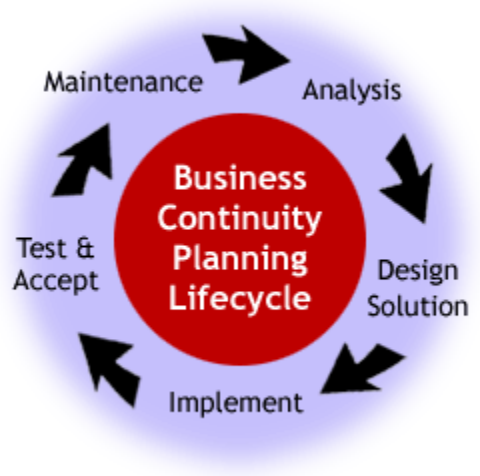
BUSINESS CONTINUITY PLAN GUIDELINES AND TEMPLATES



If you need assistance in filling out any of this plan
Please contact Randy Jones at ext. 23868.

Introduction

The University of Texas Medical Branch and its employees have faced many disasters – from the 1900 Storm, the Texas City Disaster of 1947 to hurricanes Carla in 1961, Alicia in 1983, and lastly hurricane Ike in 2008. In order to maintain our status as one of the leading health care institutions in the nation, we must continue to be prepared for these and other potential disasters.

The onset of homeland terrorism in the United States, coupled with the Gulf Coast's vulnerability for natural disasters make it essential for UTMB to ensure that plans are in place, tested true, and viable, should we find ourselves in a threatening situation – be it man-made or natural.

Therefore, in response to these challenges and in alignment with the Homeland Security Act, the Texas State Infrastructure Protection Committee, and State of Texas Department of Information Resources (DIR), Information Services at UTMB has been asked to develop a model Business Continuity Plan to assist you in developing and testing work plans for your own areas. Ultimately, your plans should be structured to make it possible to continue to do business and function during and after whatever crisis may arise.

IS will also identify resources and coordinate the process for developing, testing and evaluating these plans. Critical functional areas have been identified to participate in this process and will continue to be addressed on an ongoing basis. This year's plan creation and testing will include Invision, Signature, and EPIC.

Developing a Business Continuity Plan is a multi-dimensional process and includes a number of phases as prescribed by the DIR. These phases include: Project Initiation, Business Impact Analysis, Recovery Strategies, Plan Development, Testing, and Maintenance & Training – all of which will be addressed at UTMB.

It is imperative that each of our leaders support and cooperate in the development of the plans that will keep UTMB operating through the most difficult of times.

If you need assistance in filling out any of this plan
Please contact Randy Jones at ext. 23868.

Executive Summary

An Executive Summary of the Business Continuity Plan will need to be constructed. This will be a brief overview of your plan's recovery strategy. This should be done after you have completed section four (4) of this template.

******* Examples from other Plans***

If you need assistance in filling out any of this plan
Please contact Randy Jones at ext. 23868.

Table of Contents

If you need assistance in filling out any of this plan
Please contact Randy Jones at ext. 23868.

If you need assistance in filling out any of this plan
Please contact Randy Jones at ext. 23868.

1.1 Executive Sponsor

The Executive Sponsor is the Departmental Representative or Group that has the responsibility to make sure that this critical function is delivered to the university. Therefore it is the responsibility of the Executive Sponsor to make sure that a Business Continuity Plan is developed, maintained, and tested.

The Executive Sponsor is responsible for the following:

- Implementing the team,
- Developing a Business Continuity Policy Statement,
- Reviewing Risk Analysis,
- Approving overall plan content,
- Reviewing all testing outcomes; and,
- Reviewing any changes and maintenance to the plan.

Return to Table of Contents

1.2 Team Leader

For a project of this significance and complexity to be successful, a suitably qualified Team Leader will need to be appointed. The Team Leader should possess good leadership qualities, a good understanding of business processes and business management and strong project management skills.

An alternate Team Leader should also be appointed who would be able to take over the functions of the Team Leader if needed.

It will be the responsibility of the Team Leader to make sure the team is progressing in accordance with the Project Plan guidelines, give regular status reports to the Business Continuity Plan (BCP) Sponsor, and obtain approval from the Sponsor as needed.

Return to Table of Contents

1.3 BCP Project Team

The Business Continuity Plan (BCP) Project Team members should be selected; permission obtained for their involvement (if necessary); and formally notified. Each of the main business and operational areas within the organization should be represented on the BCP Project Team.

Representatives from each of the key business areas should have a comprehensive understanding of how their own business area functions, in addition to an overall understanding of the organization as a whole. Each area representative should be able to bring to the BCP Project Team information on how his or her own area functions, its key business activities or support functions, and its key risk areas.

Return to Table of Contents

1.3.1 Select and Notify BCP Project Team

Each of the business and operational areas within the organization are to be represented on the BCP Project Team. The Project Team has overall responsibility for the development and maintenance of the Plan. Members of the BCP Project Team are currently as follows:

BCP PROJECT EXECUTIVE SPONSOR	**JOB TITLE AND DEPARTMENT/DIVISION**	**CONTACT INFORMATION (Location, Phone, Email, Pager, Cell Phone)** **EMERGENCY CONTACT INFORMATION (Home, Pager, Cell Phone)**
Any individual responsibilities within Project Team:		
BCP PROJECT TEAM LEADER	**JOB TITLE AND DEPARTMENT/DIVISION**	**CONTACT INFORMATION (Location, Phone, Email, Pager, Cell Phone)** **EMERGENCY CONTACT INFORMATION (Home, Pager, Cell Phone)**
Any individual responsibilities within Project Team (i.e. Business Function or Process):		
BCP PROJECT <u>ALTERNATE</u> TEAM LEADER	**JOB TITLE AND DEPARTMENT/DIVISION**	**CONTACT INFORMATION (Location, Phone, Email, Pager, Cell Phone)** **EMERGENCY CONTACT INFORMATION (Home, Pager, Cell Phone)**
Any individual responsibilities within Project Team (i.e. Business Function or process):		

BCP PROJECT TEAM MEMBER	JOB TITLE AND DEPARTMENT/DIVISION	CONTACT INFORMATION (Location, Phone, Email, Pager, Cell Phone) EMERGENCY CONTACT INFORMATION (Home, Pager, Cell Phone)
Any individual responsibilities within Project Team:		

BCP PROJECT TEAM MEMBER	JOB TITLE AND DEPARTMENT/DIVISION	CONTACT INFORMATION (Location, Phone, Email, Pager, Cell Phone) EMERGENCY CONTACT INFORMATION (Home, Pager, Cell Phone)
Any individual responsibilities within Project Team:		

Add rows as needed

Return to Table of Contents

1.3.2 Mission Critical Activities

The following is a descriptive list of the organization's mission critical activities and/or critical business processes, together with a brief description of the business process and main dependencies.

KEY BUSINESS AREA	BRIEF DESCRIPTION OF BUSINESS PROCESS	MAIN DEPENDENCIES

Return to Table of Contents

1.4 Plan of Approval

Procedure for Approving Business Continuity Plan (BCP) Content

There must be a clear procedure for adoption and approval of the BCP. Updates and changes to the plan should also be included in this process.

The team should select from the following possible approval phases.

