

WORKBOOK FOR BUSINESS CONTINUITY PLANNING AND MAJOR HEALTH EMERGENCY PLANNING



UNIVERSITY OF ALBERTA

Table of Contents

1. Introduction

- 1.1 Message from the Provost
- 1.2 Integrated Emergency Management Program
- 1.3 Overview of Emergency Preparedness and Business Continuity
- 1.4 Major Health Emergency Planning (Pandemic Influenza)

2. Phase 1 of Workbook - Conduct Analysis of Your Services and Functions

- 2.1 Faculty or Department Information
- 2.2 Develop Project Team
- 2.3 Conduct a Business Impact Analysis
 - 2.3.1 Identify Major Services and Functions
 - 2.3.2 Identify the Critical Services and Functions From Your List

3. Phase 2 of Workbook - Develop Solutions and Strategies For Resumption of Your Critical Services and Functions. Identify Hazards, Risks and Vulnerabilities

- 3.1 Strategize solutions to service outages
 - Select Recovery and Resumption Strategies
 - Determine Recovery Time Objectives for selected Recovery Strategies
 - Develop Action Plans for Implementing Strategies
- 3.2 Determine Risks and Vulnerabilities
 - 3.2.1 Mitigation/Counter Measures and Vulnerability Identification
- 3.3 Contact Lists for Personnel
 - **Internal**
 - All faculty/department staff
 - List essential personnel as applicable
 - **External**
 - Key Partners
 - ◆ Key Vendors
 - Key Customers
- 3.4 List minimum resources needed to recover and resume critical services and functions
 - Equipment
 - Facilities
 - Vehicles
 - Special Needs

4. Appendices in Workbook

- 4.1 Appendix A Slide of Upstream and Downstream Interdependencies
- 4.2 Appendix B Maximum Acceptable Downtime of a Service
- 4.3 Appendix C Public Health Response Strategy Document
- 4.4 Appendix D - Vital Records, Information Technology and Telecommunications

End of Workbook

Next Phase of Development and Workbook Template for Unit Action Plan (To be developed)

5. Phase 3 - Implementation

- a. Complete the Faculty/Department Action Plan/Emergency Operations Plan Template
- b. Conduct Training for Faculty/Department
- c. Evaluate the Faculty/Department Action Plan
- d. Implement the Faculty/Department Action plan

6. Phase 4 - Maintenance

- a. Develop Maintenance Program for the Faculty/Department Action Plan
- b. Develop Change Management Process
- c. Complete program audits

Acknowledgements:

We would like to acknowledge that material from the following institutions (see list below) have been referenced during the development of some of our Emergency Preparedness and Business Continuity Planning documents.

List: University of California, Berkeley, University of California Davis, Arizona State, University of Colorado, University of Michigan, University of North Carolina and the Commonwealth of Australia, Business Continuity Management.

SAMPLE ONLY

1.1 Message from the President/Provost

Purpose and Scope for a Faculty/Department Emergency Preparedness and Business Continuity Plan

To fulfill our Dare to Discover mandate and to support the Cornerstones building and sustaining our future, the University of Alberta needs to be as resilient as possible when disasters or major business interruptions strike. A robust emergency management program is required when unplanned events negatively impact our core businesses and the ability to deliver critical services. In addition, the University has an obligation to the students, staff, faculty, the community and the Provincial Auditor General to develop and implement emergency preparedness and business continuity plans. To that end the University has implemented an emergency preparedness and business continuity policy, developed a steering committee and is committed to developing an Integrated Emergency Management Program (IEMP). The IEMP will be comprised of plans, standards, training, exercises, performance criteria and a change management process for the program. The goal is to have a program that positions the University to be as ready as possible to respond, recover and resume our critical services when impacted by a disaster or major business interruption. That means all Departments, Faculties and Units must have an emergency preparedness and business continuity plan that will be a component of the overall University program. In an effort to help you and your team develop a plan we have dedicated some resources to assist in the development and implementation of your plan.

The purpose of preparing, implementing and maintaining a Faculty/Department Emergency Preparedness and Business Continuity (EPBC) Plan is to ensure reasonable and practical delivery of our core businesses in the event of a disaster or interruption/outage of a critical service or function. Disasters and major outages can arise from several sources; natural disasters, human-made business interruptions, technological failures and financial collapses. A comprehensive Program at the University includes elements such as. Preparedness, prevention, contingency measures, response, assessment, recovery and resumption. Associated with the key program elements is the need for document control, change management procedures, communication, training and exercises.

The intent of the plan is to provide the framework for the pre-emergency analysis and strategies and the organizational structure complete with roles and responsibilities to execute the plan. Details within the plan will describe the recovery and resumption elements of the Faculty or Department. Recovery planning focuses on the set of actions a Department must take to restore services/functions and return to as near as normal operations in the shortest period of time. The process for developing the plan uses a systematic means of analyzing the critical services and function, determining the downtime before our core businesses are impacted and highlighting the common elements, interdependencies and single points of failure that could occur during a disaster or major outage. Rather than having a focus on the disaster event itself e.g. a major structure fire, the process seeks out commonalities such as: loss of facilities, loss of access to facilities, loss of personnel, loss of information and loss of equipment.

The key component of a Faculty or Department plan is the development of alternative measures or contingency plans designed to maintain the Department's services and functions when disaster strikes or we experience a major outage. Your plan will provide details with respect to actions to be taken by the Faculty or Department such as, activation of the plan and identification of key personnel and resources (internal and external to the University) in order for the department to resume services within a defined period of time. Your plan will be designed to provide timely efficient and controlled response, recovery and restoration of critical services and operations.

The University Emergency Master Plan will form the base document for the development of the Faculty and Department EPBC plans. Consistency in format, structure and execution of the plans is required to support the integrated model of managing the risks to our core businesses when a major emergency impacts the University or the region. It is the intent to have the templates and plans web based, user friendly, current and readily accessible. A Workbook has been created to assist in the development and implementation of your plan. The target is to have all University plans completed and in place on or before December, 2007.

Dated:

Signed:

1.2 Integrated Emergency Management Program

To fulfill our Dare to Discover and Dare to Deliver mandates and to support the Cornerstones for building and sustaining our future, the University of Alberta is developing a program that will ensure the University is as robust and resilient as possible when disasters or major business interruptions strike. A comprehensive management program is required when unplanned events negatively impact the University's ability to deliver critical services and challenge us to maintain order during chaotic and turbulent times. The University has an obligation to the students, staff, faculty, and the community to develop an **Integrated Emergency Management Program (IEMP)**.

The Integrated Emergency Management Program is a dynamic, proactive, system based, team driven approach to understanding, managing and communicating during a major emergency or business outage/interruption. It is about making critical decisions that will contribute to the continuity of critical services supporting the core businesses and the overall goals and objectives of the University. The program is a substantial contributor to the University's enterprise wide risk management strategy. Through a scenario planning process, the analysis and identification of risk exposures and vulnerabilities and pre-emergency planning activities, the University will be better positioned to implement preventative measures.

To that end the program will build capacity into the University to implement prevention measures while at the same time are able to manage through and recover from an emergency. The program will improve teamwork, enhance trust and build partnership relations internally and with important external organizations. The results will increase the University community's confidence in emergency management and will provide a boost to the University's integrity and reputation

1.3 Emergency Preparedness and Business Continuity

The University has implemented an [Emergency Preparedness and Business Continuity Procedure](#) enabled through a [Risk Management Policy](#), developed a steering committee and is committed to developing an Integrated Emergency Management Program. The desired state includes all faculties and departments conducting emergency preparedness and business continuity planning and the development their respective [Unit Action Plan](#). The Unit Action Plans will be components of the overall university integrated emergency management program. To that end the University has dedicated resources to assist in the development and implementation of faculty or department action plans.

The current focus in the development of the integrated plan for emergency preparedness and management is on **business continuity planning** within the faculties and departments. With concentration on elements such as, identification of critical services, interdependencies, maximum acceptable downtimes, recovery time objectives and vulnerabilities, a phased approach to the development of a faculty or department unit action plan has been implemented. The methodologies applied to conduct the business continuity planning include the development of a university workbook, awareness presentations, development of work teams and the delivery of workshops within the faculties and departments. Rather than having a focus on the disaster event itself such as a major structure fire, the process seeks out commonalities that include loss of facilities, loss of access to facilities, loss of personnel, loss of information technology, loss of equipment and loss of a key vendor.

Key principles of EPBC plans and outcomes of the planning process include:

The outcome of the analysis and planning processes must produce plans that are realistic, practical, achievable and reasonable for the University to uphold.

The identification and assessment of risks across the University will produce a total risk index that will provide the basis for developing cost benefit analysis and business cases for eliminating, reducing or mitigating the risks.

Emergency preparedness, response, recovery and resumption are all components of business continuity at the university.

Plans are built from the bottom up in the departments and faculties with commitment to the planning and desired future state coming from the University Executives and Deans.

Each department or faculty will designate a position having the responsibility to develop, implement and maintain the respective unit action plan.

1.4 Major Health Emergency Planning (Pandemic Planning)

Appendix C of the workbook provides a planning form to analyze and prepare for the impacts of a major health emergency such as an avian influenza pandemic.

