HANOVER RESEARCH

1101 Pennsylvania Ave. NW, Suite 600 Washington, DC 20004
P 202.756.2971 F 866.808.6585 www.hanoverresearch.com

Best Practices in Business Continuity Planning in Higher Education

In the following report, Hanover Research provides an overview of business continuity planning within the context of higher education. The report presents the general planning strategies used to create such a plan, as well as a comparative overview of established business continuity plans at five higher education institutions.

Introduction

Every organization is susceptible to serious causes of business interruption. Business continuity planning aims to anticipate this threat and ensure the maintenance of critical operations when an organization is confronted with interruptions such as natural disasters, technology failures or threats, human errors, terrorism, or maintenance failures. By developing a business continuity plan, an organization is able to minimize losses during times of business interruptions, while continuing to serve customers and maintain administrative operations.

This report, which provides relevant information to assist in the creation of a business continuity plan, is divided into two main sections. In the first section, the report describes the stages of business continuity planning, from initial devising meetings to the plan implementation. Information taken from institutional plans and websites provides details and requirements for each commonly developed aspect of a continuity plan.

The second section of this report details the business continuity plans in place at five higher education institutions. These colleges and universities were chosen on the basis of the public availability of detailed plan documents. Information taken from these plans provides thorough examples of each stage of continuity planning, as well as examples of the surveys and tables used in plan creation. Much of the information provided in this section could provide assistance to other institutions beginning the continuity planning process, and we have selected these particular examples with an appreciation of the unique characteristics and requirements of one member.

The plans examined in this report serve the following institutions:

- The University of Maryland
- The University of California at Los Angeles
- North Carolina State University
- Stanford University
- The University of Minnesota

Overview of Business Continuation Planning

In order to manage disasters and business interruptions, many organizations have traditionally relied on a Disaster Contingency Recovery Plan (DCRP) or Disaster Recovery Plan (DRP). Although these plans are vital to an organization, they reflect a primarily reactive approach and do not generally provide comprehensive guidelines for disruption forecasting, risk management, or long term recovery. A business continuity plan, on the other hand, aims to "eliminate or reduce the impact of a disaster condition before the condition occurs."[1]

As in the for-profit sector, business continuity plans are vital in higher education. Colleges and universities are obligated to protect and provide for students, faculty, staff, and visitors at all times, even in the event of a major interruption of operations. For institutions of higher education, a business continuity plan ensures the ability to resume business operations should a crisis occur. The plan should cover all technical and non-technical areas of the university's business operations, including a plan for communication, data storage and recovery, system applications, network access, institutional processes, and human resources.[2] The failure of an institution to prepare a comprehensive business continuity plan could lead to significant consequences, including financial loss, interruptions to the academic schedule, failure of current projects, or other unforeseen delays in the completion of critical activities.[3]

A business continuity plan should provide a clear roadmap for the recovery of all normal business operations, thus allowing the organization to return to "business as usual." For institutions of higher education, business continuity planning requires a university-wide approach combined with individual, department-based plans for units in charge of mission critical functions. These include all processes that are essential to each department, allowing them to minimize losses, resume administrative functions, and continue to serve students, faculty and staff, or visitors. The development and implementation of a universal business continuity plan, which can be adopted by multiple organizations, is impossible and impractical; every institution must develop a unique plan based on specific circumstances. A business continuity plan must also be dynamic – constantly updating as departmental and technological changes occur.

The creation of a business continuity plan benefits the university whether or not it is ever required in a crisis situation. As noted by Cynthia Golden and Diana G. Oblinger, vice presidents of EDUCAUSE, "the **process** of producing an institutional plan for continuity after a disaster is probably as important as the plan itself; its

[1] Virginia Cerullo and Michael J. Cerullo, "Business Continuity Planning: A Comprehensive Approach," Information Systems Management, 2004.
[2] Eugene L. Zdziarski, et al. "Campus Crisis Management: A Comprehensive Guide to Planning, Prevention, Response, and Recovery," Wiley, 2007.
[3] "University of Maryland Business Continuity Plan," University of Maryland, http://www.oit.umd.edu/ITCouncil/materials/BCP_Final_Draft052005.pdf
http://www.oit.umd.edu/ITCouncil/materials/BCP_Final_Draft052005.pdf

benefits will be evident even if the plan is never needed."[4] Creating such a plan requires discussions among leaders of different university departments and units, a process that often calls attention to current weaknesses and initiates strategies for improvements in current campus operations.

While every business continuity plan must be unique to the university, institutions typically follow similar steps in the development process. These steps include:

- *Identify* critical business processes;
- *Develop* a plan to address how critical processes will be restored in the event of a disruption;
- *Implement* the plan;
- *Test* the plan on a frequent basis; and
- *Update* the plan as the institution's processes change.[5]

Common Components of the Business Continuity Plan

Many business continuity plans also share the following four key components, which are described in detail in this section:

- **Business Impact Analysis**
  This component identifies the institution's critical processes, provides estimates of the maximum threshold for downtime, and prioritizes essential business processes and functions for the restoration process.

- **Risk Assessment**
  This second element recognizes specific threats to the institution, evaluates vulnerability to each threat, and assigns a "degree of risk" associated with each potential event or hazard.

- **Risk Management/Continuity Planning**
  This component examines the results of the Risk Assessment to decide which risks require specific management and provides a written, widely distributed plan outlining the actions necessary to restore business functions in the occurrence of a disruption.

[4] Cynthia Golden and Diana G. Oblinger, "The Myth about Business Continuity and Disaster Recovery," EDUCAUSE Review, May/June 2007. http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume42/TheMythaboutBusinessContinuity/158137

[5] Catherine Lewis, "Simple Things that Could Save Your Institution," EDUCAUSE Center for Applied Research, Apr 2007. http://net.educause.edu/ir/library/pdf/ERB0709.pdf

- **Testing, Training, and Updating**
  The final component establishes the methodology used by the institution to consistently train staff members, test and update the plan, and communicate plan changes to employees.[6]

Business Impact Analysis

At institutions of higher education, the business impact analysis is conducted as one of the initial stages in the business continuity planning process. According to the University of Maryland, this process includes identification of critical business functions, development of estimates for allowable downtime, and prioritization of the recovery process.

Other sources offer a broader description and incorporate many of the risk assessment and management components. According to the authors of "Business Continuity Planning: A Comprehensive Approach," the business impact analysis not only involves the identification and prioritization of critical business functions, but also of associated risks according to probability of occurrence and potential impact on the institution. Further, the analysis should recommend a solution such as avoidance, mitigation, or absorption for each risk and, if deemed appropriate, identify specific mechanisms by which the institution will avoid or mitigate risks with highly detrimental consequences.[7]

At institutions of higher education, critical business processes may be placed into one of three categories:

- **Safety and Security**
  This category includes activities which are necessary to maintain a safe and secure environment for all students, faculty, staff, campus visitors, and the surrounding community.

- **Business Support Services**
  These services include activities that allow the institution to maintain vital business operations, safeguard assets, and secure the financial viability of the institution. Examples of business support services include payroll, revenue collection, accounts payable, and financial reporting.[8]

- **Learning, Education, and Research**
  This category consists of all programs and services that directly support the academic mission of the institution. Examples include student services such as

[6] "University of Maryland Business Continuity Plan," University of Maryland, op. cit.
[7] Virginia Cerullo and Michael J. Cerullo, op. cit.
[8] "University of Maryland Business Continuation Plan," op. cit.

admissions and registration, academic courses, research programs, and graduation services.