- Appointment of BCP Team Members
- Overall Plan Content
- Testing Plan Outcomes
- Changes/Maintenance to Plan

Return to Table of Contents

Approving Business Continuity Plan (BCP Content)

BCP Content	Sent Date	Approved Date	Comments

Return to Table of Contents

1.5 Project Plan

Task Name	Duration	Start	Finish	% Complete
Patient Care Delivery Process				
Phases				
Begin – Project Initiation/Risk Analysis	2 wks			
Business Interruption Recovery Plans/Strategies	8 wks			
Approval – Executive Sponsor	1 wks			
Training & Communication	2 wks			
Validation & Testing	2 wks			
Plan Updates & Maintenance	1 wks			
Quarterly Review/Testing/Plan Modifications				

Return to Table of Contents

2.1 Objectives and Deliverables

The objectives for the project need to be clearly defined, together with the deliverables. Concise definition will enable the BCP Project Team to focus its efforts on the most important issues and to ensure the work undertaken is relevant in the context of the original project expectations. The departmental BCP sponsor would normally approve these objectives and deliverables.

Suggested Wording for a Suitable Objective

The project's principle objective could be stated as:

> *"The development and testing of a well structured and coherent plan which will enable the department / or function to recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts normal business operations."*

The department / or function could additionally have a series of sub-objectives which could cover issues such as specialized research and development activities, the need to ensure that all employees fully understand their duties in implementing such a plan, the need to ensure that information security policies are adhered to within all planned activities or the need to ensure that the proposed contingency arrangements are cost effective.

Suggested Wording for a Suitable List of Deliverables

The deliverables, in outline, should consist of:

- Business Risk and Impact Analysis
- Documented activities necessary to prepare the department / or function for possible emergencies (including strategic recovery measures)
- Detailed activities for dealing with the Disaster Recovery Phase
- Procedure for managing the Business Recovery Process
- Plan for testing the Business Recovery Process
- Plan for training the staff in the Business Recovery Process
- Procedure for keeping the Plan updated

****** Examples from other Plans***

Return to Table of Contents

2.1.1 Project Objectives and Deliverables

To enable the BCP Project Team to focus efforts on the key issues, and to ensure the work undertaken is relevant to the requirements of the project, the project's objectives and deliverables must be clearly defined. The Department / Executive Sponsor is responsible for approval of objectives and deliverables.

OBJECTIVES OF BCP PROJECT:

Main objective of BCP Project:
Sub-objectives of the BCP Project:

DELIVERABLES OF BCP PROJECT:

Return to Table of Contents

3.1 Business Impact Analysis

The purpose of the Institutional Business Impact Analysis (BIA) is to assist executive leadership in determining the perceived criticality of discrete UTMB business unit entities.

Ideally the BIA should facilitate the high level identification of:

- Community impacts
- Operational impacts
- Financial impacts
- Regulatory impacts
- Accreditation impacts
- Process interdependencies
- Data sensitivity
- Downtime tolerance
- Recovery complexity
- Technology dependencies

Further, the aggregated results of the Institutional BIA will ultimately define project scope for a subsequent, more rigorous evaluation of associated services and work product. Hence, please complete all questions and provide as much information as possible to ensure key data elements are not missed.

NOTE: See footnote below for examples of the term department

1. Department *(as per FRS four digit Org ID):*

2. Department Alignment (*as per Executive Level Reporting Structure*):
   ( ) Department within Business Unit
   (i.e,. FOAM is a department within Support Services; a business unit within Business Administration)
   ( ) Business Unit within Entity
   (i.e., Support Services is a Business Unit within Business Administration; an entity)

3. Description of Department:
   (What are your department's primary functions and processes? What services does the department provide the University?)

4. Process Output:
   (What primary services, work products or information created/provided is made available by your department? List 5 of the most important.

5. Process Input:
   (What primary services/resources does your department rely on to perform its activities? i.e., Information Technology/software, special equipment information, etc. List up to five.)

6. The loss of these services/resources would have the following cumulative effect on entity function and processes:

   ( ) Significant harm or effect
   (i.e., entity/department could supply some services/resources to the university but in such a diminished capacity that services would be unacceptable)
   ( ) Moderate harm or effect
   (i.e., entity/department could supply services/resources in a diminished but acceptable capacity to the university)
   ( ) Minimal harm or effect
   (i.e., entity/department could supply services/resources to the university in a "somewhat normal" capacity by altering processes or procedures)
   ( ) No harm or effect
   (i.e., entity/department could to supply services/resources in a normal manner to the university)

7. The loss of your department would affect the following breadth of harm: (check all that apply)

( ) Potential endangerment to public health or safety
(i.e., the state, community, or any subset of population served. This would include patient, student, and staff health or safety)

( ) Adversely impact business, or organization, state agency, office, commission, board, university, institution, center, program, or other entity external to UTMB
(i.e., would adversely impact outside entities external to UTMB; i.e., partnerships with other universities, research that supports other businesses, etc)

( ) Adversely impact UTMB only
(i.e., would only impact UTMB's service level or integrity/reputation)

( ) No harm or effect
(i.e., entity/department could supply services/resources in a normal manner to the university)

8. The loss of your department would have the following effect on UTMB missions (select one):

( ) Minor effect on one division or business unit
(the loss of your department would be an inconvenience to one department or business unit of the university.)

( ) Minor effect on the institution, some divisions, or business units
(the loss of your department would be an inconvenience to several divisions or business units of the university)

( ) Moderate effect on some divisions or business units
(the loss of your department would cause some divisions to change procedures and the way their business functions are supplied to the university)

( ) Moderate effect on the institution
(the loss of your department would cause the university to alter the way they supply normal delivery processes)

( ) Catastrophic effect on one division or business unit
(the loss of your department would cause seriously affect one division/business unit's the inability to provide normal services to the university)

( ) Catastrophic effect on the institution, some divisions, or business units
(the loss of your department would significantly impact normal services provided by the university.)

9. Could this function be performed for a period of time at a reduced operating efficiency?
(i.e., degraded performance such as manual versus automated process)

If yes, for how long?

( ) Less than 24 hours
( ) Up to 3 to 5 days
( ) Greater than 5 days
( ) Greater than 2 weeks

Additional comments?

_____
_____
_____
_____

10. How long could your department be **completely idle (i.e., totally lost)** before it experiences or creates a significant adverse impact?

(i.e., "totally lost" cannot perform its functions in any capacity for any reason)

( ) Less than 24 hours
( ) Up to 3 to 5 days
( ) Greater than 5 days
( ) Greater than 2 weeks

Additional comments?

_____
_____
_____
_____
_____

11. How long can the department continue to function without its usual automated information systems either departmental or centralized UTMB systems?
(Assume that loss of these systems occurs during the **busiest, or peak, work period.)**

( ) Less than 24 hours
(Operation of the Department has an extreme reliance on information system and requires immediate disaster recovery plans, which have been tested, for the replacement/access to either internal or centrally supported systems.

( ) Up to 3 to 5 days
(The department has a significant dependence on information systems. A major interruption of service delivery would occur if information systems were unavailable for 3 to 5 days.