2. PHASE I ANALYSIS

2.1 Business Continuity Plan Development

Faculty: _____

Department: _____

HISTORY OF THIS PLAN		
	Name	Date
Original submission		
-Reviewed by Dean of Faculty or VP of Department		
Most recent update		
Business Continuity Plan Communicated to staff		

Department Information

Name of Faculty, Department (or Sub Unit within a Faculty or Department)

Number of Staff (headcount, approximation is OK)

- Full-time:
- Part-time:
- Student-Staff (if there is or will be involvement in emergency management):

Location(s) of Offices, Facilities (note buildings only):

What is the primary mission of this Faculty or Department?

The primary contact for this plan is: _____.

The alternate contact for this plan is: _____.

2.2 Business Continuity Planning Team

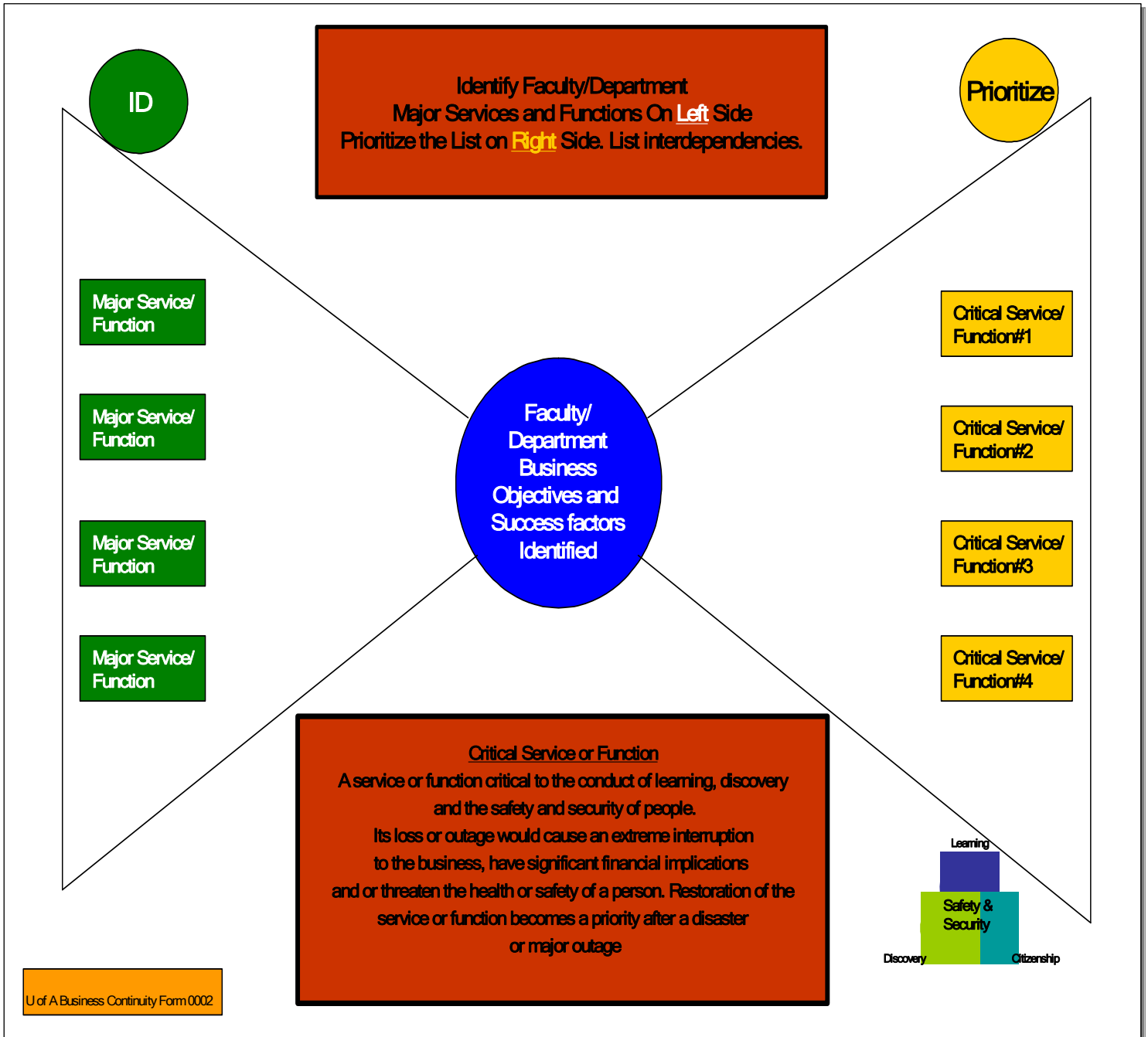
Identify the people that will put this plan together.

Key University Personnel:	Position/Title	Work Phone	Cell Phone	E-mail
Team Leader				
Team Member (Alternate Leader)				
Team Member				
Team Member				
Team Member				
Team Member				
Team Member				
Team Member				
Team Member				
Team Member				

Business Continuity Planning

2.3 Business Impact Analysis Model 1

1. Identification of Functions and Critical Services.



2. Identification of Interdependencies

Step 1 - Identify your Faculty or Department's major functions/services.

Step 2 - Determine your critical services from the list developed.

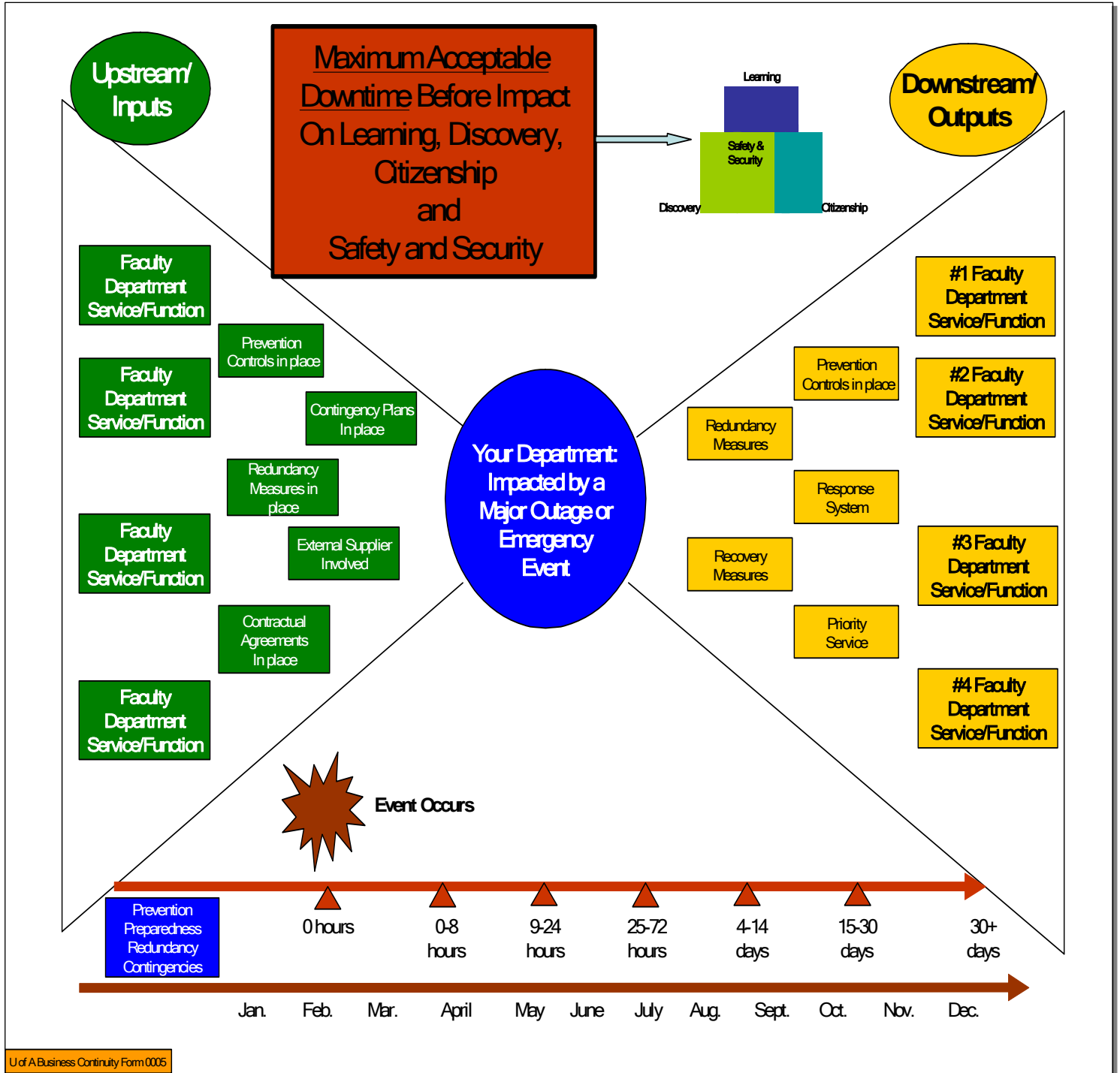
Step 3 - Prioritize (rank) your critical services.

Step 4 - List key interdependencies between faculties, departments, units and major suppliers

**Business Continuity Planning
Business Impact Analysis Model 2
Determining: Maximum Acceptable Downtime
& Restarting (RTO) Your Critical Service
Determining Critical Times**

Identifying Prevention Measures, Redundancy, Recovery and Contractual Arrangements

Determining a maximum acceptable downtime (MAD) for your critical service when an outage occurs is important in defining the negative consequences that impact the university. How long can the service be out before harmful consequences occur?