The business impact analysis typically begins with a survey of the leadership of vital business processes to gather input on how various types of disruptive events might impact institutional procedures. Mark C. Sheehan and Ronald Yanosky, the authors of "Shared Responsibility for Business Continuity: The Team Approach at UCLA" establish four classes of information within such analysis:

- *Recovery time objectives:* The length of time a business process could be unavailable before the impact reaches an unacceptable level.
- *Recovery point objectives:* The maximum acceptable period of time between the most recent data backup and a system disruption.
- *Financial and intangible impacts:* Includes impacts such as the "interruptions of cash flow into the institution, the costs of mitigating a disaster, [and] financial penalties for failing to meet contractual obligations,"[9] in addition to intangible consequences such as those dealing with safety of students and staff, the level of quality maintained by academic and research programs, and public imagine and reputation.
- *Application dependencies:* Modern business applications are commonly dependent on information technology resources, such as systems, software, data, and personnel. The business impact analysis should consider the interdependencies of institutional processes.

After estimates for these four variables have been made at the departmental level, the analysis advances to a "group validation stage" commonly conducted by an external facilitator. During this phase, interdependencies among business processes are identified and discussed, as well as group agreements regarding impacts, recovery time objectives, and recovery point objectives.[10]

Risk Assessment

Risk assessment focuses on the potential hazards and threats that could negatively impact institutions and attempts to predict the likelihood of occurrence, the severity of impact, and the institution's level of vulnerability for each disruptive event.[11] This vulnerability analysis is the foundation of a business continuity plan, and it outlines how the institution might allocate additional time and resources towards mitigation or planning efforts for events with high likelihood of occurrence and high levels of severity.

[9] Mark C. Sheehan and Ronald Yanosky, "Shared Responsibility for Business Continuity: The Team Approach at UCLA," EDUCAUSE Center for Applied Research, 2007.
http://net.educause.edu/ir/library/pdf/ers0702/cs/ECS0702.pdf
[10] Ibid.
[11] Ibid.

Risk Management and Continuity Planning

During the risk management phase, the institution develops specific strategies to be enacted if a disruptive event occurs. These strategies should include:

- Steps to prevent interruptions and protect assets;
- Procedures to be followed during a disruptive event, including those from the institution's emergency management plan;
- Planned responses to the incident, such as reversion to paper-based systems or the activation of remote information technology facilities; and
- Plans to resume normal business operations after the crisis has passed.[12]

Each unit or department within the university should develop its own risk management practices and develop a customized plan that enables the continuation of critical functions. Divisions of similar size and function may elect to combine their business continuity planning efforts as long as they jointly ensure that all essential functions are addressed. Even as they address autonomous areas of operation, these division-based plans should remain integrated with the wider organization and take into account the potential for an institution-wide disruption that impacts multiple units across the university. Departments that depend on other divisions or external suppliers to provide critical functions must coordinate with these groups to ensure that each are addressed in the continuity plan.[13]

The University of Maryland proposes the following guidelines, worth citing at length, for the development of unit- and division- based continuity plans:

- Determine which subset of critical business process(s)…are being addressed by the unit plan.
- Develop a unit risk analysis that…identifies risks and/or hazards that might reasonably pose a threat to the operating unit's ability to function…
- Identify existing and easily implemented controls to avoid these risks and hazards.
- Develop and document procedures for recovering all or part of the highest priority functions, given specific failure scenarios and time horizons.
- Determine whether each process could be suspended or degraded, or whether it must be fully operations immediately. In many cases, service levels may be considerably less than existed prior to interruption, but nevertheless sufficient to sustain the critical mission function for some time.
- Determine the time frame for full recovery of critical functions if a degraded service level is deemed initially acceptable.
- Identify alternate work sites or other temporary facilities for the most critical functions.

[12] Bulleted points taken verbatim from: Ibid.
[13] "University of Maryland Business Continuity Plan," op. cit.

- Provide for the ongoing backup of critical data and protection of critical equipment.
- Assign local recovery roles, responsibilities, and authority.
- Develop procedures for recovering impacted operations quickly, and strategies for providing programs and services under various emergency conditions.
- Determine when the plan needs to be activated and identify who within the unit is authorized to implement the plan.
- Identify all persons with copies of the plan. Store at least one current copy in an off-site facility with immediate availability.
- Maintain the list of resources, vendors, etc., with which the department has agreements for the provision of services, supplies, or equipment to be used in the event of an interruption of operations.
- Establish procedures for contacting appropriate [university] departments and [university] suppliers in the event of an interruption of operations.
- Establish procedures for return to full, normal operations of the operating unit, including that of non-critical functions.[14]

Testing, Training, and Updating

Testing is important to business continuity planning and development for a number of reasons. If an institution has not established realistic recovery timelines, a wide expectation gap between the needs of the institution and the actual procedures of the continuity plan could arise after a disruption. Institutions should develop a methodology to regularly test the proposed strategies and should also ensure adequate training is made available to staff. Testing is absolutely essential to determining whether the business continuity plan adequately addresses critical risks, and testing in realistic conditions allows staff to better understand the procedures, thus reducing panic in the event of an actual disaster.

Unit- and division-based continuity plans should also be regularly tested. Through testing, the viability of the plan is evaluated and results may inform modification and improvement. Individual plans should also be reviewed by the unit or division head on an annual basis. In particular, the unit or division head should ensure that:

- Critical functions have been identified;
- Continuity and recovery strategies are in place;
- Documentation for the plan is current;
- Minimum levels of required operation and recovery time frames have been established; and
- Exercising of the plan has been completed during the past 24 months.[15]

[14] Ibid.
[15] Bulleted points taken verbatim from: Ibid.

Each unit or division should train staff on the proper use of the plan and ensure that each employee is aware of any specific responsibilities during the recovery process. Employees should participate in continuity plan training within a reasonable time period after the date of hire.

The Disaster Recovery Plan

Many institutions have developed a Disaster Contingency Recovery Plan or a Disaster Recovery Plan in conjunction with a business continuity plan. These plans lay out specific procedures that should be enacted after a disaster occurs. They typically include the following components:

- Identification of primary and alternate team members and their specific duties, including executive management roles;
- Notification procedures and alternate meeting site locations;
- Work-around processes to keep the function operational while damaged resources are being restored;
- A contract list of all staff and the functions they are qualified to perform;
- Identification of all internal and external vendors and each vendor's primary and alternate contacts; and
- Report forms (expenses, activities, etc.).[16]

In general, disaster and emergency recovery plans focus on addressing the incident and the time period immediately following the disruption. These plans can involve outside agencies, such as local fire and police department staff, in the case of larger emergencies. Regardless of the size of the disaster, the majority of the plan procedures occur in a short period of time, until the situation is brought under immediate control and safety is ensured. Emergency plans must also include basic medical and human services, such as emergency housing and food provisions.[17]

A disaster recovery plan compliments a business continuity plan, as business operations would not resume without emergency control and management clearance. After a crisis has occurred, the business continuity plan is implemented once all health and safety issues have been addressed. The business continuity plan focuses on long-term reinstallation of business operations, and it assumes that the following campus and local services have been restored:

- Police, Fire, and Ambulance Services
- Electricity, water, reasonable climate control, and adequate lighting
- Access to and egress from campus, classrooms, and administrative facilities

[16] Bulleted points taken verbatim from: Virginia Cerullo and Michael J. Cerullo, op. cit.
[17] "Emergency Response vs. Business Continuity Plans," Loyola University in Chicago, http://www.luc.edu/environmentalservices/emer_res_bus_con.shtml

- Safe handling and proper disposal of toxic substances, biologically hazardous materials, and radioactive materials[18]

Although the disaster recovery plan is essential to restoring the safety of the campus or affected area, it does not focus on the recovery of business operations and services. Many emergency response plans, including that of XYZ University, solely emphasize strategies and plans for surviving and reporting disasters.