( ) Up to 2 weeks
(The Department has a minimal reliance on information systems and, could function in a manual mode for up to two weeks at an acceptable service level.)

( ) More than 2 weeks
(The Department process/procedures are not dependent upon information systems and can be accomplished in a manual mode for an extended period of time until systems become available with no impact to service delivery.)

12. In the event of a significant outage or disruption, when is the severity of impact more significant?

(i.e., if an outage occurs, are some months worse than others? some days? some hours?)

Check all that apply

( ) *some months versus others*
( ) *some days of the week versus others*
( ) *certain times of the day*
( ) *certain times of the year*
(particular week of the month, month/quarter end, fiscal year end, etc.)
( ) *no particular timing of an event is significantly greater than another*

13. From the list of exposures below, please indicate the relative importance of each type to the institution using the rating scale of 0 to 10, for the specific department.

Also using the scale of 0 to 4, indicate the severity of each impact and how it would escalate over time if the department was not able to function.

Exposure type	**Relative Importance Scale 0-10** 0 = no importance 5 = moderate importance 10= extreme importance	**Impact Severity Scale 0 – 4** 0 = no impact 1 = little impact 2 = some impact 3 = significant impact 4 = severe impact			
		Less than 24 hours	**Up to 3 to 5 days**	**Greater than 5 days**	**Greater than 2 weeks**
Loss of revenue/cash flow *(Does your department create revenue/cash flow to the university?)*					
Lost discounts *(Would the loss of your department create lost discounts?)*					
Lost interest earned *(If your department earns revenue/cash flow, would the loss of it also create lost interest earned?)*					
Contractual fines/penalty *(Does your department perform contract work? Would there be fines or penalties, associated with not being able to fulfill these contracts?)*					
Failure to deliver services/work product *(Would the loss of your department result in failure to deliver services/work product to anyone?)*					

Exposure type	Relative Importance Scale 0-10 0 = no importance 5 = moderate importance 10= extreme importance	Impact Severity Scale 0 – 4 0 = no impact 1 = little impact 2 = some impact 3 = significant impact 4 = severe impact			
		Less than 24 hours	**Up to 3 to 5 days**	**Greater than 5 days**	**Greater than 2 weeks**
Loss of customers/reduced market share/lost opportunity *(Would the loss of your department result in the loss of customers [i.e. patients, students, research, etc] or the loss of market share or lost opportunity?)*					
Interest incurred *(Would the loss of your department result in some type of interest being incurred?)*					
Additional costs to recover *(Would the loss of your department require additional cost from: acquisition of outside services, temporary employees, emergency purchases, rental/lease fees, wages paid to idle staff, relocation expenses, capital outlays, etc?)*					
Liability/potential litigation *(Would the loss of your department/function result in liability or potential litigation?)*					
Regulatory or non-compliance violations *(Would the loss of your department violate regulatory practices resulting in the division/university being non-compliant?)*					
Accreditation jeopardy or violations *(Would the loss of your department jeopardize any institutional accreditation or violate terms of that accreditation?)*					

14. Operational Impacts (those impacts that are difficult to quantify monetarily but can have a significant, long-term effect on the institution – use same scale as question 13):

Exposure type	**Relative Importance Scale 0-10** 0 = no importance 5 = moderate importance 10= extreme importance	**Impact Severity Scale 0 – 4** 0 = no impact 1 = little impact 2 = some impact 3 = significant impact 4 = severe impact			
		Less than 24 hours	**Up to 3 to 5 days**	**Greater than 5 days**	**Greater than 2 weeks**
Competitive Advantage					
Consumer Confidence					
Reporting Requirements					
Employee Morale					
Customer Service					
Staff Retention					
Vendor Relations					
Work Backlog					

15. The loss of your department would result in **lost revenue/cash flow** from fees, collections, interest, penalties, gifts, grants, etc. and/or diminish the department's cost avoidance capacity (i.e., fines, penalties, litigation, etc.)

During the indicated time **after the disaster**, the loss would be:

Time Frame										
Less than 24 hours	☐	*<$500K*	☐	*$500K-$1M*	☐	$1M-$5M	☐	$5M-$10M	☐	>$10M
Up to 3 to 5 days	☐	*<$500K*	☐	*$500K-$1M*	☐	$1M-$5M	☐	$5M-$10M	☐	>$10M
Greater than 5 days	☐	*<$500K*	☐	*$500K-$1M*	☐	$1M-$5M	☐	$5M-$10M	☐	>$10M
Greater than 2 weeks	☐	<$500K	☐	*$500K-$1M*	☐	$1M-$5M	☐	$5M-$10M	☐	>$10M

16. Total annual revenue for your department:

( ) None
( ) <$100K
( ) $100K-$500K
( ) $500K-$1M
( ) $1M-$5M
( ) $5M-$10M
( ) $10M-$25M
( ) >$25M

17. Total annual budgetary funding for your department:

( ) <$100K
( ) $100K-$500K
( ) $500K-$1M
( ) $1M-$5M
( ) $5M-$10M
( ) $10M-$25M
( ) >$25M

18. Based upon your experiences and knowledge of your environment, select the statement that best reflects the **vulnerability** of your department to a prolonged disruption or outage. *(Vulnerability can be related to availability of its technology infrastructure, specialized or unique equipment, or any other limiting factor.)*

( ) Not vulnerable
(No known factors that would cause a prolonged outage.)
( ) Somewhat vulnerable
(There are some factors present that may cause a prolonged outage. Experience indicates a low likelihood of occurrence.)
( ) Vulnerable
(There are factors present that may cause a prolonged outage. Experience indicates a medium likelihood of occurrence.)
( ) Extremely vulnerable
(There are multiple factors present that may cause a prolonged outage. Experience indicates a high likelihood of occurrence.)

19. The restoration complexity of a department is the relative measure of how difficult it would be to recover the department to an acceptable level of service following a significant disruption. (Complexity can be related to availability of its technology infrastructure, specialized or unique equipment, or any other limiting factor.) Please rate the complexity of your department using the following definitions.

( ) Easily recoverable
(Assumes an alternate location and required information and/or data from off-premise storage.)
( ) Somewhat recoverable
(Some information or elements may be difficult to replace in a reasonable timeframe.)
( ) Difficult to recover
(Many of the elements of your department may be difficult to replace in a reasonable timeframe.)
( ) Extremely difficult to recover
(There are elements that would be extremely difficult to replicate or the timeframe is extremely long.)

20. Does your department create, process, manage, or store identifiable records on persons relative to confidentiality or privacy? (check all that apply)

( ) Information relating to chemical or biological agents

( ) Protected patient data
(i.e., HIPAA implications)
( ) Protected student data
(i.e., FERPA implications)
( ) Personal ID
(i.e., social security numbers, employee numbers, drivers license numbers, credit card numbers, etc.)
( ) Other personal data
(i.e., physical addresses, phone numbers, pager numbers, email addresses, etc.)
( ) None

21. Does your department create, process, manage, or store information that would be of commercial value to parties external to UTMB? (check all that apply)

( ) Sensitive information
(i.e. proprietary and/or research data, employee data, etc.)
( ) Confidential Information
(i.e. patient data, student data, social security numbers, etc.)
( ) Operational Information
(i.e., vendor list, contact information, business strategic plans, etc.)