2.3.2 MAD - MAXIMUM ACCEPTABLE DOWNTIME of a SERVICE

Determining: Maximum Acceptable Downtime & restarting Your Critical Service (see Appendix B for guidance)

- o In the table below, list your critical services you identified and prioritized already. List them in priority order starting with the most important. Then check off the time area that service can be down before negative consequences occur.
- o The recovery time objective should be a shorter time period than the MAD. Identify that time.

Critical Services as ranked from Page 8	What is the MAD before negative consequences occur?						Recovery Time Objective (RTO)
	Timeline Range						
	0-8 hours	9-24 hours	25-72 hours	4-14 days	15-30 days	30 + days	When your service will be up and running again
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							

3. BUSINESS CONTINUITY PHASE 2
3.1 SOLUTIONS, STRATEGIES AND RISK ANALYSIS
Business Continuity Planning

Critical Service # 1:

MAD:

Key University Personnel:	Office Phone	Cell Phone	Home Phone	E-mail
Primary Contact:				
Alternate Contact #1:				
Alternate Contact #2:				
Contract Personnel (if important to the provision of the service):				

- Description of this critical service

- Responsible staff (key contact responsible for the provision of this service)

- **Upstream dependencies:** (What other units or systems, outside your control, have to be operational before you can perform this critical function?) (see appendix A at the end of this package for two graphs to aid you in making these decisions)

- **Downstream dependencies:** (What units or systems will be affected by failure of this critical function?)

- Peak Periods

- 1. How would you carry out this critical service if your usual **space/facility/office** was not available?
I.e. you may consider scenarios such as: your office was not accessible, your building was not accessible or your building was destroyed.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

- 2. How would you carry out this critical service if the usual **equipment or vehicles** were not available?
I.e. desk top computers, laptops, diagnostic equipment, specialized tools, delivery vehicles etc.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

- 3. How would you carry out this critical service if some **staff** were not available?

❖ **Alternate measures/contingency plans:**

1. Brainstorm here but reference and complete Appendix C for structured analysis process.

- 4. How would you carry out this critical service if **computer networks** (University network such as provide through AICT or internal department network) and **telecommunications** were not available?

NOTE: Respective IT and Telecommunications staff reference Appendix D to analyze your services to develop your contingency and recovery measures.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

- 5. How would you carry out this critical service if an **outage of utilities** occurred?
(Note: Utilities (F&O) is responsible for power, water and natural gas to the building footprint.)

❖ **Alternate measures/contingency plans:**

- Natural gas
- Water
- Electricity
- Heat/Steam
- Cooling

- 6. How would you carry out this critical service if there was a **loss of a critical vendor**?
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.

- 7. Other Critical Single Points of Failure or Show Stoppers not captured above?

- 8. Additional Risks Generated by Implementing Alternate Measures/Contingency Plans
I.e. are you adding a new hazard to the work environment through the implementation of your alternate/contingency measure?
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.

- 9. Policy Exceptions needed for Implementing Alternate Measures/Contingency Plans
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.

Critical Service # 2

MAD:

Key University Personnel:	Office Phone	Cell Phone	Home Phone	E-mail
Primary Contact:				
Alternate Contact #1:				
Alternate Contact #2:				
Contract Personnel (if important to the provision of the service):				

- Description of this critical service

- Responsible staff (key contact responsible for the provision of this service)

- **Upstream dependencies:** (What other units or systems, outside your control, have to be operational before you can perform this critical function?) (see appendix A at the end of this package for two graphs to aid you in making these decisions)

- **Downstream dependencies:** (What units or systems will be affected by failure of this critical function?)

- Peak Periods

- 1. How would you carry out this critical service if your usual **space/facility/office** was not available?
I.e. you may consider scenarios such as: your office was not accessible, your building was not accessible or your building was destroyed.
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.

- 2. How would you carry out this critical service if the usual **equipment or vehicles** were not available?
I.e. desk top computers, laptops, diagnostic equipment, specialized tools, delivery vehicles etc.
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.

➤ 3. How would you carry out this critical service if some **staff** were not available?

❖ **Alternate measures/contingency plans:**

1. **Brainstorm here but reference and complete Appendix C for structured analysis process.**

➤ 4. How would you carry out this critical service if **computer networks** (University network such as provide through AICT or internal department network) and **telecommunications** were not available?

NOTE: Respective IT and Telecommunications staff reference Appendix D to analyze your services to develop your contingency and recovery measures

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

➤ 5. How would you carry out this critical service if an **outage of utilities** occurred?

(Note: Utilities (F&O) is responsible for power, water and natural gas to the building footprint.)

❖ **Alternate measures/contingency plans:**

- Natural gas
- Water
- Electricity
- Heat/Steam
- Cooling

➤ 6. How would you carry out this critical service if there was a **loss of a critical vendor**?

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

➤ 7. Other Critical Single Points of Failure or Show Stoppers not captured above?

➤ 8. Additional Risks Generated by Implementing Alternate Measures/Contingency Plans
I.e. are you adding a new hazard to the work environment through the implementation of your alternate/contingency measure?

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

- 9. Policy Exceptions needed for Implementing Alternate Measures/Contingency Plans
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.

Critical Service # 3

MAD:

Key University Personnel:	Office Phone	Cell Phone	Home Phone	E-mail
Primary Contact:				
Alternate Contact #1:				
Alternate Contact #2:				
Contract Personnel (if important to the provision of the service):				

- Description of this critical service

- Responsible staff (key contact responsible for the provision of this service)

- **Upstream dependencies:** (What other units or systems, outside your control, have to be operational before you can perform this critical function?) (see appendix A at the end of this package for two graphs to aid you in making these decisions)

- **Downstream dependencies:** (What units or systems will be affected by failure of this critical function?)

- Peak Periods

- 1. How would you carry out this critical service if your usual **space/facility/office** was not available?
I.e. you may consider scenarios such as: your office was not accessible, your building was not accessible or your building was destroyed.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

- 2. How would you carry out this critical service if the usual **equipment or vehicles** were not available?
I.e. desk top computers, laptops, diagnostic equipment, specialized tools, delivery vehicles etc.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

- 3. How would you carry out this critical service if some **staff** were not available?

❖ **Alternate measures/contingency plans:**

1. **Brainstorm here but reference and complete Appendix C for structured analysis process.**

- 4. How would you carry out this critical service if **computer networks** (University network such as provide through AICT or internal department network) and **telecommunications** were not available?

NOTE: Respective IT and Telecommunications staff reference Appendix D to analyze your services to develop your contingency and recovery measures.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

- 5. How would you carry out this critical service if an **outage of utilities** occurred?
(Note: Utilities (F&O) is responsible for power, water and natural gas to the building footprint.)

❖ **Alternate measures/contingency plans:**

- Natural gas
- Water
- Electricity
- Heat/Steam
- Cooling

- 6. How would you carry out this critical service if there was a **loss of a critical vendor**?
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.

- 7. Other Critical Single Points of Failure or Show Stoppers not captured above?

- 8. Additional Risks Generated by Implementing Alternate Measures/Contingency Plans
 I.e. are you adding a new hazard to the work environment through the implementation of your alternate/contingency measure?
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.

- 9. Policy Exceptions needed for Implementing Alternate Measures/Contingency Plans
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.

Critical Service # 4

MAD:

Key University Personnel:	Office Phone	Cell Phone	Home Phone	E-mail
Primary Contact:				
Alternate Contact #1:				
Alternate Contact #2:				
Contract Personnel (if important to the provision of the service):				

- Description of this critical service

- Responsible staff (key contact responsible for the provision of this service)

- **Upstream dependencies:** (What other units or systems, outside your control, have to be operational before you can perform this critical function?) (see appendix A at the end of this package for two graphs to aid you in making these decisions)

- **Downstream dependencies:** (What units or systems will be affected by failure of this critical function?)

- Peak Periods

- 1. How would you carry out this critical service if your usual **space/facility/office** was not available?
I.e. you may consider scenarios such as: your office was not accessible, your building was not accessible or your building was destroyed.
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.

- 2. How would you carry out this critical service if the usual **equipment or vehicles** were not available?
I.e. desk top computers, laptops, diagnostic equipment, specialized tools, delivery vehicles etc.
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.

➤ 3. How would you carry out this critical service if some **staff** were not available?

❖ **Alternate measures/contingency plans:**

1. **Brainstorm here but reference and complete Appendix C for structured analysis process.**

➤ 4. How would you carry out this critical service if **computer networks** (University network such as provide through AICT or internal department network) and **telecommunications** were not available?

NOTE: Respective IT and Telecommunications staff reference Appendix D to analyze your services to develop your contingency and recovery measures

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

➤ 5. How would you carry out this critical service if an **outage of utilities** occurred?

(Note: Utilities (F&O) is responsible for power, water and natural gas to the building footprint.)

❖ **Alternate measures/contingency plans:**

- Natural gas
- Water
- Electricity
- Heat/Steam
- Cooling

➤ 6. How would you carry out this critical service if there was a **loss of a critical vendor**?

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

➤ 7. Other Critical Single Points of Failure or Show Stoppers not captured above?

➤ 8. Additional Risks Generated by Implementing Alternate Measures/Contingency Plans
I.e. are you adding a new hazard to the work environment through the implementation of your alternate/contingency measure?