The XYZ University Emergency Response Plan details a number of potential threats or hazardous situations within the "Emergency Procedures" section. While this section provides information on handling such situations as they are occurring, it could also provide a background for the Risk Assessment section of a business continuity plan. The Emergency Procedures section lists all potential physical risks, including fire or explosion, uncontained hazardous materials, bomb threats, severe weather, and more. This list could be expanded to include all technological, financial, marketing, reputation, and legal risks, such as the examples of risk provided by North Carolina State University in Table 2, below.[19]

Many of the other essential procedures for creating a business continuity plan, including prioritization of critical functions and vital records storage, cannot be derived from an emergency response plan and must be assessed separately.

Timeline

As demonstrated above, the creation of a business continuity plan is an extensive, complex, and collaborative process. According to our research, the time required to create these plans has varied widely from institution to institution, and detailed recommendations on timeframe do not appear to be publicly available. We did uncover two sources that specifically address timeline. The University of Minnesota, one of the first institutions to tackle business continuity planning, reported that the process took years to complete. The University of California at Los Angeles, by contrast, recommends that the institutional planning process will require between two and four months to move from the formation of a planning committee to the creation of a draft institutional plan, which must then be subject to ongoing testing and refinement.[20]

In the first weeks, a business continuation committee is created and initial meetings are held. This centralized committee designs and distributes surveys to each departmental area, gathering information on specific essential functions, potential risks, and dependencies on other divisions or outside vendors. In the middle stages of planning, committee meetings are held to determine institution-wide essential functions and to evaluate potential threats. Departments are also asked to create lists

[18] "University of Maryland Business Continuity Plan," op. cit.
[19] See page 26.
[20] "UC Ready," The University of California at Los Angeles, http://www.oirm.ucla.edu/UCReady.pdf.

of emergency contact information for all current employees and outside vendors. In the final phase of departmental continuity planning, files are appropriated and backed up to ensure protection during a disruptive situation, and the committee meets to map departmental and unit plans towards the creation of an institution-wide plan. After an institution-wide plan is completed, the committee must schedule frequent testing opportunities to ensure the plan is appropriate and sufficient.

In any given institution, it is likely that actual timeframe will depend considerably on the speed with which coordinators are able to enlist a central committee, create a schedule of meetings, circulate surveys to department and unit heads, and follow up to ensure participation in the process.

In the next section, we turn to a consideration of what elements mitigate or ensure success and efficacy in the planning process.

Successful Business Continuation Plan Initiatives

There are a number of factors that influence the success of an institution's business continuity planning efforts. One of the most crucial factors is the assignment of an appropriate leader. It is suggested that, in order to ensure a consistent execution across the institution, the assigned leader should be "highly placed, but from an area other than IT or one of the functional areas directly involved in [business continuity] planning."[21]

It is also critical that business continuity planning is not perceived by employees as merely an IT-related plan that does not involve the entire institution. The continuity planning team should reinforce the message that the planning process is essential to the university's educational mission and administrative functions.

For continuity planning efforts to be successful, the process and resulting documentation need to be clear and accessible to all participating units. Higher education risk assessment projects often involve elaborate documentation designed for an outside audience such as an auditor. These documents can be impractical and intimidating, and complex processes can be difficult to implement on strained university budgets. In addition, lengthy business continuity plans prepared by outside sources often come across as either overly detailed or impractically generalized.

Frustration with the process often occurs when unit or division heads devote significant time and energy to identifying risks and developing a business continuity plan for their particular functions, only to have unit-specific issues deemed to be low priority and inappropriate for inclusion in the institution-wide continuity planning agenda. Of course, concerns that affect a greater number of people or processes often top an institution's priority list. Unfortunately, this triage approach, especially when implemented unilaterally or without clear explanation, does not allow for the democratic inclusion of the important concerns of individual departments and may be negatively perceived.

Some departments may find it difficult to accept that their business processes are not viewed as critical to the institution as a whole. It must be remembered that a process may be very important to the university, but not necessarily *critical* for operations. For example, accounts receivable is a critical process, but it can survive a 7-10 day interruption with roughly 90 percent of revenues recoverable after the disaster is resolved.[22] An objective facilitator can be an invaluable resource for ensuring that the interests of all parties are addressed fairly and consistently.

Support from the executive leadership of the university is essential for continuity planning efforts, ensuring institutional commitment and adequate funding will be

[21] Mark C. Sheehan and Ronald Yanosky, op. cit.
[22] Ibid.

provided for the initiative. Lack of sufficient funding is reported as the primary barrier to business continuity planning, according to respondents to a 2007 EDUCAUSE Center for Applied Research survey. The development of a financial model that allocates resources for business continuity planning across all institutional units is considered a key component of a successful business continuity plan.[23]

Finally, rapid and ongoing changes in technology, personnel, and institutional priorities require that business continuity planning similarly evolve through a testing and refinement process. After an initial plan is developed and distributed, a basic exercise is an adequate first test in the plan's development. Consider the following hypothetical example: a disaster scenario is described to a representative team, whose responsibility it is to then walk through how the university would respond to the disaster. An accompanying discussion draws attention to gaps and inconsistencies, and forms a basis for necessary changes. As the institution continues to alter its business continuity plans, tests must become increasingly challenging and complex in order to cover all possible areas of improvement.

In the next section, we turn to a review of business continuity plans and planning processes that have been adopted by five institutions of higher education.

[23] Cynthia Golden and Diana G. Oblinger, op. cit.

Examples in Higher Education

The following section provides a sample of business continuity plans currently in place on university campuses across the United States. The institutional plans examined here derive from various geographic regions and from both large and small universities, including many institutions comparable to XYZ University in student enrollment size. These five institutions were selected for review based on the public availability of strong business continuity plans and detailed planning materials.

Our review focuses on the following institutions:

- The University of Maryland
  - Total enrollment, College Park campus: 37,195
- The University of California at Los Angeles
  - Total enrollment: 38,550
- North Carolina State University
  - Total enrollment: 33,819
- Stanford University
  - Total enrollment: 18,498
- The University of Minnesota
  - Total enrollment, Minneapolis "Twin Cities" campus: 51,659[24]

[24] Numbers represent total undergraduate and graduate student enrollment at each campus. Statistics taken from: IPEDS Data Center. National Center for Education Statistics Website, accessed August 2010. www.nces.ed.gov/ipeds/datacenter

University of Maryland[25]

Business continuity planning at The University of Maryland follows four stages: business impact analysis, risk assessment, risk management, and testing and maintenance. The following points provide specific information on the business continuity management process, which follows a timeline from the initial planning to incident response.