22. List and briefly describe additional departmental factors, issues or concerns not addressed in this survey which should be considered when evaluating the impact of the loss of this business unit department. Also, please list additional items you would consider important for the development of recovery strategies and plans for your department.

_____
_____
_____
_____
_____

Department Point of Contact:

_____

Date: _____

Thank you for your time and effort in completing this survey.

3.2.1 Risk Analysis

The BCP Project Team will examine each potential environmental disaster or emergency situation including, but not limited to, organized disruption (i.e. human cause); loss of utilities and services disruption; equipment or system failure; serious information security incidents; and any other disruption caused by other emergency situations not already covered.

Each of the above potential threats, as well as any others that might be unique to the individual department or function, must be examined in detail and an analysis developed to evaluate the consequences of each. Each scenario should also be assessed for possibility or occurrence (probability rating), possible impact (impact rating) and any compensating controls that are in place. Compensating Controls are internal controls that compensate for risk.

PROBABILITY RATING		IMPACT RATING	
SCORE	**LEVEL**	**SCORE**	**LEVEL**
1	VERY LOW	1	IRRITATING
2	LOW	2	CONTROLLABLE
3	MEDIUM	3	CRITICAL
4	HIGH	4	DEVASTATING
5	VERY HIGH	5	TERMINAL

Formula for calculating potential risk:

Probability Rating x Impact Rating = Risk

Scale of Risk

1	<	13	<	25
Low Risk		Moderate Risk		High Risk

Return to Table of Contents

3.2.2 Environmental Disasters

The BCP Project Team has examined each potential environmental disaster or emergency situation. The focus in this section, is on the level of business disruption, which could arise from each type of disaster.

Potential environmental disasters have been assessed as follows:

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Hurricane					
Tornado					
Flood					
Electrical Storms					
Fire					
Freezing Conditions					

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Contamination and Environmental Hazards					
Epidemic					

(Use cut and paste facility to add further entries)

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY LOW	1	IRRITATING
2	LOW	2	CONTROLLABLE
3	MEDIUM	3	CRITICAL
4	HIGH	4	DEVASTATING
5	VERY HIGH	5	TERMINAL

*Impact Rating should take into consideration compensating controls that have been implemented to lessen the severity of event.

Return to Table of Contents

3.2.3 Organized and / or Deliberate Disruption

The BCP Project Team has examined each potential disaster or emergency situation resulting from “organized disruption”. The focus in this section, is on the level of business disruption, which could arise from each type of disaster.

Potential disasters resulting from 'organized disruption' have been assessed as follows:

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Acts of Terrorism					
Acts of Sabotage					
Act of War					
Theft					

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Arson					

(Use cut and paste facility to add further entries)

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY LOW	1	IRRITATING
2	LOW	2	CONTROLLABLE
3	MEDIUM	3	CRITICAL
4	HIGH	4	DEVASTATING
5	VERY HIGH	5	TERMINAL

*Impact Rating should take into consideration compensating controls that have been implemented to lessen the severity of event.

Return to Table of Contents

3.2.4 Loss of Utilities and Services

The BCP Project Team has examined each potential disaster or emergency situation resulting from loss of utilities and services. The focus in this section, is on the level of business disruption, which could arise from each type of disaster.

Potential disasters as a result of loss of utilities and services have been assessed as follows:

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Electrical Power					
Loss of Gas Supply					
Loss of Water Supply					
Petroleum and Oil Shortage					
Communications Services Breakdown					

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Loss of Drainage/Waste Removal					

(Use cut and paste facility to add further entries)

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY LOW	1	IRRITATING
2	LOW	2	CONTROLLABLE
3	MEDIUM	3	CRITICAL
4	HIGH	4	DEVASTATING
5	VERY HIGH	5	TERMINAL

*Impact Rating should take into consideration compensating controls that have been implemented to lessen the severity of event.

Return to Table of Contents

3.2.5 Equipment or System Failure

The BCP Project Team has examined each potential disaster or emergency situation resulting from equipment or system failure. The focus in this section, is on the level of business disruption, which could arise from each type of disaster.

Potential disasters as a result of equipment or system failure have been assessed as follows:

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Internal Power Failure					
Air Conditioning Failure					

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Equipment Failure (excluding IT hardware)					

(Use cut and paste facility to add further entries)

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY LOW	1	IRRITATING
2	LOW	2	CONTROLLABLE
3	MEDIUM	3	CRITICAL
4	HIGH	4	DEVASTATING
5	VERY HIGH	5	TERMINAL

*Impact Rating should take into consideration compensating controls that have been implemented to lessen the severity of event.

Return to Table of Contents

3.2.6 Serious Information Security Incidents

The BCP Project Team has examined each potential disaster or emergency situation resulting from serious information security incidents. The focus in this section is on the level of business disruption, which could arise from each type of disaster.

Potential disasters as a result of serious Information Security incidents have been assessed as follows:

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Cyber Crime					
Loss of Records or Data					
Disclosure of Sensitive Information					

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
IT System Failure					

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY LOW	1	IRRITATING
2	LOW	2	CONTROLLABLE
3	MEDIUM	3	CRITICAL
4	HIGH	4	DEVASTATING
5	VERY HIGH	5	TERMINAL

*Impact Rating should take into consideration compensating controls that have been implemented to lessen the severity of event.

Return to Table of Contents

3.2.7 Other Emergency Situations

The BCP Project Team has examined each potential disaster resulting from other emergency situations. The focus in this section is on the level of business disruption, which could arise from each type of disaster.

Other potential emergency situations have been assessed as follows:

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF COMPENSATING CONTROLS	*IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Workplace Violence					
Neighborhood Hazards					
Island Accessible					

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY LOW	1	IRRITATING
2	LOW	2	CONTROLLABLE
3	MEDIUM	3	CRITICAL
4	HIGH	4	DEVISTATING
5	VERY HIGH	5	TERMINAL

*Impact Rating should take into consideration compensating controls that have been implemented to lessen the severity of event.

Return to Table of Contents

4.1 Back-Up, Recovery and Resumption Strategies

This section of the Plan should contain a list of the key administration and operational processes with an indication of the criticality of the process within the disruption period.

It is necessary to establish standard time-bands for measuring periods when, during an emergency, normal business services could become unavailable. These time-bands are then applied to each key business process and an assessment made of the financial and operational impact for outages.

UTMB has established three time-bands for addressing alternative procedures.

- Scheduled/Anticipated Outage – this option assumes that communication as been made to all departments that downtime will occur at a pre-posted data and time duration (this is determined by the department).

- Unscheduled Outage – Short Duration – this option assumes that there is a service interruption, but is projected to be of a short-term duration (this is determined by the department).

- Unscheduled Outage – Long Duration – this option assumes that there is a service interruption, due to systems or facilities, for an extended period of time (this is determined by the department).

Identify the potential disruption and impact to each of these processes. Additionally identify alternative methods of handling each of these activities. Manual back up procedures will be developed for Administration and Operations functions as these are usually relatively easy to implement when IT systems are not available. These can often be supported by business or office software providing spreadsheet, database and word processing capabilities.