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

- 9. Policy Exceptions needed for Implementing Alternate Measures/Contingency Plans
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.

Critical Service # 5

MAD:

Key University Personnel:	Office Phone	Cell Phone	Home Phone	E-mail
Primary Contact:				
Alternate Contact #1:				
Alternate Contact #2:				
Contract Personnel (if important to the provision of the service):				

- Description of this critical service

- Responsible staff (key contact responsible for the provision of this service)

- **Upstream dependencies:** (What other units or systems, outside your control, have to be operational before you can perform this critical function?) (see appendix A at the end of this package for two graphs to aid you in making these decisions)

- **Downstream dependencies:** (What units or systems will be affected by failure of this critical function?)

- Peak Periods

- 1. How would you carry out this critical service if your usual **space/facility/office** was not available?
I.e. you may consider scenarios such as: your office was not accessible, your building was not accessible or your building was destroyed.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

- 2. How would you carry out this critical service if the usual **equipment or vehicles** were not available?
I.e. desk top computers, laptops, diagnostic equipment, specialized tools, delivery vehicles etc.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

- 3. How would you carry out this critical service if some **staff** were not available?

❖ **Alternate measures/contingency plans:**

1. **Brainstorm here but reference and complete Appendix C for structured analysis process.**

- 4. How would you carry out this critical service if **computer networks** (University network such as provide through AICT or internal department network) and **telecommunications** were not available?

NOTE: Respective IT and Telecommunications staff reference Appendix D to analyze your services to develop your contingency and recovery measures.

❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

- 5. How would you carry out this critical service if an **outage of utilities** occurred?
(Note: Utilities (F&O) is responsible for power, water and natural gas to the building footprint.)

❖ **Alternate measures/contingency plans:**

- Natural gas
- Water
- Electricity
- Heat/Steam
- Cooling

- 6. How would you carry out this critical service if there was a **loss of a critical vendor**?
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.
- 7. Other Critical Single Points of Failure or Show Stoppers not captured above?
- 8. Additional Risks Generated by Implementing Alternate Measures/Contingency Plans
I.e. are you adding a new hazard to the work environment through the implementation of your alternate/contingency measure?
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
- 9. Policy Exceptions needed for Implementing Alternate Measures/Contingency Plans
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.

Critical Service # 6

MAD:

Key University Personnel:	Office Phone	Cell Phone	Home Phone	E-mail
Primary Contact:				
Alternate Contact #1:				
Alternate Contact #2:				
Contract Personnel (if important to the provision of the service):				

- Description of this critical service

- Responsible staff (key contact responsible for the provision of this service)

- **Upstream dependencies:** (What other units or systems, outside your control, have to be operational before you can perform this critical function?) (see appendix A at the end of this package for two graphs to aid you in making these decisions)

- **Downstream dependencies:** (What units or systems will be affected by failure of this critical function?)

- **Peak Periods**

- 1. How would you carry out this critical service if your usual **space/facility/office** was not available?
I.e. you may consider scenarios such as: your office was not accessible, your building was not accessible or your building was destroyed.
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.

- 2. How would you carry out this critical service if the usual **equipment or vehicles** were not available?
I.e. desk top computers, laptops, diagnostic equipment, specialized tools, delivery vehicles etc.
 - ❖ **Alternate measures/contingency plans:**
 - 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.

- 3. How would you carry out this critical service if some **staff** were not available?
 - ❖ **Alternate measures/contingency plans:**
 1. Brainstorm here but reference and complete Appendix C for structured analysis process.

- 4. How would you carry out this critical service if **computer networks** (University network such as provide through AICT or internal department network) and **telecommunications** were not available?

NOTE: Respective IT and Telecommunications staff reference Appendix D to analyze your services to develop your contingency and recovery measures.

- ❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

- 5. How would you carry out this critical service if an **outage of utilities** occurred?

(Note: Utilities (F&O) is responsible for power, water and natural gas to the building footprint.)

- ❖ **Alternate measures/contingency plans:**

- Natural gas
- Water
- Electricity
- Heat/Steam
- Cooling

- 6. How would you carry out this critical service if there was a **loss of a critical vendor**?

- ❖ **Alternate measures/contingency plans:**

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

- 7. Other Critical Single Points of Failure or Show Stoppers not captured above?

- 8. Additional Risks Generated by Implementing Alternate Measures/Contingency Plans
I.e. are you adding a new hazard to the work environment through the implementation of your alternate/contingency measure?

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

- 9. Policy Exceptions needed for Implementing Alternate Measures/Contingency Plans

- 1.
- 2.
- 3.
- 4.
- 5.

3.2 Identifying Hazards, Ranking Risks and Determining Vulnerabilities

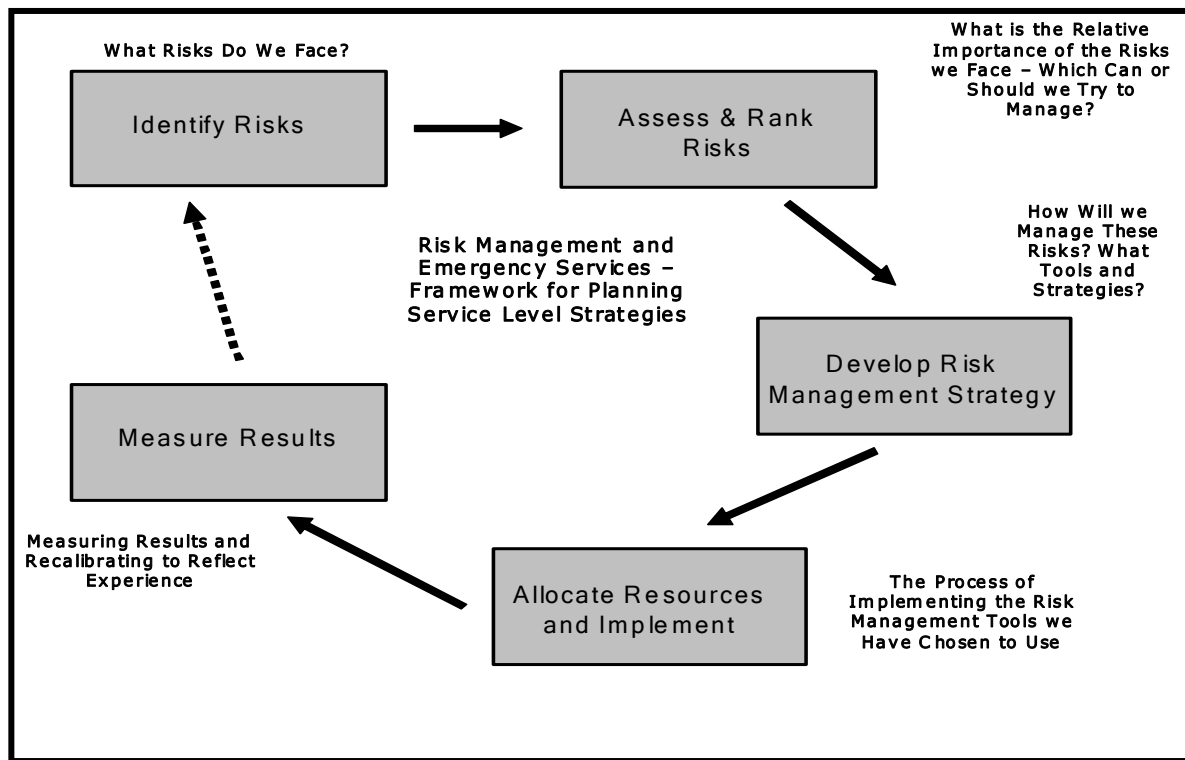
Hazard Identification, Risk Assessment, Vulnerabilities and Emergency Management

Introduction

Best practice indicates that to be as ready as reasonably practical to manage potential emergencies, an organization must identify, analyze and assess the potential hazards and risks it faces. Risk assessment is recognized as a critical component of an emergency management program. The outcomes of a risk assessment are used as the basis for decision making related to the risk appetite of the organization and the measures taken to deal with residual risk i.e. the risk that cannot be eliminated and is inherent to operating the business.

The risk analysis and assessment process produces the risk profile for the organization. The risk profile will assist the organization in development risk treatment and emergency management programs. The outcomes of the plans are designed to eliminate, reduce, mitigate, control, transfer the risk and have plans in place to deal with emergency conditions.

Diagram 1: A Risk Management Process



The risk assessment process produces the risk profile for the organization. The risk profile will assist the organization in development the risk treatment plans. The outcomes of the plans are designed to eliminate, reduce, mitigate, control or transfer the risk.

Purpose

The purpose of identifying hazards, analyzing and assessing risk within the integrated emergency management program is to assist in developing hazard specific emergency management plans that will be included in the Emergency Operations Plan (EOP) section of the faculty or department program. Examples of plans that will be included in the EOP include: evacuation plans, bomb threat plans, chemical spill/release plans and a medical response plan.

The hazard identification and risk assessment process aligns the University's Integrated Emergency Management Program (IEMP) with Standards in the emergency management industry. This process meets the intent of Chapter 5, Section 5.3 "Risk Assessment" of the National Fire Protection Association 1600: Standard on Disaster/Emergency Management and Business Continuity Programs.

Risk can be the result of surprises, of bad planning, no planning or simply no action.