Pre-Incident Planning

- *Project Initiation:* Obtain management support and organize planning committees.
- *Risk Identification:* Identify threats to the specific university, including natural disasters, fire, equipment breakdown, utility outage, hazardous materials, supply interruption, and workplace violence.
- *Risk Quantification:* For each specific risk, develop loss scenarios, estimate impact on buildings, operations, personnel, and equipment, identify and prioritize critical functions, determine maximum allowable downtime, and identify resource requirements
- *Mitigation:* Avoid disasters through protection systems, hazard elimination, duplication of resources, assessment of alternative operating strategies, and development of recovery strategies

Plan Development

- *Documentation:* Create working plan documents for business continuation, crisis management, and emergency response.
- *Implementation and Training*
- *Testing*
- *Maintenance and Updating:* Adjust and alter the plans to be more effective by changes in personnel, facilities, operations, and potential hazards, and the creation of regulatory requirements

Incident Response

- *Emergency Response:* Prepare for various types of necessary responses, including evacuation, fire fighting, removal of hazardous materials, rescue, medical assistance, security, or property conservation.
- *Crisis Management:* Determine how to continue internal communications and external public relations, as well as retain management in positions of decision-making.
- *Business Continuation:* Plan to execute alternative operating strategies, restore critical functions, and implement long-term recovery.

[25] All following information taken from: "University of Maryland Business Continuity Plan," op. cit.

Business Impact Analysis

The business impact analysis calls for critical divisions across the University to identify vital business processes. Critical divisions include Academic Affairs, Administrative Affairs, Research, Student Affairs, University Relations, and the Office of Information Technology. The following tables display the positions within each department, as well as the allowable downtime and priority to recover if a disaster or emergency were to occur. The tables provide a thorough example of the evaluation of the essential services of each individual department, as well as the importance of each position in a business continuation situation.

Table 1A: Critical Business Processes, Academic Affairs

Business Unit	Business Process/Business Function	Allowable Downtime	Priority for Recovery
Office of the Sr. VP and Provost	Academic Affairs Administration	1-2 days	High
Provost Senior Staff	Academic Affairs Administration	1-3 days	High
Grd/Ugrd Admissions	Admissions Peak (Oct-late May)	0-1 days	High
Grd/Ugrd Admissions	Admissions Non Peak	1-2 days	High
Financial Aid	Award Cycle Peak (Sept-late May)	0-1 days	High
Financial Aid	Award Cycle Non Peak	1-2 days	High
Registrar	Registrations/Grade Submission/ Drop/Add Peak	0-1 days	High
Registrar	Registrations, etc. Non Peak	1-2 days	High
International Student Services	Visa Processing, interface with International students and INS, etc.	1-2 days	High
Office of the Senior VP and Provost	Academic Affairs Personnel and Budget Office	0-1 days	High
Other Academic Affairs Units	Office of Org. Effectiveness, Baltimore Incentive Awards Prgm., Intl. Prgm., etc.	3-5 days	Medium
OIRP	Institutional studies and reporting	2-3 days	Medium
College/Libraries/ Other Academic Units	Instruction/Admin./Support	TBD	TBD

Source: University of Maryland Business Continuity Plan

Table 1B: Critical Business Processes, Administrative Affairs

Business Unit	Business Process/Business Function	Allowable Downtime	Priority for Recovery
Business Services	Mail Services	1 day	High
Business Services	Information Technology Group	1 day	High
Business Services	Motor Transportation Services	½ day	High
Business Services	Copy/Printing Services	1-2 days	Medium
Business Services	Terp Services	2-3 days	Medium
Business Services	Travel Services	1-2 days	Medium
Human Resources	Compensation and Classification	2-3 days	High
Human Resources	Data Services/PHR	1 day	High
Human Resources	Employment	1 day	High
Human Resources	Staff Relations	2-3 days	Medium

Business Unit	Business Process/Business Function	Allowable Downtime	Priority for Recovery
Human Resources	Organizational Development and Training	5 days	Low
Procurement	Purchasing	½ day	High
Procurement	Construction and Facilities Procurement	½ day	High
Procurement	Physical Distribution Center	½ day	High
Procurement	Central Receiving	½ day	High
Procurement	General Stores	½ day	High
Procurement	Central Shipping, Distribution	½ day	High
Comptroller	Bursar- Peak Period- Online Payments	1 day	High
	Bursar- Peak Period- Bill Generation	1 day	
	Bursar- Peak Period- Walk Up Payments	2-3 days	
Comptroller	Bursar- Non Peak- Online Payments	1 day	Medium
	Bursar- Non Peak- Bill Generation	1 day	
	Bursar- Non Peak- Walk Up Payments	2-3 days	
Comptroller	Accounts Payable/Accounts Receivable	1 day	High
Comptroller	General Accounting	½ day	High
Comptroller	Payroll	None	High
Comptroller	Budget- Peak	1 day	Medium
Comptroller	Budget- Non Peak	2-3 days	Medium
Comptroller	Contract and Grants Accounting	1 day	High
Facilities Management	Facilities Planning	1-2 days	Medium
Facilities Management	Architecture, Engineering & Construction	1-2 days	Medium
Facilities Management	Operations and Maintenance	None	High
Facilities Management	Building and Landscape Services	None	High
Facilities Management	Office of Facilities Administration	None	High
Environmental Safety	Staffing operations of critical personnel for emergency response	None	High
Environmental Safety	Providing emergency response for campus	None	High
Environmental Safety	Investigating accidents, incidents, exposures, and discharges	None	High
Environmental Safety	Providing technical assistance and evaluation to assess and communicate risk	None	High
Environmental Safety	Access to emergency communications equipment and vehicles	None	High
Environmental Safety	Managing insurance claims process for all incidents	2 days	Medium
Environmental Safety	Managing/reporting workers' compensation injuries	1 day	Medium
Environmental Safety	Provide notice of hazardous material releases to regulatory agencies	None	High
Environmental Safety	Maintain security and integrity of controlled waste facility	None	High
Environmental Safety	Provide collection, packaging, and secure storage of controlled waste	7 days	Low
Environmental Safety	Access to chemical inventories	None	High
Environmental Safety	Access to material safety data sheet info and lab signage	None	High
Environmental Safety	Access to personal protective equipment	None	High
Environmental Safety	Secure radiation facilities	None	High

Business Unit	Business Process/Business Function	Allowable Downtime	Priority for Recovery
Environmental Safety	Ensure safety and security of select agents	None	High
Public Safety	Staffing operations of critical personnel for emergency response	None	High
Public Safety	Providing emergency communications equipment and vehicles	None	High
Public Safety	Activation of Campus Emergency Operations Center	None	High
Public Safety	Mobilizing field incident command post	None	High
Public Safety	Investigating criminal activity related to incident	None	Medium
Public Safety	Providing site security and orderly traffic flow	None	High
Public Safety	Acquiring other law enforcement and governmental resources	1 day	Medium