To resume normal operations it is essential to plan for the potentially complex activities necessary to complete your recovery process. Once the emergency is over, you may need to transition from a manual process back to an electronic process. This may involve extensive data entry and reconciling of data. In order for this process to be effective, it must be carefully planned and structured. Resumption Strategy contains the format for recording activities, which need to be, carried out in priority sequence and which person or teams are responsible for completing those tasks. Where supplies and vendors are required to supply goods or services, as part of the resumption process then these activities will be involved.

Return to Table of Contents

4.1.1 Back-Up, Recovery and Resumption Strategies

Identify each essential activity, along with its potential disruption and impact of each process. Additionally identify alternative methods of handling each of these activities along with resumption procedures for resuming normal operations. Each activity will have a separate grid.

ESSENTIAL ACTIVITIES	**SCHEDULED/ANTICIPATED OUTAGE Generally < (Time Frame??)**	**UNSCHEDULED OUTAGE – Short Duration < (Time Frame??)**	**UNSCHEDULED OUTAGE- Long Duration > (Time Frame??)**
(Name Activity Here)			
Potential Disruption			
Potential Impact:			
Recovery Strategy			
Resumption Strategy			

Return to Table of Contents

4.2 Facilities and Essential Equipment Back-Up and Recovery Strategies

Many unexpected events can affect facilities and essential equipment that are vital to continuation of normal business activities. These include fire, flood, hurricane, terrorist activity, etc. The Team must therefore develop a plan of how to continue to provide business services to its customers in the event of a disaster, which affects either its facilities or essential equipment.

We recommend that each department contact and work with Facilities Operations and Management (409-772-3500) to obtain alternative locations for conducting your business functions.

This section of the Business Continuity Plan (BCP) will contain details of such arrangements and an estimate of potential costs.

Return to Table of Contents

4.2.1 Facilities and Essential Equipment Back-Up and Recovery Strategies

Many unexpected events can affect facilities and essential equipment vital to the continuation of normal business activities. This plan has therefore been developed to ensure a continued service to customers in the event of a disaster affecting either the department's / or function's facilities or its essential equipment.

The department's / or function's back-up and continuity strategies for its facilities and essential equipment are as follows.

1. FACILITIES

NAME OF FACILITIES	AGREED BACK-UP AND CONTINUITY STRATEGY

(Use cut and paste facility to add further entries)

2. ESSENTIAL EQUIPMENT

NAME OF EQUIPMENT	DESCRIPTION OF EQUIPMENT	LOCATION	COST ESTIMATE TO REPLACE
Agreed Back-up Continuity Strategy			

NAME OF EQUIPMENT	DESCRIPTION OF EQUIPMENT	LOCATION	COST ESTIMATE TO REPLACE
Agreed Back-up Continuity Strategy			

(Use cut and paste facility to add further entries)

Return to Table of Contents

4.3 Departmental and University IT Systems Back-Up and Recovery Strategies

In General one of the most important aspects of Business Continuity Planning for the majority of departments or functions is in choosing an appropriate strategy for the back-up and recovery of the IT- based systems.

In this section of the Plan, the key business processes are matched against the IT system and an appropriate time frame to complete recovery is chosen. This section may require in-depth research to determine the relevant costs of each strategy. It may also be necessary to prepare a detailed Request for Proposal for vendors to establish the viability and cost of the preferred strategic approach.

Consideration should also be given to the impact of potential severe damage to both facilities and communication's systems, which could have a significant impact on the department's /or function's IT, services and systems.

Return to Table of Contents

4.3.1 Departmental and University IT Systems Back-Up and Recovery Strategies

One of the most important aspects of Business Continuity Planning is choosing of an appropriate strategy for the back-up and recovery of IT- based systems. Consideration has been given to the impact on the department / or function's IT systems of potential severe damage to facilities or communications systems.

A summary of the Departmental IT systems and the agreed back-up strategy are listed below. Each department systems will also need to develop disaster recovery/restoration procedures. (see example of UTMB Information Services disaster recovery documentation)

NAME OF IT SYSTEM	**RECOVERY TIME REQUIRED**	**KEY BUSINESS PROCESS SUPPORTED**	**POTENTIAL IMPACT**
IS SYSTEM BACKED UP? HOW OFTEN IS SYSTEM BACKED UP? WHERE ARE BACKUP TAPES KEPT? DOES THIS SYSTEM HAVE VITAL ELECTRONIC RECORDS AND/OR DATA:			
AGREED BACK-UP STRATEGY: (What is your strategy if system is not available?)			
PERSON RESPONSIBLE FOR SYSTEM (i.e. maintenance, backup, restoration)		ALTERNATE PERSON RESPONSIBLE FOR SYSTEM	
IS SYSTEM BACKED UP? HOW OFTEN IS SYSTEM BACKED UP? WHERE ARE BACKUP TAPES KEPT?			
AGREED BACK-UP STRATEGY: (What is your strategy if system is not available?)			
PERSON RESPONSIBLE FOR SYSTEM (i.e. maintenance, backup, restoration)		ALTERNATE PERSON RESPONSIBLE FOR SYSTEM	

A summary of the University centralized IT Systems/Applications, which support department functions, and the Information Services contact information. *(It is Information Services responsibility to establish back-up strategy for the IT System listed below)*

NAME OF IT SYSTEM	**KEY BUSINESS PROCESS SUPPORTED**	**POTENTIAL IMPACT**
Campus Data Network	Connectivity for data access/exchange from all servers on the campus.	Inability to access/process data filed on any server on the campus.
IS CONTACT INFORMATION; IS Help Desk – ext 25200		
NAME OF IT SYSTEM	**KEY BUSINESS PROCESS SUPPORTED**	**POTENTIAL IMPACT**
IS CONTACT INFORMATION:		

Return to Table of Contents

4.4 Strategies for Protecting Non-Electronic Critical and/or Sensitive Documents and/or Records

The BCP Project Team has assessed both electronic records and paper based records listed below as being vital and/or sensitive to the organizations business activities. Strategies for protecting and recovering these documents have been reviewed and are documented below.

Name of Document/Record	Brief Description	Does this document hold confidential or sensitive information (what type)	Location Held
What safeguards are in place to protect records from damage and/or disclosure:			
Would these documents need some type of restoration in the event of damage?			

Name of Document/Record	Brief Description	Does this document hold confidential or sensitive information (what type)	Location Held
What safeguards are in place to protect records from damage and/or disclosure:			
Would these documents need some type of restoration in the event of damage?			

Name of Document/Record	Brief Description	Does this document hold confidential or sensitive information (what type)	Location Held
What safeguards are in place to protect records from damage and/or disclosure:			
Would these documents need some type of restoration in the event of damage?			

4.5 Key Staff

Employees are an important and valuable assets who in an emergency will assist department / or function in a quick recovery. Main suppliers of critical goods and services are also essential to continue to support recovery of business operations to normal operating mode.

Your Disaster Recovery Plan and BCP will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth business recovery process. These key members of management or staff will be selected and responsible for the implementation of the BCP in the event of an emergency. A well-organized and structured approach will reduce the potential for the unexpected crisis to become unmanageable.

This information is for departmental use and will not be generally distributed.

Return to Table of Contents

4.5.1 Key Personnel

When an emergency occurs it is necessary to have access to all key personnel for the functional areas and systems affected by the crisis. This information should be made available to the BCP recovery teams and should be constantly updated.