Embedded in the IEMP is the concept of an "all hazards approach" to emergency management. The all hazards approach includes features such as: coordinated emergency management systems, collaboration with external response agencies and partners, consistent command and control structures and common language regardless of the type of emergency. The all hazards approach will produce emergency management plans that address the hazards and potential emergencies that may be expected but at the same time remain flexible to adapt to the unknown.

Risk and Emergency Management Terminology for Identification and Assessment Process

To best approach the process of hazard identification, risk analysis and assessment a set of common terms and definitions is a requirement.

What is Risk Assessment

Risk assessment is the process of evaluating risk and applying risk estimates to decide on management strategies and actions.

Hazard

A condition, material, work process or situation with the potential for causing an undesirable consequence such as harm to people, animals and the environment. The hazard has the potential to cause loss.

Example: Gasoline is a hazard if mishandled and of sufficient quantity and ignition occurs can cause injury and damage to people, property and the environment.

Hazards can be grouped under broad based terms that assist with risk assessment for a particular institution or a segment of the institution. For example:

- ◆ Natural Hazards can include: Tornado, Drought, Flood, Ice Storm, Earthquake
- ◆ Technical hazards can include: Utility failure such as loss of electricity, Telecommunications failure, IT failure, Structural failure/collapse, fire alarm system failure, hazardous material spill/release
- ◆ Human Related Hazards can include: Arson, Robbery, Violent acts, Medical emergency/Public Health Emergency, Sabotage, Acts of Terrorism
- ◆ Financial hazards can include: Loss of revenue, Loss of government funding, Substantial fines or legal action

Hazardous Incident

An undesired and unplanned event that results in injuries to people, damage to property, harm to the environment and an interruption to the delivery of critical services.

Example: The sudden failure of a propane storage tank resulting in a release of propane to the environment and/or an ignition of the propane.

Risk

A measure of the probability and severity of adverse effects of the undesired or unplanned event. The chance of something happening that will have an impact upon the institutions services and objectives. As related to emergency management risk is used to describe the likely potential of harmful consequences and negative impacts resulting from a hazard in or around the University and the interaction with people, structures, the environment and services.

Example: The chance (probability) of being killed (severity) in an automobile accident.

Probability

A measure of how likely it is that an event will occur during some period of time or other defined parameter.

Example: The chances of winning a lottery are described as a probability e.g. 1 in a million chances of winning the big prize.

Severity

Severity is a measure of how serious the adverse effects or consequences of the event are. How bad can it be?

Example:

An accident can produce two commonly referred to degrees of severity: a fatality or an injury.

Consequence

The main outcome(s) of the event associated with the hazard

Example: The sudden failure of a propane tank causes a release of propane to the atmosphere that ignites in an explosion that injures people and causes property damage.

Adverse Effects

The potential for risk to produce an emergency condition can produce a variety of adverse effects such as:

- Health and safety impacts on people and/or animals
- Property damage
- Environmental harm
- Economic loss
- Damage to reputation
- Business interruptions

Risk Analysis

The estimation of the risk measures describing the chance of an undesired event occurring and the severity of its consequences.

Risk Mitigation

The reduction of risk through measures that reduce the probability and severity of a potential undesired event. The measures taken to prepare for residual risk related to operations of the business.

Example: Fire evacuation plans.

University and Risks

- Risk of fire
- Risk of death and injuries
- Risk of crime and disorder
- Risk of terrorism
- Risk to water supplies
- Risk to hazardous waste disposal
- Risk of vehicle accidents
- Risk of hazards on roads, streets, in parks
- Risk to critical infrastructure
- Risk to reputation
- Risk of market failure
- Risk of politics

Accepting a defined level of risk means that your organization has implemented policies and procedures for assessing, evaluating, monitoring and reporting risk.

It also means that your organization can react rapidly to dynamic change in risk, recognize unacceptable levels and respond to reduce the exposure.

Risk Management

The policies, procedures and practices applied to analyze, assess and control risk.

Risk Control

The minimization of risk exposure through the implementation of risk mitigation measures or delegation of liability.

Emergency

An event or condition that is real or imminent which threatens or imperils the health, safety and security of people, can cause damage to buildings and structures, can harm the environment, disrupt critical or essential services at the University and negatively impact the institution's reputation.

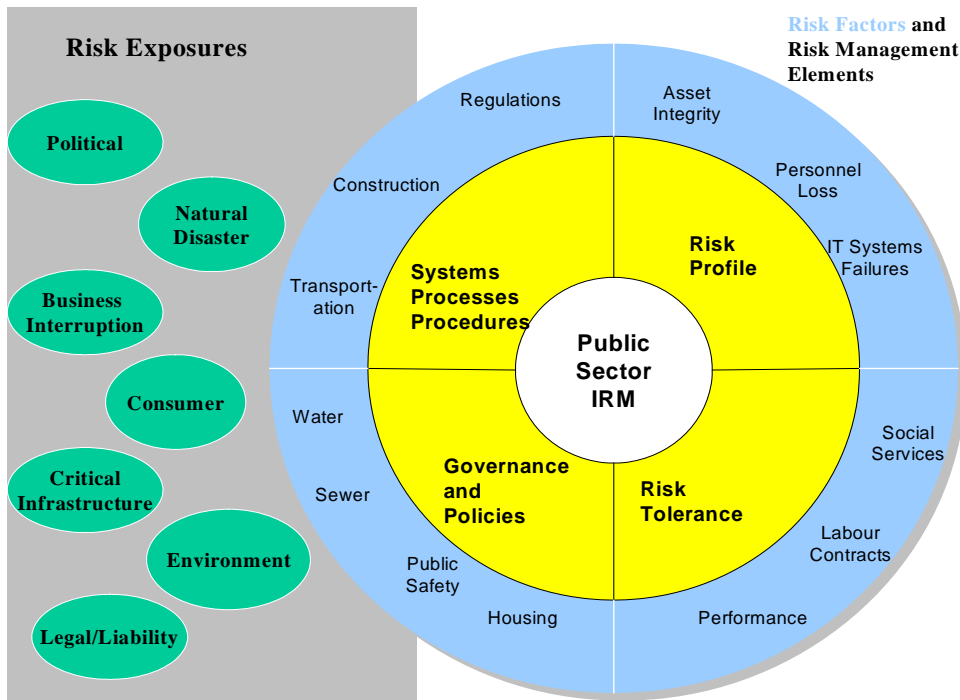
Emergency Management

The activation of response teams, the execution of protocols, implementation of contingency measures, application of a command and control system and recovery actions to manage risks to the University.

Event

A condition, situation or incident that occurs on or near the University during a period of time that results in some form of response by the University

Diagram 2: Risk Exposures, Risk Factors, Risk Management



Process for Identification and Risk Assessment

Identifying and assessing risk is a key element of the emergency management program for the University. Through the identification and assessment process, areas of vulnerability that could lead to potential losses to people, property, the environment or negative impacts on the operation of the leisure center will be highlighted. Prevention measures, mitigation actions and contingency plans will be identified in the section including the risk treatment plans.

The goal is the development of a risk profile for the University using a simple five-step process for identification and assessment of risks. An outcome of the assessment is the ranking of the risks identified i.e. prioritization of the risks such that mitigation measures can be developed and implemented. *The five-step process that follows includes examples related to each step that act as a training component of the program for hazard identification and risk assessment.*

3.2 Determining Risks and Vulnerabilities

Hazard Identification, Risk Assessment and Vulnerability Analysis Steps

A five step process to analyze and rank the risks to your faculty/department/unit is provided. Examples related to each step in the risk analysis process are included.

Step 1

Column 1 in the following table lists the potential natural, human made, technical and financial hazards that could result in major emergencies, disasters or business interruptions that could negatively impact the University.

This table is meant to be flexible and adaptable to your department/faculty or unit. If you want to add other specific risks please just add to the list in the pertinent sector. If you are filling this out electronically it is recommended that you print pages 35-38 to help you fill out the table, it will simplify the process greatly when doing so.

Column 1 Major Emergency, Disaster Sector	Column 2 Probability	Column 3 Severity	Column 4 Risk level	Column 5 Ranking
Natural				
Wild Fire				
Flood				
Cold Wave				
Ice Storm				
Severe Storm Rain/Snow				
Tornado				
Earthquake				
Lightning				
Heat Wave/Drought				

Technical				
Utilities Failure i.e. water, natural gas, power, steam, waste removal				
Telecommunications System Failure				
IT Infrastructure Disruption i.e. virus, loss of network, loss of equipment				
Critical equipment failure				
IT Security Breach/Theft				
Flooding (Internal)				
Structure Fire/Explosion				
Structural Collapse				
Hazardous Material Release/Spill				
Aircraft Crash on University				
New risk not listed in template: (please add here)				
New risk not listed in template: (please add here)				
Human Related				
Sabotage i.e. deliberate act to disrupt a system, a program, an application or other work process,				
Arson (criminal activity)				
Labour Interruption i.e. work stoppage, deliberate slow down, strike				
Riot/Civil/Sports Event Disruption				
Public Health Event i.e. flu pandemic, outbreak of norovirus, meningitis				
Workplace Violence (internal source)				
Violent Act (from external source)				

Loss of Senior Management				
Transportation Event (e.g. bus accident, heavy equipment vehicle accident, pipeline breach other)				
Theft of assets e.g. robbery, fraud, stolen property other,				
Act of Industrial espionage				
Terrorism				
Bomb Threat				
Suspicious Package (received at the university)				
Active Shooter on campus				
Animal/Crop Vandalism/Disruption/Release/Contamination				
Hostage Taking Event				
Bioterrorism Event				
Protester/Activist Action Involving violence				
Financial				
Loss of Government Funding				
Loss of Research Funding				
Loss of Student Revenue				
Loss of Asset				
Legal Action/Fines				
Institutional Reputation				
Bad Media Press				
Community outrage				
Student outrage				

Step 2 - Working Through Column 2

Use the Probability Matrix below to determine the probability of occurrence for each of the potential hazards and risks identified in column 1 that could impact the University. One method of assessment involves the referencing of any historical records of events that have occurred at the University or in the region having the potential to impact the facility. Remember this is your subjective qualitative sense regarding risk assessment.