Source: University of Maryland Business Continuity Plan

Table 1C: Critical Business Processes, Research

Business Unit	Business Process/Business Function	Allowable Downtime	Priority for Recovery
ORAA	Pre-proposal routing and review	1 day	High
ORAA	Electronic proposal/data submission	1 day	High
ORAA	Electronic data entry	2 days	Medium
ORAA	Electronic data management	2 days	Medium
ORAA	Campus outreach	5 days	Low
IACUC/LAC	Animal care and welfare	1 day	High
IRB	Review and approval of applicable research proposals	2 days	Medium
VPR	DRIF requests/research council activities	5 days	Low
OTC	Intellectual property protection	5 days	Low
IGS	Outreach to UM and the State	5 days	Low

Source: University of Maryland Business Continuity Plan

Table 1D: Critical Business Processes, Student Affairs

Business Unit	Business Process/Business Function	Allowable Downtime	Priority for Recovery
Student Affairs	PHR, Time and Attendance	8 hours	High
Campus Recreation Center	Campus Recreation Center	1-2 days	Low
Career Center	Career Fairs	4 hours	Medium
Conference and Visitor Services	Summer Conferences	4 hours	Medium
Conference and Visitor Services	Visitor Center	4 hours	Medium
Counseling Center	Counseling Service	1 day	Medium
Counseling Center	Disability Support Services	None	High
Dining Services	South Campus Dining Hall	1-2 hours	High
Dining Services	The Diner	1-2 hours	High
Dining Services	Facilities Management and Maintenance	1-2 hours	High

Business Unit	Business Process/Business Function	Allowable Downtime	Priority for Recovery
Dining Services	Financial and Information Technology services	1-2 hours	High
Greek Life	Residential Operations	None	High
Health Center	Primary Care	4 hours	High
Health Center	Medical Records	4 hours	Medium
Health Center	Information Systems	1-2 hours	Medium
Residential Facilities	Housekeeping and Maintenance	None	High
Residential Facilities	Security and Special Services	None	High
Residential Facilities	Financial and Information Technology services	None	High
Resident Life	Assignments and public inquiry	1 day	Low
Resident Life	Residence halls	None	High
Stamp Student Union	General Operations	1 day	Low
Transportation Services	Fleet management	None	High
Transportation Services	Shuttle UM Route Services	None	High

Source: University of Maryland Business Continuity Plan

Table 1E: Critical Business Processes, University Relations

Business Unit	Business Process/Business Function	Allowable Downtime	Priority for Recovery
University Communications	Public information, including internet communications	None	High
Information Systems	Computer services, Peak	2 days	High
Information Systerms	Computer services, Non peak	3-5 days	High
CP Foundation	Payables and receivables	1 day	High
Development	Fundraising, Peak	2 days	High
Development	Fundraising, Non peak	5 days	High
Alumni Association	Alumni Association Events, Peak	None	Medium
Alumni Association	Alumni Association Events, Non peak	5 days	Medium
Alumni Association	Alumni Association membership dues processing and gift telemarketing, Peak	2 days	High
Alumni Association	Alumni Association membership dues processing, Non peak	5 days	Medium
University Publications and Marketing	University Calendar, Magazine, etc.	5 days	Low

Source: University of Maryland Business Continuity Plan

These five tables display the core business processes that must be restored for the University of Maryland to resume normal business operations. The categories of Allowable Downtime and Priority for Recovery demonstrate which services and processes are deemed most critical, and which could be suspended for multiple days without seriously impacting the integrity of the University.

Core services provided by the University's Office of Information Technology – such as network maintenance, telephone services, and software applications – are imperative for the recovery of nearly all the business processes identified by other critical divisions. In order to ensure that information technology services recover as

quickly as possible, the Office of Information Technology at the University of Maryland created a separate Disaster Recovery Plan.

Risk Assessment

During the risk assessment phase, the University of Maryland created a hazard matrix outlining the likelihood of occurrence for all potential threats, as well as the estimated severity should a specific incident occur. We reproduce this matrix below:

Table 1F: University of Maryland Hazard Matrix

Hazard	Likelihood of Occurrence		Severity		
	Likely	Unlikely	High	Moderate	Low
Active Shooter	X		X		
Air Crash	X				X
Civil Disorder	X		X		
Disease Outbreak		X			X
Earthquake		X	X		
Extreme Weather	X		X		
Flood		X			X
Hazmat	X		X		
Hostage Situation	X			X	
Major Fire		X		X	
Power Failure		X	X		
Public Assembly Emergency	X				X
Structural Collapse		X		X	
Telecomm Failure		X	X		
Terrorist Threat	X		X		
Tornado	X		X		
Train Accident		X	X		
Utility Failure		X	X		

Source: University of Maryland Business Continuity Plan

Risk Management and Continuity Planning

The University of Maryland articulates the following policy for risk management and business continuity planning, which occurs at the departmental and unit levels. This policy statement is worth citing at length:

> Each University division will appoint a person responsible for continuity planning. This person will be the division focal point for determining which of its units operates processes that are critical and ensuring those processes are identified in [the institution's business impact analysis].

> Each division will ensure that operating unites responsible for critical business processes identified in [the business impact analysis] develop a Business Continuity Plan that enables the operating unit to continue to perform those critical functions and services in the event of a disaster. Divisions may determine the degree to which continuity planning is consolidated across multiple units within a division. This decision will be based on factors such as commonality of business process, size of the division, etc. However, all identified critical processes must be covered by a plan.
>
> Unit plans must take into account the possibility that a University-wide interruption may affect multiple units. Departments that depend on other departments or external suppliers to provide its critical functions should coordinate with those departments or external suppliers to ensure these suppliers or units also have a continuity plan.
>
> Division coordinators will provide central coordination of the continuity planning process to assist units in determining space, equipment, and services that might be available within the University and to make the planning process coherent across units.
>
> OIT's Policy and Procedure unit will be responsible for collecting all unit plans and the combination of this document and the unit plans will constitute the University's complete Business Continuity Plan. Initial versions of unit plans will be completed and forwarded to OIT no later than six months from the approval of this plan.
>
> In the event plan activation requires prioritization among units for the recovery of services or allocation of limited resources, that prioritization will be accomplished by the President's Cabinet after consideration of the exact circumstances surrounding the plan activation.[26]

The development of department-based plans should follow the guidelines discussed in the opening section. In this case, the University developed the following series of questions to be used by colleges and divisions as they provided guidance for constituent departments.

- What are your department's business interdependencies? What do you need from other departments to perform critical functions? What departments depend on you to perform critical functions?
- Are there days of the week or month, or months of the year, when a major emergency would be even more disruptive than at other times?
- Is your essential data backed up regularly? Would the information be accessible if your building was closed, or if the University network was down?

[26] Ibid.

- Does the College/Division and its constituent Departments have planning documents for continuing operations in the event of disaster?
- Is there a process for tracking the cost of business recovery (including funds spent on overtime, special materials/supplies, temporary personnel, etc.) and a mechanism for distinguishing emergency recovery costs from other business expenditures?
  - Are special vendor/contractor arrangements necessary for the department(s) to insure continuity of services?
  - Does the College/Division have a method to make emergency purchases?
- What human resources would you need to restore the most critical functions?
  - Do employees have personal emergency preparedness plans for their households?
  - If only 50 percent of your staff/faculty could return to work, could you open?
  - Can some employees telecommute during a disaster? What can you do now to plan for that?
  - If the University had volunteer workers available after a disaster, what skills would be needed in your department?
- What equipment is necessary for the department to perform its functions?
- Have precautions been taken to secure essential equipment in the event of most likely emergencies?
- How would you replace equipment within hours or days to be able to resume normal business?
- If your department couldn't use its office space to operate, how much space would you need to relocate? What kinds of equipment are essential for performing your unit's critical functions?[27]

[27] Ibid.

