Shared Responsibility for Business Continuity: The Team Approach at UCLA

Mark C. Sheehan, ECAR
Ronald Yanosky, ECAR

ECAR Case Study 2, 2007

Case Study from the EDUCAUSE Center for Applied Research
Shared Responsibility for Business Continuity: The Team Approach at UCLA
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

The mission of the EDUCAUSE Center for Applied Research is to foster better decision making by conducting and disseminating research and analysis about the role and implications of information technology in higher education. ECAR will systematically address many of the challenges brought more sharply into focus by information technologies.

Copyright 2007 EDUCAUSE. All rights reserved. This ECAR case study is proprietary and intended for use only by subscribers and those who have purchased this study. Reproduction, or distribution of ECAR case studies to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior written permission is granted by EDUCAUSE. Requests for permission to reprint or distribute should be sent to ecar@educause.edu.
Shared Responsibility for Business Continuity: The Team Approach at UCLA

Preface
The EDUCAUSE Center for Applied Research (ECAR) produces research to promote effective decisions regarding the selection, development, deployment, management, socialization, and use of information technologies in higher education. ECAR research includes
- research bulletins—short summary analyses of key information technology (IT) issues;
- research studies—in-depth applied research on complex and consequential technologies and practices;
- case studies—institution-specific reports designed to exemplify important themes, trends, and experiences in the management of IT investments and activities; and
- roadmaps—designed to help senior executives quickly grasp the core of important technology issues.

From its most recent research, ECAR published a study, Shelter from the Storm: IT and Business Continuity in Higher Education (Yanosky, 2007), to provide subscribers with empirical information about where their business continuity vulnerabilities, plans, and practices stand in relation to surveyed institutions, and what factors are associated with success in planning for the delivery of IT-dependent business services following service disruptions. Study results indicate that business continuity planning is commonly carried out among respondent institutions but that it is often incomplete and resource-constrained, and most plans are not tested.

Literature Review
Our review of the disaster recovery (DR) and business continuity (BC) literature focused particularly on the multiple standards that address these areas, including the ISO/IEC 17799 information security specification, the emergency-preparedness-oriented National Fire Prevention Association 1600 standard, and best practice frameworks such as the Information Technology Infrastructure Library (ITIL) and the Information Systems Audit and Control Association’s Control Objectives for Information and Related Technology (CobiT). In addition, we reviewed a wide range of secondary materials from DR and BC certification organizations and from the IT trade press, academic journals, and journalistic publications.

Online Survey
We e-mailed 1,615 EDUCAUSE member institutions, asking them to take our Web-based survey. Senior IT administrators at 340 institutions completed the survey. Most
respondents held the position of chief information officer (CIO) or a comparable title indicating that they are their institutions’ senior IT leaders.

**Interviews**

We supplemented survey data with in-depth interviews with 15 IT and executive leaders from higher education institutions and corporations involved in DR and BC efforts. In addition, ECAR took part in a two-day business continuity forum sponsored by Microsoft and hosted by EDUCAUSE, at which 40 attendees representing 36 institutions and other organizations discussed BC issues in a facilitated-discussion setting.

Such interviews and forums enabled us to deepen our understanding of the processes that are used for DR and BC planning and testing as well as their results. They provided insight into the factors that drive BC planning and those that inhibit it. And they provided interesting examples of how institutions approach the many challenges inherent in this complex undertaking.

**Case Studies**

Researchers conducted four in-depth case studies to complement the core study. This document presents a case study about the development of business continuity planning at the University of California, Los Angeles (UCLA).

For their many contributions to this case study, the authors wish to thank the following UCLA personnel: Sue Abeles, assistant vice chancellor/controller, Corporate Financial Services; Jim Davis, associate vice chancellor for information technology and chief information officer; Jack Ewart, director, Data Center Services, Administrative Information Systems; Paula Farrington, director, Payroll Systems and Services; Karen Melick, director, Systems, Network, Architecture, and Planning, Administrative Information Systems; Sam Morabito, vice chancellor, Business and Administrative Services; Craig Squire, director, Corporate Accounting; and Don Worth, executive director, Administrative Information Systems. Troy Jassey, a consultant with IBM Global Technology Services, also provided valuable insights.

**Introduction**

No one who is paying attention to world events in the 21st century can be unaware of the need for disaster preparedness. Threats to life and property—including IT resources and services—range from local to global in scale, and from the nuisance of brief power outages to the devastations of earthquake, hurricane, and terrorist attack. To be aware of these threats yet fail to prepare for them is obviously a mistake. Nevertheless, higher education institutions vary widely in their levels of readiness to cope with disaster, and even more so in their levels of planning to resume normal or near-normal academic and administrative services afterward.

