L/M/H)
- Identify risk reduction contingencies
- Identify any limitations/critical dependencies
- Determine the essential recovery time

Recovery – returning to BAU

What is to be recovered	Who is tasked with the recovery	Special Role(s) in Team (eg team leader, communications, etc)	What external help is required	How is progress reported and to whom	Remarks

Once the cause of the emergency or business interruption is resolved and the contingencies identified as necessary to allow the University to provide essential services are in place, the Recovery Phase of the Business Continuity Plan should be invoked.

The University's ITS recovery plan is attached to the University Emergency Response and Business Continuity Plan.
Local arrangements for IT recovery should be documented as part of this recovery plan.

Recovery Resources

Personnel / Company	Equipment / Services	Contacts	Remarks

Resources (external and internal) for recovering the Essential Services and Core Functions should be identified.

This information can be derived from the Critical Dependencies listed in the Business Impact Analysis.

Learn the Lessons

Was the cause of the incident within or outside your control?

Was recovery achieved within the essential recovery time?

Did your plan contain all the essential elements and information necessary to deal with the incident from emergency response through to recovery of BAU

Did you have access to all the people and resources that were needed for successful and efficient management of the incident

Were there any unidentified critical dependencies that did or could have easily jeopardised the success of your plan

How will you communicate any lessons learned and use them to improve your plan for the future.