University of California, Los Angeles[28]

The University of California at Los Angeles is the largest university in the state of California, with close to 37,000 total students. Due to its size, one of the major challenges for UCLA has been to establish similar levels of information technology resiliency across multiple campuses. In order to provide guidelines and prioritize the importance of various systems and functions, UCLA launched a business impact analysis in December 2005, with IBM Global Technology Services serving as an external facilitator. The intent of the business impact analysis was to prompt campus leaders to consider the potential impacts of various hazards and incidents, and to determine acceptable timeframes for the recovery of critical functions.

Participants were selected based on their ownership of automated business processes affecting the entire campus, and they represented 15 campus divisions: Administrative Information Systems, University Library, Undergraduate Admissions and Relations, Student Loan Services, Financial Aid Office, Student Affairs/Registrar, Academic Technology Services, Office of Research Administration, Housing and Hospitality Services, Graduate Division, Facilities Management, External Affairs, Corporate Financial Services, Communications Technology Services, and the College of Letters and Sciences.

The overarching goal of the business impact analysis was to achieve balance between the risks and impacts of business interruptions and the costs of mitigation and recovery efforts. UCLA faced numerous obstacles through the creation process, including:

- *Coordination:* Often a wide range of departments have systems with potentially campus-wide impact. It becomes a complex problem to identify the right participants, coordinate large meetings, and follow up to ensure that assignments are completed in a timely manner.
- *Leadership:* It may require extraordinary leadership to manage the multitude of priorities and attitudes brought by differing department heads.
- *Prioritization:* In the early stages of impact analysis, many departments' representatives believe their issues should receive top priority. It requires patience and time to prioritize the services and explain their position within the greater institutional perspective.
- *Enterprise Vision:* Most institutions conducting impact analysis discover that providers of distributed systems are oftentimes only partially aware of the extensive interdependencies between the many elements of the campus information technology infrastructure and the application suite. The establishment of final priorities must take this into account.[29]

[28] All information regarding the University of California at Los Angeles taken from: Mark C. Sheehan and Ronald Yanosky, op. cit.
[29] Ibid.

As the initial step to begin dialogue about a business impact analysis, the University held an opening meeting and administered a detailed survey to the campus's functional areas. The survey focused on the four areas of recovery time objective, recovery point objectives, financial and intangible impacts, and application dependencies. This survey laid the foundation for IBM-facilitated interviews in which the participants were asked to explicate on their initial responses. All participants then convened at a group meeting to discuss the survey questions and their responses. Overseen by IBM facilitators, the participants from different functional areas compared recovery time objectives and explored application dependencies.

Significant findings of the impact analysis include:

- *Recovery Time Objectives*
  Over 50 percent of 132 business processes assessed were assigned a recovery time objective of at least seven days. However, an additional 16 percent of processes were assigned 24 hours or less. The majority of the remaining processes were assigned a time objective of roughly 72 hours. The most vital processes identified were restoration of basic utilities such as water and electricity, services related to health, safety, and communication, and financial activities such as payroll.

- *Recovery Point Objectives*
  Student enrollment at peak periods of registration was determined to be most sensitive to data loss, with clear impacts on revenue generation and student satisfaction. Roughly two-thirds of the processes examined would be able to continue through a 24-hour period of data loss, although lengthier periods would seriously impact data integrity. The remaining one-third of processes reviewed would be sustainable through 72 hour to 14 day data loss periods.

- *Financial and Intangible Impact*
  The most serious consequences for the university would be intangible, such as the safety and security of students and staff, the quality of academic and research programs, and institutional reputation, among others. The most serious financial impacts would be caused by long-term interruptions in the usability of classrooms and dormitories, as well as from fines, penalties, and lost interest income if the university's computer-based finance system became unavailable.

- *Application Dependencies*
  The university mainframe computer was regarded as the most vital technological system, as many campus units rely on its databases and applications to operate.

Success Factors

As of 2007, the University was still in the process of testing the business continuity plan and performing gap analyses in order to better understand time estimates and cost effectiveness. Despite ongoing refinement, campus leaders believe the plan has a strong foundation, which they attribute to many factors:

- *High level executive support*: Both the President and the Chancellor of UCLA were involved in the planning process and pledged funding to support the plan from its inception.

- *Campus consensus:* Members of the community are cognizant of the various potential disasters and interruptions the campus could encounter in the future, and have demonstrated dedication to the business continuity planning efforts.

- *Peer leadership:* The Administrative Information Systems Department has become the leading department for business continuity planning efforts, and has contributed to activities from the departmental budget while also allocating central monies towards the efforts.

- *Personal commitment*: The University largely attributes the success of the continuity efforts to the individual and joint commitments of staff in Information Technology Services and in functional areas across campus.

- *Partners:* UCLA received support and assistance from consulting firms and facilitation services, which contributed additional knowledge and expertise in the continuity planning process.

- *Governance structure and processes*: UCLA operates with a clearly defined governance structure, the constituents of which have been willing to commit the necessary time and resources to encourage the continuity efforts.

North Carolina State University

Business continuity planning at North Carolina State University in Raleigh, North Carolina shares the same general approach as many of the other institutions examined in this report. The University has a Business Continuity and Disaster Recovery Department, which adheres to the traditional planning stages of:

- Risk assessment and business impact analysis;
- Identification and selection of strategies;
- Maintenance of life cycle;
- Testing and exercising; and
- Training[30]

Risk Assessment and Business Impact Analysis

North Carolina State University performs risk assessments for over 300 specific departments. The University works with PricewaterhouseCoopers LLP, using the COSO framework, to analyze potential risks to the campus and business operations.[31] The risk assessments help determine which disruptive events possess the highest likelihood of occurring and negatively impacting the University. The Business Continuity and Disaster Recovery Department chooses to draft plans that address those specific threats to critical business processes that have the highest probability of occurrence.[32] The Director of Business Continuity facilitated this process by providing each department and college with a 47 question template to determine institution-wide risks and potentially threatened operations.[33]

As outlined on the following page in Table 2, North Carolina State University has identified six categories of potential business risks: operational, technological, legal, financial, marketing/strategic, and reputation.