This section of the BCP will contain a list of key personnel, their position, functional area, and procedures or systems for which they are responsible. This section will also include normal and emergency contact information. This information is for departmental use and will not be generally distributed.

Due to changes in personnel (i.e. attrition, moves, etc it is recommended that this be tested and updated at least quarterly.)

NAME	DIVISION/ DEPARTMENT	FUNCTION OR PROCESS FOR WHICH RESPONSIBLE	OFFICE EXT. EMERGENCY CONTACT DETAILS (Home, Pager, Cell Phone)

Return to Table of Contents **Last Revision_____**

4.6 Emergency Contact Information

EXTERNAL EMERGENCY CONTACT NUMBERS

Police, Fire and Ambulance 911
UTMB Emergency Alert Line – (409) 77-Alert (772-5578)
Toll Free 1-888-772-5449
UTMB Campus Operator (409) 772-1011

INTERNAL EMERGENCY CONTACT NUMBERS

Add numbers as needed.

UTMB POLICE	21111
UTMB FIRE LINE	21211
Office of University Advancement (call them for media communication)	22618
FACILITIES MAINTENANCE	21586
POISON CONTROL CENTER	800-764-7661

www.utmb.edu/alert
www.utsystem.edu/utmb/alert.htm

Return to Table of Contents

4.7 Critical Supplies

It is necessary to prepare for emergencies where the department's supplies may be destroyed or unobtainable through usual sources. Such an occurrence could, for example, be caused through fire or flood damage.

The department / or function should decide on a suitable strategy to deal with this situation, which could include holding an emergency stock of supplies at an off-site location. Alternatively, the BCP could include a list of emergency supplies, which could be ordered on a next-day delivery basis. Details of alternative suppliers should also be included, in the event that your normal supplier is also affected by an emergency.

This section of the BCP should include information on the supplies held off-site, together with a list of items that could be ordered in an emergency at short notice. It should also list alternative suppliers.

Return to Table of Contents

4.7.1 Critical Supplies

In the event of an emergency where the department's supplies are destroyed, back-up stock can be obtained from off-site locations, as follows. Also listed below are details of suppliers who can provide emergency supplies on a next-day delivery basis.

1. CRITICAL SUPPLIES STOCK HELD OFF-SITE

ITEM	NAME OF LOCATION	ADDRESS OF LOCATION	CONTACT PERSON	CONTACT NO.

(Use cut and paste facility to add further entries)

2. SUPPLIES THAT CAN BE ORDERED ON A NEXT DAY BASIS FROM REGULAR SUPPLIER

ITEM	NAME OF REGULAR SUPPLIER	CONTACT PERSON	CONTACT NO.

3. ALTERNATIVE SUPPLIERS ABLE TO SUPPLY ON NEXT DAY BASIS IF REGULAR SUPPLIERS AFFECTED BY EMERGENCY

ITEM	NAME OF ALTERNATIVE SUPPLIER	CONTACT PERSON	CONTACT NO.

Return to Table of Contents

4.8 Critical Vendor

Depending upon the nature of the disaster, it is feasible that vendors of critical services may also be affected. This can affect your own back-up and recovery arrangements where your department is dependent upon a particular vendor for that recovery process to be achieved successfully. It is important therefore that your own key vendor also have an effective BCP for dealing with emergencies. You should request information from your vendors to ensure they have this.

This section of the BCP should include a list of key vendors the critical services they are supplying, their normal contact information, and their emergency contact information. Further consideration should be given to vendors who would be able to provide critical services in the event of failure to deliver from one of your identified key vendors.

Return to Table of Contents

4.8.1 Critical Vendors

Listed below are the department / function key vendors who may need to be contacted in the event of an emergency. In the event of these regular vendors are not able to provide the services required in an emergency, an alternative list of vendors has also been identified.

1. REGULAR VENDORS

NAME OF VENDOR	SERVICES PROVIDED	NORMAL CONTACT DETAILS	EMERGENCY CONTACT DETAILS

2. ALTERNATIVE VENDORS

NAME OF VENDOR	SERVICES PROVIDED	NORMAL CONTACT DETAILS	EMERGENCY CONTACT DETAILS

5.0 Plan Education and Training

All staff should be trained in the business continuity process. This is particularly important when the procedures are significantly different from those pertaining to normal operations. This training may be integrated with the training phase or handled separately.

A training needs assessment must be conducted to identity what training should be established. The plan must specify which person or group of persons requires which type of training. It is t is necessary for all new or revised processes to be explained carefully to the staff. For example it may be necessary to carry out some process manually if the IT system is down for any length of time. These manual procedures must be fully understood by the persons who are required to carry them out. For larger organizations it may be practical to carry out the training in a classroom environment, however, for smaller organizations the training may be better handled in a workshop style.

This section of the BCP will identify for each business process what type of training is required and which persons or group of persons need to be trained.

5.1 Training Assessment

KEY BUSINESS AREA	TYPE OF TRAINING REQUIRED	PERSONS OR GROUPS TO BE TRAINED	NO. OF PERSONS

Return to Table of Contents

5.2 Training Completed

It is important to keep a record of all employees who have been trained in the BCP Process.

PERSONS OR GROUPS TO BE TRAINED	KEY BUSINESS AREA TRAINED	DATE COMPLETED

Return to Table of Contents

6.0 Plan Testing

An untested plan can often be more of a hindrance than help. The ability of the BCP to be effective in emergency situations can only be assessed if rigorous testing is carried out in realistic conditions. The BCP Testing Phase contains important verification activities, which should enable the plan to stand up to most disruptive events.

The BCP should be tested within a realistic environment, which means simulating conditions, applicable in an actual emergency. It is also important that the persons who would be responsible for those activities in a crisis carry out the tests.

In most cases a tabletop test will be conducted. A scenario will be given to your BCP group along with questions that will need to be answered during the test.

Return to Table of Contents

7.0 Plan Maintenance

It is necessary for the BCP updating process to be properly structured and controlled. This would include an evaluation of the Disaster Recovery Plan (IT Plan) for potential change due to the dynamic nature of the threat population and system configuration

Whenever changes are made to the BCP they are to be fully tested and appropriate amendments should be made to the training materials. This will involved the use of formalized change control procedures under the control of the BCP Team Leader.

The following form should be used for the request and approval of such changes. Following approved changes to the plan, it is important that the BCP leader, BCP recovery team, Executive Sponsor and the IRM are kept fully informed.

Return to Table of Contents

7.1 Test all Changes to Plan

Whenever there is a change to the BCP Plan a complete test should be carried out and documented.

Follow the appropriate test procedures as outlined in Section 5 of this plan.

Return to Table of Contents

8.0 Post Incident Analysis/Report

On completion of any incident, that impacts your delivery of normal service, the BCP Team should prepare an incident analysis on your BCP plan. This is to assess the adequacy of the plan and any deficiencies.

The principal overall objectives in conducting the post incident analysis are to; verify that the business recovery/resumption plans are current and up to date, that the recovery/resumption plan performed effectively and recovered the affected functions, identify areas of the plan to improve, evaluate the flow of communications, and evaluate the effectiveness of the plan.