Probability Matrix

Probability	
Descriptive Word	Definition
Frequent	Likely to occur repeatedly
Probable	Likely to occur several times
Occasional	Likely to occur sometime
Remote	Not likely to occur
Improbable	Probability of occurrence is extremely remote

As you examine the potential emergency that could occur assess the probability of the event occurring and insert the descriptive word in of your working table.

Example: Table with Column 2 Completed

Based on the Probability Matrix Column 2 has been completed in the table below.

Column 1 Major Emergency, Disaster Sector	Column 2 Probability	Column 3 Severity	Column 4 Risk level	Column 5 Ranking
Natural				
Fire	Probable			
Tornado	Occasional			
Technical				
Burst water pipe	Occasional			
Man made				
Riot	Remote			
Financial				
Legal action/fines	Improbable			

Step 3 - Working Through Column 3

Use the Severity Matrix below to identify the probable consequences of each hazard that could result in an emergency event that could impact your operations. Select the most accurate severity level (catastrophic, critical, marginal or negligible) and record in Column 3.

Severity Matrix

SEVERITY LEVEL	Human Impact	Impact on Animals/Research Specimens	Property Damage	Environmental Impact	Reputation Damage	Financial Impact	Non Compliance (with legislation, policy, procedure)
CATASTROPHIC	Fatalities involved. Very large number of people affected. Multiple serious injuries. Loss of some key staff for more than 1 week.	Extensive loss of animals. Long term research lost. Specimens not recoverable.	Extensive damage to structures and infrastructures . Widespread displacement of people (>500)	Serious long term impact on environment with some permanent damage	Serious damage to University reputation. Extensive adverse comments on campus. Media relentless in damaging reports.	Serious impact on University economics. Financial loss in excess of \$10 million	Extensive legal action against the University involving, criminal and civil litigation. Government inquiry called. Senior executives impacted.
CRITICAL	Potential fatalities. Significant number of people affected. Multiple injuries. Temporary loss of some key staff for more than 1 day.	Significant impact on animal health and welfare and research projects. Some specimens at risk of loss.	Significant damage to structures and/or infrastructure. Some people displaced (<500)	Significant impact on environment with medium to long term effects	Significant adverse comments on campus. Significant interest from external media. Press comments negative and harmful to University reputation	Significant impact on University economics. Financial loss between \$1 - \$10 million	Limited legal action against the University related to breach of contractual obligations or applicable acts and regulations.
MARGINAL	No fatalities. Small number of people affected. Small number of minor injuries. Some key staff unavailable for a few hours	Limited impact on animal health and welfare and research specimens. Some disruption to animal and specimen research but no significant losses	Damage is confined to a specific location. Infrastructure not impacted. Localized displacement (<100)	Limited impact on environment with some short term and long term effects	Some adverse comments on campus. Limited interest from external media	Limited impact on University economics. Financial loss between \$100k - \$1 million	Internal investigation relate to non compliance with University policies and procedures.
NEGLIGIBLE	Insignificant injuries or impact on human health	Insignificant impact on animal health and specimens	Insignificant impact on structures or infrastructure	Insignificant impact on the environment	Internal to Faculty or Department only	Insignificant impact on University economics. Financial loss of <\$100k	Internal investigation at faculty or department level applicable to non compliance with policies and procedures.

Example: Table Column 3 Completed

Based on the Severity Matrix Column 3 has been completed in the table below.

Column 1 Major Emergency, Disaster Sector	Column 2 Probability	Column 3 Severity	Column 4 Risk level	Column 5 Ranking
Natural				
Fire	Probable	Catastrophic		
Tornado	Remote	Catastrophic		
Technical				
Burst water pipe	Occasional	Critical		
Man made				
Riot	Remote	Marginal		
Financial				
Legal action/fines	Improbable	Negligible		

Step 4 Working Through Column 4

The Risk Matrix below highlights the areas for determining low, medium and high risk with respect to the hazards, risk and potential events that you analyzed thus far. Place each event that you analyzed in Column 1 above in the appropriate cell in the matrix based on cross referencing the probability and severity assessments you determined above in Columns 2 and 3.

Risk Assessment Matrix

Risk Levels					
Probability / Severity	Frequent	Probable	Occasional	Remote	Improbable
Catastrophic	High Risk	High Risk	High Risk	Medium Risk	Low Risk
Critical	High Risk	High Risk	Medium Risk	Low Risk	Low Risk
Marginal	Medium Risk	Medium Risk	Low Risk	Low Risk	Low Risk
Negligible	Low Risk	Low Risk	Low Risk	Low Risk	Low Risk



Example: Table Column 4 Completed

Based on the Risk Matrix and the information from Columns 2&3, find the correct risk level for each event.

Risk Levels					
Probability / Severity	Frequent	Probable	Occasional	Remote	Improbable
Catastrophic		Fire		Tornado	
Critical			Burst Water Pipe		
Marginal				Riot	
Negligible					Legal action/fines

Step 5 Working Through Column 5 and Ranking the Risks

Now prioritize each event according to the risk level. The greatest priority should be given to the risk events with the highest level.

Example Table (This is what a finished assessment should look like)

Column 1 Major Emergency, Disaster Sector	Column 2 Probability	Column 3 Severity	Column 4 Risk level	Column 5 Ranking
Natural				
Tornado	Occasional	Catastrophic	Medium	2
Fire	Probable	Catastrophic	High	1
Technical				
Burst water pipe	Occasional	Marginal	Medium	3
Man made				
Riot	Remote	Marginal	Low	4
Financial				
Legal action/fines	Improbable	Negligible	Low	5

3.2.1 Next Step: Mitigation/Counter Measures/Alternate measures and Vulnerability Identification for Risk Treatment and Action Plan

1. Take the top risks that you identified in the previous process and list them in this chart from highest to lowest ranked.
2. Analyze each one of those risks based on the set of questions in the columns below.
3. Determine vulnerability if any
4. Determine action plan to mitigate or eliminate the risk

<p>Key Risks identified and ranked in this column.</p> <p>I.e. Start with the number 1 risk identified. Try to list a minimum of 5 - 10</p>	<p>Do you have alternate measure/ mitigation/contingency plan in place already to manage the risk</p> <p>If Yes? Briefly Identify</p> <p>If No? Identify vulnerability in next column</p>	<p>Vulnerability Identified. Provide some details. i.e. Computer servers may be damaged due to water (leak/spill/breach of pipe), evacuation plan needed</p>	<p>What can be done today at little or no cost to reduce the risk?</p>	<p>Need a longer term action PLAN to mitigate or eliminate the risk. (Include projected costs where you can for implementation).</p>
1.				
2				
3.				
4.				
5.				
6.				
7.				
8.				
9.				

The following three sections are designed to capture critical information needed and related to lists of Key Personnel/Vendors/Contractors.

3.3 Contact Lists for Personnel

Section 1 asks you to list the key department/faculty/unit personnel you would need to have access to in the event of a major outage or emergency impacting your services. The list begins with your faculty/department/unit then extends to other university faculties/departments/units on main campus followed by key contacts at other university campus locations.

Section 2 initiates the list of external resources required in support of a response, recovery and resumption of department/faculty critical services and functions. Key vendors, suppliers and contractors should be identified.

Section 3 provides the means to list the major resources you will need to apply your contingency measures and alternate means of continuing to deliver your critical services.

The information on the lists will form a section in your faculty/department/unit action plan that will be accessed in the event of a major outage or emergency impacting the University. Ensuring that your lists are as complete as possible, having them accessible to key staff and maintaining them in as current form as possible will be keys to a timely, efficient and effective response and recovery.