ECAR research suggests that while BC planning is widespread in higher education, efforts are often incomplete and struggle to obtain appropriate priority. Nine of 10 ECAR survey respondents reported at least one documented BC-related procedure (out of 13 separate procedures asked about), and half reported eight procedures or more. But when asked about the status of a formal central IT disaster recovery or business continuity (DR/BC) plan, only 17 percent said they had a completed plan. More than half (52 percent) said their IT DR/BC plan was in progress, while another 26 percent said they planned to create one in the future. To be sure, respondents with in-progress plans often showed signs of substantial DR/BC readiness. On average, they had almost 90 percent of the number of documented procedures reported by those with completed plans, and many seemed to say their plans were in progress more because of concerns that procedures were out of date than because of completeness per se. This probably explains why some studies using
different categories have found higher plan possession rates. For example, the 2006 Campus Computing Survey (Green, 2006) reported that 56 percent of institutions had a strategic plan for IT disaster recovery. No study, however, has found higher education DR/BC plan completion rates as high as the 67 percent cited for companies reporting a business continuity plan in a national survey of businesses and other organizations commissioned by AT&T (Opinion Research Corporation, 2005).

Nevertheless, concern about business continuity has escalated in the past year and may still be increasing. The topic failed to place among the top 10 issues in the EDUCAUSE 2005 Current Issues Survey, but in 2006 it ranked fourth and was third among issues judged most likely to become more significant (Dewey, DeBlois, & EDUCAUSE Current Issues Committee, 2006).

The Planning Process

Developing a business continuity plan is not a single, discrete action; it’s a complex process that, once initiated, moves through many stages and eventually folds back on itself for renewal. Certain early stages determine much of what happens downstream. BC-related standards like ISO 17799, the National Fire Prevention Association 1600 standard, the IT Infrastructure Library framework, and the CoBiT specification typically describe a succession of efforts.

The first of these, and perhaps the most crucial, is assigning organizational responsibility. In the words of Troy Jassey, a business continuity consultant with IBM Global Technology Services, “A key to successful BC planning is to ensure that the right person is put in charge of the process. To ensure a consistent implementation across the enterprise, that person should be highly placed, but from an area other than IT or one of the functional areas directly involved in BC planning. And he or she should have full coordinating authority, through a steering committee or similar body, over the planning process.” This is even more important in higher education than in traditional business contexts, Jassey adds, “because educational institutions tend to be more siloed than traditional businesses.”

The first group exercise in disaster recovery and business continuity planning is risk assessment. This is typically a guided brainstorming exercise in which the threats to the enterprise—those events or conditions that might interrupt business processes—are identified. Typically, these potential threats are prioritized along two dimensions: the likelihood that a threat event will occur and the severity of the impact it will have. Subsequent steps in the planning process tend to focus on those threats that are in the high-likelihood/high-severity quadrant.

In general, the next step in the BC planning process is the business impact analysis (BIA). In this step, the owners of key business processes are asked by a facilitator, often external to the institution, to envision various types of service interruption and estimate their impact upon institutional business processes. According to IBM’s Jassey, “This stage of the process usually begins with a survey filled out by the process owners. In our role as facilitators, we then join our business expertise with the process expertise of those individuals or departments to validate the input they provide—to help keep it realistic and reasonable.”

In assessing the impact of various disasters, the BIA process establishes four classes of information:

- *Recovery time objectives (RTOs).* These indicate the length of time a business process can be unavailable before the impacts become unacceptable.
- *Recovery point objectives (RPOs).* These indicate the maximum acceptable length of time between the most recent data backup and a disruption to a system.
◆ **Financial and intangible impacts.** Financial impacts involve interruptions of cash flow into the institution, the costs of mitigating a disaster, financial penalties for failing to meet contractual obligations, and so forth. Intangible impacts deal with the safety and security of employees and students, the quality of the institution’s instruction and research, institutional reputation and image, and nonmonetary penalties for failing to meet contractual and regulatory obligations.

◆ **Application dependencies.** Most modern business applications are dependent on IT resources: systems, software, data, and personnel. Many applications are also dependent on the output of other applications, often managed by different functional areas.

Once initial estimates for these variables have been established and validated at the departmental level, the BIA process moves forward to a group validation stage, again often conducted by an external facilitator. In this session, interdependencies among business processes are identified and discussed, and consensus about impacts, RTOs, and RPOs is sought.