8.1 Post Incident Analysis

The BCP team has reviewed the following incident.

Date of incident:	Time:
Description of incident:	
What critical function/functions were interrupted during this incident?	
Did your BCP address the recovery of the interrupted critical function effectively?	
If not, what areas of the recovery plan can be improved?	
Did communication flow effectively?	
Where there any problems getting or receiving communications?	
Where all phone numbers accurate and available?	

What changes need to be made to the BCP?
Who will be making the changes to the plans?
Will changes need to be tested?
Who will approve the changes made to the BCP?
Who will be reporting changes made to the Executive Sponsor of the plan?

9.0 Glossary of Terms

Act of Sabotage: An act of sabotage is the deliberate serious disruption of an organization's activities with an attempt to discredit or financially damage the organization. Business will often be immediately and seriously affected by successful acts of sabotage. This can affect the normal operations and also serve to de-stabilize the workforce. An internal attack on the IT systems through the use of malicious code can be considered to be an act of sabotage.

Act of terrorism: Acts of terrorism include explosions, bomb threats, hostage taking, sabotage and organized violence. Whether this is perpetrated through a recognized terrorist organization or a violent protest group, the effect on individuals and business is the same. Such acts create uncertainty and fear and serve to destabilize the general environment.

Act of War: An act of war is the commencement of hostilities between one country and another. This could take the form of air strikes, ground strikes, invasion or blockades. Business could be immediately affected where they are either located near the outbreak of hostilities or where they are dependent upon imports or exports for survival. Many businesses do not survive a prolonged outbreak of war.

Air conditioning failure: An air conditioning (AC) failure could have serious consequences where the AC unit is protecting particularly sensitive equipment such as a main computer processing unit, and the rise in temperature could cause the equipment to fail and be damaged. It can also affect the workforce as conditions in buildings can become extremely uncomfortable with a significant rise in temperatures and where the staff is adversely affected. Portable AC equipment may possible be used as back up.

Alert: A formal notification that an incident has occurred which may develop into a disaster.

Alternate Site: A location where critical business functions can resume processing in the event of an interruption or disaster.

Arson: Arson is the deliberate setting of a fire to damage the organizations premises and contents. As this can cause both loss of premises and loss of goods and other assets, this can be highly disruptive to the organization.

Building denial: Any damage, failure or other condition, which causes denial of access to the building or the working area within the building, e.g. fire, flood, contamination, loss of services, air conditioning failure, and forensics.

Business Continuity Plan: A collection of procedures and information that is developed and maintained in readiness for use in the event of an emergency or disaster.

Business Continuity Planning (BCP): Preparations made to keep a business running during and after a disaster, ensuring the availability of those resources required to maintain the ongoing viability of the organization.

Business Continuity Team Leader: A member of the recovery management team who is assigned the overall responsibility for coordinator of the recovery planning program ensuring team member training, testing and maintenance of recovery plans.

Business impact analysis (BIA): A management level analysis, which identifies the impacts of losing company resources. The BIA measures the effect of resources loss and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

Business Impact Assessment (BIA): Ask the following questions: How bad can things get? What are the most important resources, systems, outputs, and dependencies by business function? What impact does unavailability have?

Cold Site: One or more data centers or office space facilities equipped with sufficient pre-qualified environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by critical staff required to resume business operations.

Command Center: This is the location set up for management and BCP to operate from during emergency situations. The continuity plan document and other needed resources should be maintained there.

Communications services breakdown: Most businesses are fully dependent upon their telecommunications services to operate their normal business processes and to enable their networks to function. A disruption to the telecommunications services can result in a business losing revenue and customers. The use of cell-based telephones can help to alleviate this but the main reliance is likely to be on the land based lines.

Contamination and Environmental Hazards: Contamination and environmental hazards include polluted air, polluted water, chemicals, radiation, asbestos, smoke, dampness and mildew, toxic waste and oil pollution. Many of these conditions can disrupt business processes directly and, in addition, cause sickness among employees. This can result in prosecution or litigation if more permanent damage to employees' health occurs.

Controllable: UTMB would be able to exercise restraint and direct influence over the event, remaining in relative control of business.

Crisis: An abnormal situation, or perception, which threatens the operations, staff, customers or reputation of an enterprise.

Critical: UTMB would find that quality, service, and/or property could suffer, causing a change or disruption in business resulting in a moderate state of crisis or emergency.

Critical Business Functions: Those functions considered essential to the ongoing operation of the organization or business unit. Critical functions also include anything that might adversely impact service deliver or significantly impair the administrative or financial integrity of the organization.

Cyber crime: Cyber crime is a major area of information security risk. It includes attacks by hackers, denial of service attacks, virus attacks, hoax virus warnings and premeditated internal attacks. All cyber crime attacks can have an immediate and devastating affect on the organization's normal business process. The average cost of an information security incident has been estimated at #30,000 and over 60% of organizations are reported to experience one or more incident every year.

Devastating: UTMB services would be significantly degraded, but would be able to conduct business.

Disaster Recovery Coordinator: Activates Disaster Recovery Plan. Works with administration, advisory committees, and Disaster Recovery Team to allocate resources and coordinate implementation of the Disaster Recovery Plan. Serves as the primary contact and coordinates the recovery effort. Insures that status of the recovery effort is communicated to the appropriate levels of the organization. Insures that a post mortem review is conducted and that upgrades are incorporated into the plan as appropriate.

Disaster Recovery Planning (DRP): Typically, the technology aspects of a business continuity plan, to recover information system resources to full or partial production processing levels in the event of an extended outage. Normally, information system resources will be restored according to a priority indicated by what is "mission critical" to the organization.

Disclosure of sensitive information: This is a serious information security incident, which can result in severe embarrassment, financial loss, and even litigation where damage has been caused to someone's reputation or financial standing. Further types of serious disclosure involve secret patent information, plans and strategic directions, research, information disclosed to legal representatives etc. Deliberate unauthorized disclosure of sensitive information is also referred to as espionage.

Electrical Storms: the impact of lightning strikes can be significant. It can cause disruption to power and can also cause fires. It may also damage electrical equipment including computer systems. Structural damage is also possible through falling trees or other objects.

Electrical power failure: All organizations depend on electrical power to continue normal operations. Without power the organization's computers, lights, telephones and other communication medium will not be operational and the impact on normal business operation can be devastating. All organizations should be prepared for a possible electrical power failure, as the impact can be so severe. Data can be lost, customers can be lost and there can be a serious impact on revenue. Pre-planning is essential as a regional outage can cause a shortage of backup electrical generators.

Epidemic: An epidemic can occur when a contagious illness affects a large number of persons within a country or region. This can have a particularly devastating short term impact on business through a large number of persons being absent from work at the same time. Certain illnesses can have a longer-term effect on the business where long term illness or death results. An example of this extreme situation is occurring in China now with the epidemic of SARS.

Equipment Failure (excluding IT hardware): All businesses rely on a whole range of different types of equipment in order to run their business processes. In many cases, it is possible to move to alternative processes to enable the businesses process to continue but his required considerable planning and preparation.