Section 1 University/Institution Personnel

1.Key Department/Faculty Personnel (Name)	Position	Work Phone	Cell Phone	Home Phone	E-mail
2. Key Department/Staff in Other U of A Departments/Faculty					

3. Key Department/Staff at other University/College Campuses					

Section 2 External Contacts to the U of A

Name	Vendor/Institution	Work Phone	Cell Phone	Home Phone	E-mail

3.4 Resources: Equipment, Facility/Workspace, Vehicles and Specialized Needs

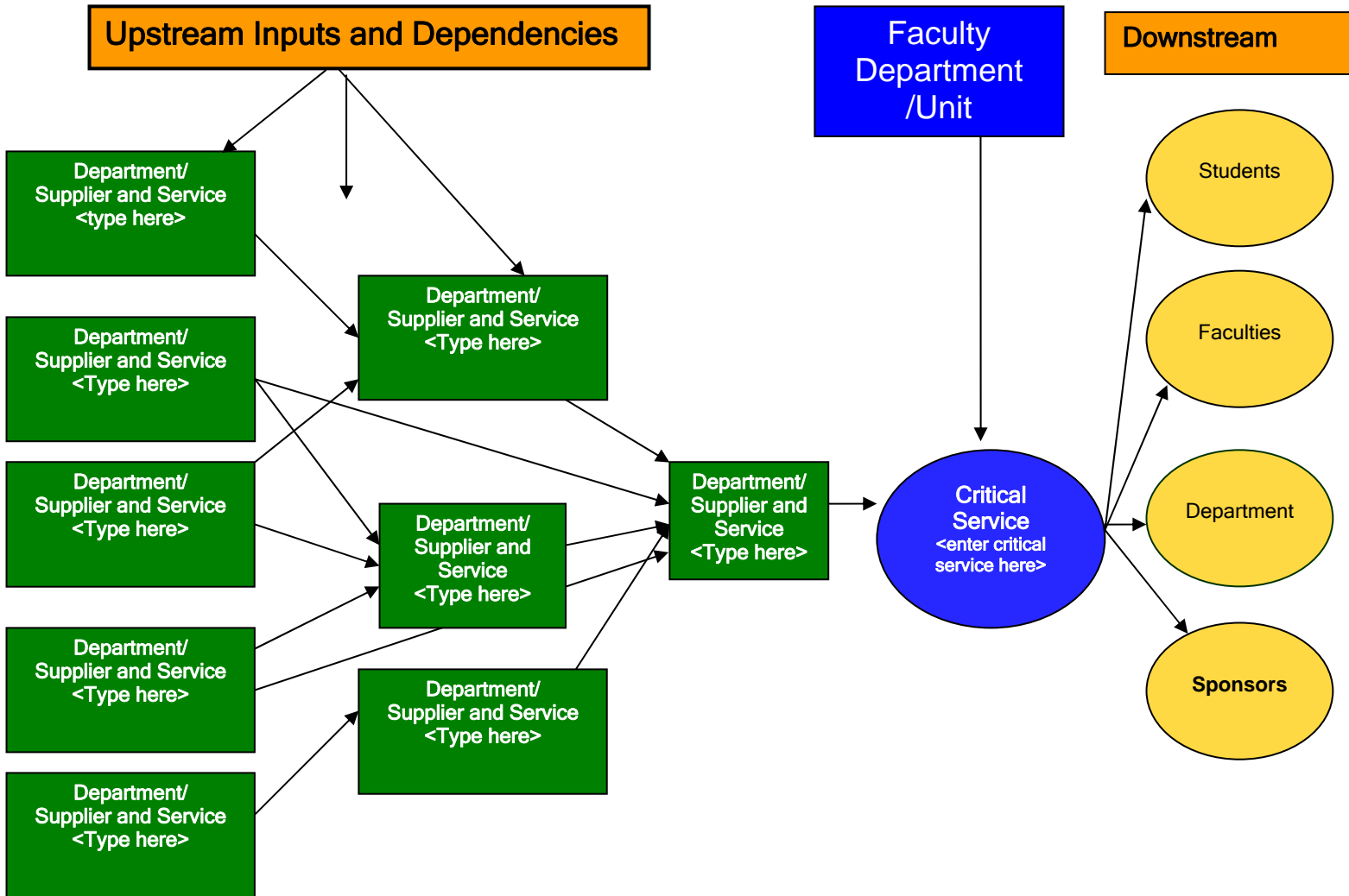
List the minimum resources needed to support your alternative measures for the critical services recorded in your plan. Please list major items only. At this time do not list consumables such as paper, inks etc. Estimate your needs.

Resource Item/Unit	Amount Required. Number of individual items needed to enable you to get your services up and running again	In stock and on site? The needed materials and equipment are available on campus.	Location of Delivery. Where on or off campus would you require the materials and equipment to be set up?	Time Constraints for Recovery e.g. Must have the computers set up within 4 hours	Required from off site Contact/Vendor? If yes, list the vendors' name. The contact information should be listed on the previous page in the External Contacts section.
Sample:	2	Yes or No answer	TBD	24 hour MAD Time	Grand & Toy
Workstations (includes desktop, computer, network connection, table, chair)			To be determined at time of emergency based on which of your alternate locations are available		
Laptop computer and charger.					
Telephone (hardwired)					
Cell phone					
Printer					
Fax					

Resource Item/Unit	Amount Required. Number of individual items needed to enable you to get your services up and running again	In stock and on site? The needed materials and equipment are available on campus.	Location of Delivery. Where on or off campus would you require the materials and equipment to be set up?	Time Constraints for Recovery e.g. Must have the computers set up within 4 hours	Required from off site Contact/Vendor? If yes, list the vendors' name. The contact information should be listed on the previous page in the External Contacts section.
Copier			To be determined at time of emergency based on which of your alternate locations are available.		
Scanner					
Other Equipment, Vehicles, Specialized Needs (List)					
Server					
Buildings/Structure					

Appendix A

Simple Slide of Upstream and Downstream Interdependencies



APPENDIX B - Optional Work
(Reference tool only if difficult to determine MAD)
MAD - MAXIMUM ACCEPTABLE DOWNTIME of a SERVICE

**Determining: Maximum Acceptable Downtime
& Restarting Your Critical Service**

- If you are having difficulty deciding how long your critical service can be down for look at the table below, check off the areas that are impacted by an outage of your service over time.
- The recovery time objective should be a shorter time period than the MAD.

Potential negative consequences	What is the MAD before negative consequences occur?						Recovery Time Objective (RTO)
	0-8 hours	9-24 hours	25-72 hours	4-14 days	15-30 days	30 + days	
Disruption of learning/teaching							
Disruption of discovery/research							
Health and safety of faculty and staff							
Health and safety of students, contractors, visitors							
Loss of faculty							
Loss of staff							
Loss of students							
Payment deadlines not met							
Loss of revenue							
Legal ramifications							
Regulatory non compliance							
Damage to University reputation							
Substantial impact on external relationship							
Impact on other University departments							

Appendix C - Business Continuity Workbook

MAJOR HEALTH EMERGENCY BUSINESS CONTINUITY PLANNING

This is a subset plan that compliments our overall Business Continuity Planning workbook. There is a high probability that material from the first part of the workbook can be cut and pasted into this sub workbook or “same as” phrase inserted into the blanks in some cases. This subset plan focuses on staff and asks you to determine essential services. The last section of this subset asks you to think about the coordination of International Business as it relates to our responsibilities.

1. Department Information

<p>Name of Faculty, Department (or Sub Unit within a Department)</p> <p>Primary Contact for this plan:</p> <p>Alternate contact for this plan:</p>
--

2. Capacity and Business Impact Analysis

This matrix is designed to capture how your faculty/department will continue to provide critical services and functions with the threat of diminishing human resource capacity as the pandemic influenza impacts the University. By completing the matrix a faculty or department will be in a position to highlight the:

- alternative methods or measures that can be implemented to continue delivering critical services;
- the other departments that you depend on in order to deliver your critical services;
- any arrangement you have made with the other university departments;
- contractual arrangement you have developed; inventory requirements you see to maintain services;
- equipment you will need, from whom and when.

This process should assist faculties and departments in determining essential personnel required to accomplish the critical services and functions. Through the analysis you may be required to examine work flow processes especially when highlighting dependencies.

List your critical services and functions necessary during the following capacity range scenarios based on the impact on people.	List the personnel that perform the critical service. (Primary and designated alternates). This may be the same as in the workbook	Based on the diminishing % of staff and capacity are there alternate methods or measures you can implement for the continued delivery of the critical service?	What other faculties or departments are critical to you to continue to deliver this critical service? Have you made any arrangements with the identified faculties or departments?	Are there contractual arrangements for the delivery of the critical service that you need to identify and consider when capacity is diminishing?	What are the essential inventory requirements, equipment needs or other resources necessary to deliver this critical service? You must have these key support items to perform the service	Any additional information pertinent to the delivery of the critical service that you should record
Scenario 1 - You are operating at 75% - 100% capacity						
Critical Service 1						
Critical Service 2						
Critical Service 3						
Critical Service 4						
Critical Service 5						
Critical Service 6						

Scenario 2 - You are operating at 50-74% capacity	List the personnel that perform the critical service. (Primary and designated alternates). This may be the same as in the workbook	Based on the diminishing % of staff and capacity are there alternate methods or measures you can implement for the continued delivery of the critical service?	What other faculties or departments are critical to you to continue to deliver this critical service? Have you made any arrangements with the identified faculties or departments?	Are there contractual arrangements for the delivery of the critical service that you need to identify and consider when capacity is diminishing?	What are the essential inventory requirements, equipment needs or other resources necessary to deliver this critical service? You must have these key support items to perform the service	Any additional information pertinent to the delivery of the critical service that you should record
Critical Service 1						
Critical Service 2						
Critical Service 3						
Critical Service 4						
Critical Service 5						
Critical Service 6						