It is at this point that Jassey says problems often emerge. “Participants in these sessions sometimes have trouble accepting that their processes aren’t critical to business continuity. We need to remind them that criticality is not the same as importance. For example, accounts receivable is undeniably important. If you can’t take in money, you probably can’t survive as a business. But AR may not be critical in the time frame of most disasters. If AR is interrupted for a week or 10 days, the consequences may not be that severe. The AR unit can probably still recover 90 percent of revenues after an interruption like that. So at this stage in BC planning, you get people together and mutually decide which events you’re going to consider cuts or scrapes and which are broken arms.” In the sidebar “Tips for Successful Business Impact Analysis,” Jassey provides suggestions for conducting a successful BIA in the context of business continuity and disaster planning.

Once the BIA is complete, the institution moves on to the development of strategies for dealing with potential service interruptions. These strategies include steps to be taken to prevent interruptions and protect assets; procedures (including those from the institution’s emergency management plan) to be followed during a disruptive event; planned responses to the interruption, such as reversion to paper-based systems or the activation of remote IT facilities; and plans to resume normal operations after the crisis has passed. Another key outcome of this phase is a set of recovery cost estimates.

When these strategies and cost estimates are agreed upon and documented, they become the basis for resource requests and the financial planning required to ensure that the institution’s BC plans can be carried out.

This case study examines how risk assessment and BIA initiatives emerged and are moving to completion at one of the largest and most technologically complex institutions in U.S. higher education.

**About UCLA**

UCLA is a public, coeducational university established as a branch of the state university in 1919. It now has 174 buildings spread across 419 acres, and its enrollment of more than 30,000 students is the largest of any university in the state. Most of UCLA’s PhD programs rank in the top 20 for academic quality in the United States, according to the National Research Council. The university was ranked by the National Science Foundation as the number one public research university in the United States on the basis of research expenditures.

Information technology at UCLA is highly distributed. A central Office of Information Technology (OIT) manages the institutional
Business Continuity at UCLA

The Communications Technology Service (CTS) unit engineers, operates, and manages the university’s 35,000-line telephone system and its fiber-optic/ATM backbone, which networks the entire institution for high-speed Internet connectivity, voice processing, and video applications. In addition, the CTS Bruin Online unit provides UCLA students, staff, and faculty with remote dial-up and on-campus access to the campus backbone network and the Internet. The Residential Telephone Service unit and the Student Technology

IT planning and governance processes. It oversees institutional outcomes by providing oversight, facilitation/coordination, architectural frameworks for processes and technologies, assessment, planning, consultation, and analysis. It also provides direct staff support and project coordination to numerous institutional and cross-unit IT projects. It has overarching responsibility for coordinating large-scale IT initiatives across the institution and for representing UCLA in statewide IT contexts.

Tips for Successful Business Impact Analysis

On the basis of his experience in leading BIAs for IBM Global Technology Services, including that conducted at UCLA, Troy Jassey offers the following pointers to institutions following that path in the business continuity context:

♦ **Involve the right people.** A business continuity initiative is about more than IT; it is about the institution’s educational and administrative functions. While these are nearly always touched by IT, the primary function of BIA is to find out what would happen if functional units couldn’t do what they ordinarily do on a day-to-day basis. If business continuity is seen as “an IT thing,” participants might not fully engage in the process or they might put too narrow a range of business processes on the table.

♦ **Ensure high-level support.** The BIA effort should be widely understood as a key element in business continuity, and BC should be understood as a top priority for the institution. A strong top-down impetus helps ensure that adequate resources are applied to the initiative and that it gets the attention it requires from all parties involved. The leader of the BIA effort should be influential and respected, but should not come from the IT unit or any one of the functional units represented. The leader should have sufficient authority to keep the participants engaged and productive.

♦ **Establish reasonableness.** An objective facilitator can be invaluable in ensuring that the interests of all parties are addressed fairly and consistently in the BIA and other business continuity processes. A facilitator can help prevent imbalances in representation resulting from differences in participants’ personalities or status. An experienced facilitator can help the functional area representatives place the importance and criticality of their functions in an institutional perspective and can help tease out subtle interdependencies among functions.