Fire: Fires are often devastating and can be started through a wide range of events, which may be accidental or environmental. The impact on the business will vary depending on the severity of the fire and the speed within which it can be brought under control. A fire can cause human injury or death and damage can also be caused to records and equipment and the fabric or structure of premises.

Flood: Floods result from thunderstorms, tropical storms, snow thaws or heavy and prolonged rainfall-causing rivers to overflow their banks and flood the surrounding areas. Floods can seriously affect buildings and equipment causing power failures and loss of facilities and can even result in injury or death.

Freezing Conditions: Freezing conditions can occur in winter periods and the effects can be devastating. Where temperatur3es fall in excess of – 30 Centigrade they can create conditions, which significantly disrupt businesses and even cause death or injury. Businesses and homes can be seriously affected through burst pipes, inadequate heating facilities, disruption to transportation and malfunctioning equipment. Work undertaken outside of buildings in the open environment will obviously be seriously affected.

Hot Site: A data center facility or office facility with sufficient hardware, communications interfaces and environmentally controlled space capable of providing relatively immediate backup data processing support.

Hurricane: Hurricanes are storms with heavy circular winds exceeding 60 miles per hour. The hurricane contains both extremely strong winds and torrential rain. Hurricanes can cause flooding, massive structural damage to homes and business premises with associated power failures, and even injury and death.

Impact: Impact is the cost to the enterprise, which may or may not be measured in purely financial terms.

Incident: Any event, which may be, or may lead to, a disaster.

Information Security: The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization.

Internal arrangement: Other rooms within the organization could be equipped to support business functions (i.e., training rooms, cafeterias, conference rooms, etc)

Internal power failure: An internal power failure is an interruption to the electrical power services caused through internal equipment or cabling failure. This type of fault will need to be repaired by a qualified electrician and delays will inevitable impact on the business process. Where particularly serious faults have occurred, such as damage to main cables, the repairs could take some time and could have a severe effect on the business.

Irritating: UTMB would be able to exercise restraint and direct influence over the event, remaining in relative control of business.

Loss of drainage / waste removal: The loss of drainage or waste removal is likely to cause a serious sanitation and health issue for most businesses. This is likely to impact on the business through the possible loss of its workforce during the period where drainage services are not available. This, in turn, will have an immediate impact on revenue.

Loss of gas supply: The loss of gas supply can be extremely serious where the business relies on gas to fuel either its production processes or provide heating within its premises. The impact that a loss of gas supply can have on the production process can result in the whole process shutting down. The impact on the organization will also be particularly acute where the loss of gas-fired heating could render the premises unusable during periods of low external temperatures.

Loss of records or data: The loss of records or data can be particularly disruptive where poor backup and recovery procedures result in the need to re-input and re-compile the records. This is normally a slow process and is particularly labor intensive. This can result in an increase in costs through additional working hours and a great deal of embarrassment where information is unexpectedly not available.

Loss of water supply: The loss of the water supply is likely to close down a business premises until the supply is restored. Where the water is used in the production process this is particularly serious. The loss of water supply is also a health and safety issue as minimum sanitary needs cannot be met. This is often caused through a fault in a water supply route or as a result of a particularly severe drought.

Island accessibility: Since Galveston is an island and has limited accessibility, access to the island by employees, supplies and customers will need evaluated and assessed.

IT system failure: With the almost total level of dependence on IT systems within the vast majority of businesses, a failure to these systems can be particularly devastating. The types of threats to computer systems are many and varied, including hardware failure, damage to cables, water leaks and fires, air conditioning system failures, network failures, application system failures, telecommunications equipment failures etc.

Neighborhood hazard: A neighborhood hazard is defined as a disruptive event in the close vicinity, which directly or indirectly affects your own premises and employees. An example would be seepage of hazardous waste or the escape of toxic gases from a local chemical plant. Health and safety regulations require that the organization take suitable action to protect its employees. This may have severe disruptive implications for the business particularly where it can take some time to clear the hazard.

Off-site location: A storage facility at a safe distance from the primary facility, which is used for housing recovery, supplies, equipment, vital records etc.

Operational Impact: An impact, which is not quantifiable in financial terms but its effects, may be among the most severe in determining the survival of an organization following a disaster.

Outage: The interruption of automated processing systems, support services or essential business operations that may result in the organization's inability to provide service for some period of time.

Period of Tolerance: The period of time in which an incident can escalate to a potential disaster.

Petroleum and oil shortage: For most countries in the world, a petroleum shortage can occur at any time. This has a serious impact on businesses as rationing is likely to be imposed immediately affecting transportation and the normal operations of diesel or petrol fuelled machinery.

Reciprocal arrangement: An agreement in which two parties agree to allow the other to use their site, resources or facilities during a disaster.

Recovery Point Objective (RPO): This is defined by the data content owner of an IT application. It is the point in time that the application must be restored to.

Recovery Time Objective (RTO): This is defined by the data content owner for an IT application. It is the time from disaster declaration to the restoration of the application.

Resumption: The process of planning for and/or implementing the recovery of critical business operations immediately following an interruption or disaster.

Risk Assessment & Management: The identification and evaluation of operational risks that particularly affect the enterprise's ability to function and addressing the consequences.

Risk Reduction or Mitigation: The implementation of the preventative measures, which risk assessment, has identified.

Scenario: A pre-defined set of events and conditions, which describe an interruption, disruption or disaster related to some aspect (s) of an organization's business for purposes of exercising a recovery plan (s).

Self-service: An organization or business function can transfer work to another of it's own locations.

Service Level Agreement (SLA): An agreement between a service provider and service user as to the nature, quality, availability and scope of the service to be provided.

Site access denial: Any disturbance or activity within the area surrounding the site which renders the site unavailable, e.g. fire, flood, riot, strike, loss of services, forensics. The site itself may be undamaged.

System Recovery: The procedures for rebuilding a computer system to the condition where it is ready to accept data and applications. System recovery depends on having access to suitable hardware.

Terminal: UTMB would be unable to achieve its core purpose and unable to conduct its mission

Theft: This hazard could range from the theft of goods or equipment to the theft of money or other valuables. In addition to possible financially damaging the organization, they can cause suspicion and uncertainty with the workforce where it may be believed that one or more of them could have been involved.

Tornado: Tornadoes are tight columns of circling air creating a funnel shape. The wind forces within the tornado can reach over 200 miles per hour. Tornadoes can often travel in excess of 50 miles per hour. They can cause significant structural damage and can also cause severe injuries and death.

Vital Records: All data and information required to support business functions (i.e., historical, regulatory requirements including, but not limited to, policy and procedures manuals, input documents or data, manuals for software and other applications, vendor/customer lists with phone numbers, and backup tape files.) Additionally, these records should be maintained off-site at a third party vendor or command center.

Warm Site: A data center or office facility which is partially equipped with hardware, communications interfaces, electricity and environmental conditioning capable of providing backup operating support.

Workplace violence: Acts of violence in the workplace can affect moral, absenteeism, create fear and uncertainty and increase the rate of turnover of employees. This can have a significant affect on productivity and could also result in claims for workers compensation, harassment claims and a need for increased security measures. Statistically, this type of incident is especially prevalent at organizations which have recently merged or are being re-sized or restructured, where there are regular threats of industrial action, or where permanent employees have been replaced with temporary employees.