Scenario 3 - You are operating at 25-49% capacity	List the personnel that perform the critical service. (Primary and designated alternates). This may be the same as in the workbook	Based on the diminishing % of staff and capacity are there alternate methods or measures you can implement for the continued delivery of the critical service?	What other faculties or departments are critical to you to continue to deliver this critical service? Have you made any arrangements with the identified faculties or departments?	Are there contractual arrangements for the delivery of the critical service that you need to identify and consider when capacity is diminishing?	What are the essential inventory requirements, equipment needs or other resources necessary to deliver this critical service? You must have these key support items to perform the service	Any additional information pertinent to the delivery of the critical service that you should record
Critical Service 1						
Critical Service 2						
Critical Service 3						
Critical Service 4						
Critical Service 5						
Critical Service 6						

Scenario 4 - From your original list itemize the critical services that could be deferred for a two week period without severe negative consequences						
Critical Service						
Critical Service						
Critical Service						
Critical Service						
Critical Service						
Scenario 6 - Worst case scenario impact and the University is declared <u>closed</u>. Essential services must be accomplished e.g. Heating plant, security, safety, care for animals.	Identify any of your critical services that are deemed to be an essential service that must be provided in the event the University closes due to a health emergency	Number of personnel required to deliver the identified essential services				
Essential Service 1						
Essential Service 2						
Essential Service 3						

3. Additional Planning Information

Faculty, Department or Portfolio Organization Chain of Command, Pandemic Planning Workgroup and Communications Contact

1. Organizational chain of command for faculty or department Name	Position i.e. Faculty or Department Leader in the event of a major health emergency follow by a hierarchical chain of command	Work Phone	Cell Phone	Home Phone	E-mail	Text Messaging Capability? Yes/No	Computer connectivity at home or other location?	Ability To Work from Home
2. Pandemic Planning Workgroup Names								
3. Communications contact for	Position i.e. Faculty	Work	Cell	Home	E-mail	Text	Computer	Ability To

the faculty, department or portfolio Name	or Department Leader in the event of a major health emergency follow by a hierarchical chain of command	Phone	Phone	Phone		Messaging Capability? Yes/No	connectivity at home or other location?	Work from Home
Primary:								
Alternate:								
4. Faculty/Department - Emergency Contact List. The staff that will get notified and called out in the event of an emergency.								

4. Question Sets to Prompt Planning and Development

Additional Faculty/Department Information Important For Emergency Preparedness and Business Continuity

Question Set 4.1: List of Personnel, Contacting Your Personnel, Personnel on Call					
Do you maintain an updated list of faculty/department personnel including work phone, cell phone, email, office etc.? Yes or No	If yes, where is the list kept? E.g. office desk or office desk with copy off site	Do you have a position designated to ensure updates to the personnel lists are completed?	Does your faculty/department have a method for rapidly contacting all personnel on your list to provide critical information? E.g. Page out system, automatic dialer...	What is your method of communicating with: <ul style="list-style-type: none"> • Faculty • Staff • Students • Inter- faculty • Inter-department In the event of an emergency?	Do you have an emergency on call method completed with designated positions in the event of an emergency event in your faculty/department?
Question Set 4.2: Recording Absences, Critical Inventory List, List of vendors and Suppliers, List of Key Partners or Sponsors, List of Key Government Contacts					
Do you record employee (and/or student as applicable) absences on a daily basis?	Who retains the absence records in your faculty/department?	Do you have a readily available and accurate list of critical inventory and supplies on hand?	Do you have readily available an accurate list of vendors and suppliers of critical resources in the event of a disaster or major outage of services?	Who are your Key Partners or Sponsors that you would need to call in the event of a major emergency?	Who are the Key Government Contacts you would need to call?

**Question Set 4.3:
Business Related to International Activities and Faculty, Staff and Students Across U of A**

<p>Do you maintain an updated list of all faculty, staff or students traveling or working abroad on programs managed by your Faculty?</p> <p>Who retains and maintains the list and do you have a means of quickly accessing the list?</p> <p>Note: Check with U of A EAP centrally managed program</p>	<p>Do you check travel advisories prior to faculty, staff or students leaving for international travel?</p> <p>Do you monitor the travel advisories while you have people abroad?</p> <p>Or, do you rely on a University centralized function for managing travel advisories?</p>	<p>Do you have any employees/students working abroad on programs managed or directed by your unit or Faculty?</p> <p>If yes how do you maintain contact with them? How would you get an emergency message to them?</p>	<p>Do you have any employees/students who travel internationally?</p> <p>If yes how do you maintain contact with them? How would you get an emergency message to them?</p>	<p>Who are your Key Partners, Sponsors or Universities that you would need to call in the event of a major emergency?</p> <p>Do you have a current list?</p>	<p>Who are the Key Government contacts you would need to call?</p>
<p>Do you collect, from the faculty, staff or student a list of family contacts when they are traveling on University sponsored business or working abroad?</p> <p>If not, is the information captured through some other department?</p>	<p>Who retains this list and do you have a means of quickly accessing the information?</p>	<p>Do you have clear policies developed for authorizing and monitoring faculty, staff or students when they are abroad?</p>	<p>Do you develop contingency plans in the event that you had to evacuate or recall your faculty, staff or student from the involved international country?</p>	<p>Do you have plans in place for dealing with international guests, faculty or students who may be working within your faculty at the U of A?</p> <p>Do you ensure the international guest (faculty member or student) is registered within the U of A employee records system?</p>	<p>Do you contact the U of A, Risk Management Office to verify insurance coverage or do you contact other insurance agencies when Faculty, staff or students travel or work abroad?</p> <p>Prior to travel occurring is insurance coverage verified and communicated to the faculty, staff or students traveling/working abroad?</p>

Appendix D - Business Continuity Planning Workbook

Vital Records, Information Technology and Telecommunications

Purpose and Goal

The University is highly dependant on information technology and telecommunications to provide the critical services that support the core businesses of learning, discovery, citizenship and health safety and security.

- ◆ The purpose of this template is to provide guidance for the IT staff in a faculty or department in analyzing and assessing their current state with respect to business continuity and disaster response and recovery.
- ◆ Using the question prompts in the template the IT staff can fill in the blanks and use the outcomes as material to develop their portion of a business continuity plan.
- ◆ The goal is for the IT staff to have a documented business continuity plan that forms part of the overall plan for the faculty or department. Within that plan will be components related to IT and telecommunications disaster response, recovery measures and evidence of protection and retention of vital records through the information technology system

Department Information

Name of Faculty, Department (or Sub Unit within a Department)

Primary Contact for this plan:

Alternate contact for this plan:

Scope

This is an appendix in the business continuity workbook for the University. The table/template provided in the appendix is designed to assist the faculties and departments in completing the analysis and solutions phases of the workbook. The template applies to the relative vital records, IT and telecommunications system, applications and components that are owned and administered within the faculty or department. The template may not be all inclusive therefore respective faculties and departments should add to the material where appropriate.

Responsibility

The administrators of the vital records, IT systems and applications and the telecommunications system for the faculty or department are responsible for completing the portion of the business continuity plan related to the itemized subjects and fields in the table.

General Guidelines for Plan Development

1. Identification of Vital Records and Documents that must be backed up and/or preserved within your Faculty, Department or Unit.

Name of vital record or document	Medium for retention; paper copy, disk, tape...	Location of record or document	Backup of records or documents required and completed	Location of backup records or documents	Access measures to the record or document	Primary contact for record or document	Alternate contact for record or document

2. Identify Backup of Applications and Measures within your Faculty or Department

Name of System or Database	Backup Frequency	Backup Media	Automatic or manual backup process	Storage location	Describe recovery measure in place	Primary IT contact and phone number	Alternate IT contact and number

3. Identify Backup of Servers owned and within your Faculty or Department. (If servers are primarily housed within AICT please note in this section and obtain backup and recovery plan outline from AICT representative).

Identification of server and location	Describe the type of server; e.g. database, web...	Backup Frequency	Backup Media	Automatic or manual backup process	Storage location	Describe recovery measure in place	Primary and alternate IT contacts and phone number

4. Identify Backup of Workstations within your Faculty or Department. (If workstations are primarily maintained by AICT please note in this section and obtain backup and recovery plan outline from AICT representative).

Files from workstations are backed up on faculty or department server.	Files from workstations are backed up on faculty or department server and through AICT	Back up frequency	Automatic backup or Manual backup by user	100% of workstation files are backed up through a faculty or departments process	Individual users are backing up files on their workstation versus faculty or departments process	Describe recovery measures in place for workstations	Primary and alternate IT contacts and phone number

5. Telecommunications

Risks have been identified with respect to the loss of normal telecommunications with the faculty or department and alternate measures for telecommunications needs have been identified and documented in your plan.

Risks Alternate measures	Primary contact for alternate measures plan

6. System Software and Documentation

Verify that system software, applications software and related documentation relative to your faculty, department or unit has been properly retained. It must be accessible in the event of relocation or rebuild need.	Verify that equipment needs, technical connections and access to materials have been documented in the event that your faculty or department must relocate to an alternate workspace

7. Documented Recovery Plan, Testing and Exercises

Verify that your faculty or department has a current documented IT and telecommunications recovery plan. Prioritization of applications and systems is identified in the plan.	Verify that maximum acceptable downtimes and recovery point objectives have been established for the systems and applications within the faculty or department	Verify that the plan is tested on a regular frequency. Document last date of testing	Identify what components within the IT system have been identified as too high a risk to test. Identify the contingency measures in the event of a failure	Identify exercises that simulate a failure of a component of the IT and/or telecommunications system relative to your faculty or departments	Primary IT contact and number Identify IT recovery team