[30] "Business Continuity and Disaster Recovery Department: Business Continuity," North Carolina State University, http://www.ncsu.edu/ehs/BCP/phases/
[31] Note: To view the COSO Enterprise Risk Management Framework, visit their website at: http://www.erm.coso.org/Coso/coserm.nsf/frmWebCOSOExecSum?ReadForm.
[32] "Business Continuity and Disaster Recovery Department: Risk Assessment/BIA," North Carolina State University, http://www.ncsu.edu/ehs/BCP/phases/bia.php
[33] Note: The template/checklist can be viewed at: http://www.ncsu.edu/ehs/BCP/documents/Checklist.pdf

Table 2: Examples of Risks

Operational Risks	Financial Risks	Market/Strategic Risks
• Loss or inaccessibility of facility • Unavailability of employees (retired, laid off, home emergency) • Utility failures (power, heating, air, water) • Campus or departmental transportation unavailable • Critical equipment/hardware failure • Vital records destroyed or unavailable to access • Dependent business unit or third party provider suffers a business disruption • Off-site storage location unavailable • Environmental controls inoperable (heating, air, humidity) • Loss of laboratory supplies and materials, research samples • No Service Level Agreements • Student protests/lack of participation, payment, etc.	• Fines • Penalties • Fees • Overdraft charges • Increase in insurance premiums • Insurance deductibles • Replacement cost for equipment/ hardware and office assets • Loss of grant or funding • Loss of financial contributions from alumni, giving, etc. • Loss of interest • Theft or misuse of funds	• Decreased enrollment • Loss of key staff and faculty • Jeopardized accreditations • Loss of permits • Loss of competitive advantage • Lower university standing • Loss of patents and technology transfer
Technological Risks	**Legal Risks**	**Reputation Risks**
• Telephone services unavailable • Critical software unavailable (client server or web) • Data (electronic or paper based) unavailable or destroyed • Data corruption or theft • Computer hardware failures	• Lawsuits • Noncompliance with regulations • Contract violations • Personal liability issues in case of injury, sickness, or harassment	• Loss of trust (public, UNC system, institutions, and internal) • Negative media publicity • Degradation in customer service • Insufficient business continuity and disaster recovery planning causing inappropriate response time

Source: North Carolina State University

Essential Functions and Recovery Strategies

The Business Continuity and Disaster Recovery Department seeks to develop alternative business continuation strategies for the most critical campus services and operations. The department's research processes include collecting information on

service sustainability requirements, benchmarking, evaluating the suitability of various strategies against the business impact analysis, and conducting a cost/benefit study.[34] Similar to the University of Maryland, the Business Continuity and Disaster Recovery Department at North Carolina State University identified the priority services necessary for continuation of critical operations after a disaster or disturbance. The following list displays these services:

- Protection of public welfare;
- Keeping the University and local community informed of status of incident recovery;
- Housing for students;
- Food for students;
- Emergency medical care;
- Provide guidance on the care for animals; central strategy for direction on how to consolidate lab animals;
- Define critical sites;
- Maintain backup of critical employee records and payroll;
- Establish protocols for banking services and payment for goods and services and purchasing;
- Establish backup systems to accommodate needs of admission, enrollment, and scheduling processes;
- Provide space for campus departments and classrooms;
- Restoration of data networking services;
- Restoration of critical administrative and academic computing services; and
- Restoration of telecommunication[35]

The above list details the most critical and essential functions in maintaining business operations and human services after a disaster or interruption. In general, the items included account for the safety and care of students and faculty/staff, the maintenance and recovery of vital documents, and the restoration of university systems.

Testing and Exercises

North Carolina State University requires ongoing testing of business continuity plans, which results in Business Continuity and Disaster Recovery Departmental meetings every three to seven months.[36] Nine tests have been performed since 2003, with testing exercises reinforcing each department's knowledge and commitment to the plan and preparing the institution to recover quickly after a disruptive event. Testing

[34] "Business Continuity and Disaster Recovery Department: Developing Business Continuity Recovery Strategies," North Carolina State University, http://www.ncsu.edu/ehs/BCP/documents/Checklist.pdf
[35] Bulleted points taken verbatim from: "Business Continuity and Disaster Recover Department: Priority Departments," North Carolina State University, http://www.ncsu.edu/ehs/BCP/priority_depts/
[36] "Business Continuity and Disaster Recovery Department: Governance." North Carolina State University, http://www.ncsu.edu/ehs/BCP/governance/

also ensures technical compatibility, furthers recovery team organization and preparedness, and allows the continuity plan to be continually improved and expanded.[37]

The Business Continuity and Disaster Recovery Department stages two types of continuity plan testing. The first test, a structured walk-though of the plans, involves a scripted rehearsal of designated team actions to assess team synchronization and capabilities. The other type of testing is an exercise simulating a disaster or disruptive event. This form of testing requires participation from the entire recovery team, and thus tests the plan as well as the capabilities of each team member.[38]

Departments are responsible for ensuring that each staff member is familiar with the current business continuity plan. The Business Continuity and Disaster Recovery Department recommends that departments test the following components on a quarterly basis:

- Call trees;
- Evacuation processes;
- The ability for staff to connect remotely;
- Wireless tests; and
- Testing data ports in alternate sites.[39]

[37] "Business Continuity and Disaster Recovery Department: Testing and Exercise," North Carolina State University, http://www.ncsu.edu/ehs/BCP/phases/testing.php
[38] Ibid.
[39] Bulleted points taken verbatim from: "Business Continuity and Disaster Recovery Department: Testing and Exercise," op. cit.

Stanford University[40]

Stanford University in Palo Alto, California does not make its own business continuity plan publicly available on its institutional website, but instead provides a general plan skeleton for use by other institutions. Similar to the template material provided by the University of Maryland, Stanford offers worksheets and blank tables for departmental surveys regarding essential functions and vital records. The first worksheet, reproduced below as Table 3A, is distributed to every department or division with the following instructions:

Worksheet 1

- Task A: List all organizations functions
  - Examine organizational mission.
  - Talk to experts and former employees familiar with the organizations.
  - In Column 1, list all organization functions identified, including essential support functions.
- Task B: Identify essential functions
  - Reexamine organization mission.
  - Examine the services the organization provides to other departments.
  - Identify supporting critical processes and services in Column 2.
  - Indicate in Column 3 which functions are "essential" after considering their relationship to the organization mission.

Table 3A: Essential Functions by Department*

Column 1: All Functions	Column 2: Description of Function	Column 3: Essential Function?

* In order to conserve space, example tables only contain four lines.

Essential functions are defined by Stanford University as those processes and services that must be sustained in an emergency for fourteen days.

Once each department has completed this worksheet, the next task is to complete a separate worksheet for each essential function. This involves identifying the recovery time objective, the priority of the specific function, and the required personnel, records, and equipment that make the function possible. This separate worksheet, the format of which is reproduced as Table 3B, should be completed for each essential function.

[40] All information taken from: "Stanford University Business Continuity Planning", Stanford University, www.stanford.edu/dept/EHS/prod/general/erprep/BCP_guide.doc

Table 3B: Essential Function Support

Description of Function	Recovery Time Objective	Priority	Personnel	Records	Equipment and Systems

On the third worksheet, departmental staff are asked to prioritize essential functions. This allows continuity planning leadership to understand which functions require operation first so that appropriate resources and plans can be established. Stanford University recommends ranking priority with numbers, using higher numbers for the functions that can be inoperable for longer periods of time. The same number can be used for multiple functions if they are of equal importance.

Table 3C: Priority of Essential Functions

Essential Function	Priority

The fourth worksheet compiles a list of records that are vital for the continued operation of critical processes of each specific essential function for the first 14 days following a disruption. Table 3D solicits information detailing if the records are in paper or electronic form, and if the records are time critical and necessary within 72 hours of an emergency. Again, this worksheet should be completed for each essential function individually.

Table 3D: Vital Records Information for a Specific Essential Function

Critical Service or Process	Vital Record	Description	Form of Record	Type of Record	Time Critical?

Finally, the fifth worksheet focuses on the protection of the vital records listed above. This table provides information about storage location, how often records are backed up or revised, and specific protection methods. Vital records that lack protection beyond backup or duplicate copies may be candidates for additional protection measures. The final column allocates space to recommend further protective measures in these scenarios.

Table 3E: Vital Records Protection Methods

Vital Record	Storage Location	Maintenance Frequency	Current Protection Method(s)	Recommendations for Additional Protection (if necessary)

These worksheets and tables provided by Stanford University present a uniform and organized method for the beginning steps of a business continuity plan. Once each department has identified essential functions, critical support of essential functions, and vital records protection, this information is transferred to the continuity planning leadership personnel. The most essential functions of each department are then prioritized within the broader institutional plan, taking into account which functions are considered essential because other divisions or services depend on them to operate. Once this information has been reviewed and discussed, institution-wide plans, such as the tables used by the University of Maryland, can be constructed with consideration of all functional areas.

The University of Minnesota[41]

The University of Minnesota is an important institution to include in our study because it has over 15 years of experience in operating a business continuity plan. The University began considering a continuity plan in 1995 in the aftermath of the Oklahoma City bombing, and the administration initially asked each institutional department to develop plans for how it would react to the following three interruption scenarios:

- The department's current office space cannot be occupied, but access to records and data is possible.
- The department cannot access important data, but the current office space is available.
- The department loses a critical staff member due to illness, death, etc.

The planning scenarios were designed to incorporate several elements, including:

- The creation of off-site data records and files;
- The distribution of emergency phone lists for all employees in case of necessary after-hours communication;
- The designation of a "second-in-command" for critical employees.

Similar to the University of Maryland, the University of Minnesota requires 16 departments to complete business and operational continuity plans. These include: the Office of Budget and Finance; Building Codes; Bursar Office; Central Computing Operations; Emergency Management; Environmental Health and Safety; Facilities Management; Office of General Counsel; Housing and Residential Life; Human Resources; Networking and Telecommunications; Office of the Registrar, Research Animal Resources; Research Subject Protection; and the University of Minnesota Police Department.

The University developed a template to assist each department in creation of individual operational continuity plans. The template addresses several elements, instructing departments to enact the following:

- Identify services, business processes, applications, and normal support tools (business records, computers, telephones, etc.) that must be sustained during an interruption.
- Ascertain services, processes or applications that are not critical and may reasonably be suspended during an interruption. Determine how long the division can function without normal support tools.

[41] All information taken from: Bernard Gulachek, "Business Continuity Planning: Process, Impact, and Implications," EDUCAUSE Center for Applied Research, Jun 2005, http://www1.umn.edu/oit/prod/groups/oit/@pub/@oit/@web/documents/asset/oit_45242.pdf

- Determine minimal personnel, supplies, data, equipment, etc. that will be essential to support essential functions and recovery efforts.
- Maintain updated contact lists with the names and telephone numbers of key personnel and their recovery responsibilities.
- Identify interfaces to other operating units' continuity plans. Which departments does yours depend on to complete regular operations? Which units depend on your division to sustain regular operations?
- Ensure that all personnel with operations continuity responsibilities are trained and prepared to respond during a disaster.[42]

Further, the University created one of the first Operational Continuity Plans to support Networking and Telecommunication Services. The University's Chief Information Officer developed the idea "because he understood that the continuity of business across the institution depended on the networks and systems for which central Information Technology was responsible."[43] Development of the Networking and Telecommunications Services plan involved consideration of several issues, including: the University departments' dependence on information systems to conduct business; information technology requirements for residence halls; information technology requirements for the campus police and security center; liabilities associated with technological failures that adversely affect academics and research; basic institutional technologies such as telephone systems; aging technology in need of security updates; and liabilities associated with IP-based systems such as 911 systems and building security systems.

Outcomes and Effects

The University of Minnesota noted several positive outcomes of the business continuity planning process, which index the considerable benefits – in general – of comprehensive and ongoing business continuity planning. In the case of Minnesota, these outcomes have included:

- *Architectural design and new service rollout:* New services and technologies are now designed with failover, redundancy, recovery, risk mitigation, and business continuation as part of the planning effort and development.

- *Operational unit discipline:* Operations engineers are more disciplined in their approach to change management. Greater levels of documentation have resulted from the need for plans that continue services.

- *Customer satisfaction and credibility:* The Office of Information Technology continues to receive higher satisfaction ratings for critical services.

[42] Ibid.
[43] Ibid.

Additionally, the University has witnessed a migration to centralization, partially due to the credibility and assurances offered by the business continuity plan risk mitigation for these services.

- *Technical cultural changes:* Enterprise-wide services and technologies are expected to include business continuity plan reliability as part of the SLAs between the Office of Information Technology and other institutional departments.

- *Resource support for information technology continuity plans*: The importance of information technology continuity planning principles to the institution is underscored by the resource support given. Leaders develop an appreciation for continuity planning disciplines while participating in mock disaster exercises that test the plan's resilience in the face of well-orchestrated, simulated disasters and disruptive events.

- *Increased communication channels across the institution:* The creation of a business continuity plan requires a thorough communication plan. Both technical and administrative components of the plan create new channels of communication among different constituencies at various institutional levels which have now become standard in general operational procedures as well as in continuity planning events.

Conclusion

In conclusion of this report, we summarize its major themes in the box below.

At a Glance: Business Continuity Planning in Higher Education

- Business continuity planning is not only an essential strategy for mitigating a wide range of threats to operation. The process of planning, itself, is extensive and complex, requiring a level of inter-unit collaboration that invariably leads to improved integration of the institution.
- The timeline required for successful business continuity planning varies widely, ranging from as little as two months to as long as several years. Coordinators can improve efficiency by designating a committee and schedule of meetings early in the process.
- The most successful business continuity plans and planning processes benefit from strong support from senior administrators who communicate the value of the effort to the institution's overall mission, and who allocate sufficient funding from the beginning.
- Business continuity planning in higher education operates on two levels: the unit or departmental level and the global, institutional level. The support of outside facilitators can help with managing expectations and ensuring transparency as departmental priorities are consolidated into a college or university-wide plan.
- Regular post-implementation testing of continuity plans is critical. Testing should occur frequently, regularly, and at every level. Business continuity plans should be designed with enough flexibility to allow for refinement based on the outcome of tests and on changing information technologies.

Project Evaluation Form

Hanover Research is committed to providing a work product that meets or exceeds member expectations. In keeping with that goal, we would like to hear your opinions regarding our reports. Feedback is critically important and serves as the strongest mechanism by which we tailor our research to your organization. When you have had a chance to evaluate this report, please take a moment to fill out the following questionnaire.

http://www.hanoverresearch.com/evaluation/index.php

Note

This brief was written to fulfill the specific request of an individual member of Hanover Research. As such, it may not satisfy the needs of all members. We encourage any and all members who have additional questions about this topic – or any other – to contact us.

Caveat

The publisher and authors have used their best efforts in preparing this brief. The publisher and authors make no representations or warranties with respect to the accuracy or completeness of the contents of this brief and specifically disclaim any implied warranties of fitness for a particular purpose. There are no warranties which extend beyond the descriptions contained in this paragraph. No warranty may be created or extended by representatives of Hanover Research or its marketing materials. The accuracy and completeness of the information provided herein and the opinions stated herein are not guaranteed or warranted to produce any particular results, and the advice and strategies contained herein may not be suitable for every member. Neither the publisher nor the authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Moreover, Hanover Research is not engaged in rendering legal, accounting, or other professional services. Members requiring such services are advised to consult an appropriate professional.