♦ **Exercise the business continuity plan.** Business continuity is a complex practice, and at any institution it will go through stages of maturity. Because technology, people, and priorities change constantly, BIA cannot be done just once. Business continuity plans have a very short shelf life. They must be exercised regularly to mature as they should. After a plan is completed, a tabletop exercise may be a sufficient first effort in the plan’s evolution. Such an exercise might involve presenting a disaster scenario to a representative team of functional staff and having them talk through how they would respond. Gaps and inconsistencies will soon emerge and form a basis for fine-tuning the plan. Subsequent tests should be increasingly complex and comprehensive, and are particularly effective when they piggyback on institution-wide emergency preparedness exercises.
Center offer special voice and data support to customers living on campus in the residential halls. Through its Bruin Online service, CTS also provides student and administrative e-mail and calendaring applications, as well as Web hosting.

UCLA’s Administrative Information Systems (AIS) group supports most campus administrative functions in academic and administrative units. AIS manages servers, databases, applications, and services that involve the university’s administrative data. It is responsible for performance monitoring and capacity planning and sets direction in computing that both affects and reflects campus-wide needs. Like most midlevel UCLA units, AIS manages its own local area networks in close cooperation with campus business units.

Academic Technology Services (ATS) provides significant institutional research support in the form of compute-cluster provisioning and management, data storage services, data center hosting, visualization code development services, statistical consulting, and research collaboration support. While support for instructional computing is largely the province of individual academic units, the central Office of Instructional Development (OID) generally supports the university’s instructional mission and enhances teaching and learning opportunities. Through grants, programs, and services, OID promotes the effective use of current and emerging instructional methodologies and technologies. At present, course management software is highly distributed at UCLA, with nearly 30 separate course management systems in use. However, the campus has embarked on the identification of a common collaboration and learning environment.

The Threat Environment

UCLA’s location, less than 40 miles from the San Andreas fault and practically astride the Santa Monica fault (United States Geological Survey, 2006), puts the university at high risk of earthquake damage. The U.S. Geological Survey has stated that “In Southern California, scientists estimate that the probability of a magnitude 7 or greater earthquake by the year 2024 is as high as 80 to 90 percent” (United States Geological Survey, 1995).

In 1994, the Los Angeles area Northridge earthquake (magnitude 6.7) reinforced existing disaster recovery and business continuity concerns among University of California executives. The quake, along with concerns about other potential disasters, natural and anthropogenic, was a catalyst for an external audit, conducted in 1998 by Deloitte & Touche, of the University of California business recovery processes and vital records management practices. The report from that audit, in turn, was the catalyst for the formation of a business continuity planning steering committee (BCPSC), seated in the University of California Office of the President (UCOP).

The BCPSC was charged with developing a manageable, pragmatic approach by which the entire UC system could respond to the external audit findings. Its members inventoried key business functions and assessed their criticality. It evaluated both survivability and risk of failure for those functions. It then selected two functions about which to conduct campus-specific pilot studies of business continuity planning and to develop contingency measures.

Completion of a risk assessment like this is recognized as a vital step by business continuity experts because it provides a common view of risk probability and response priority that institutional departments can base unit BC planning on. In the words of UCLA Vice Chancellor for Business and Administrative Services Sam Morabito, “Frankly, based on what I’ve seen, any campus—particularly one the size of UCLA—that tells you they understand all this without doing a hard assessment is probably kidding themselves.”

Completing institutional risk assess-
ments, however, is surprisingly rare in higher education. According to Yanosky’s (2007) ECAR survey data, larger institutions (those with 15,000 or more students) report the highest proportion of completed assessments (22.2 percent). Medium-size schools (4,001–15,000 students) report an 8.7 percent completion rate, and institutions smaller than that report a rate of 6.1 percent. The most common obstacles to completion of risk assessment plans (reported by 30 percent or more of responding institutions that had not conducted an analysis) include lack of leadership support, business and academic units failing to define their business continuity needs, lack of adequate funding, and difficulty in developing campus policies and procedures. Obstacles less commonly reported are campus preference for an ad hoc approach, lack of staff expertise, and a sense that the benefits don’t justify the investment or that the threats don’t justify the effort.

At UCLA the potential for disaster is clear and is well understood by senior administrative officials. Morabito summarizes the risks: “First, we’re in earthquake country so we’re one rumble away from having a pretty big disaster here. And earthquakes happen frequently enough that it’s not like we’re planning for the 100-year storm. Second, we’re in a very urban area; we’re a large public institution with a lot of media attention on us. So if we were not able to deliver services for any length of time, it would be—from a reputational standpoint—just not good. Third, with our two hospitals, which are regional trauma centers, we have first-responder responsibility in any regional disaster, and so we have to make sure that we can continue to operate, at least in that regard. Interestingly, the obligations of our hospitals are first to the region and then to the campus, which puts a different responsibility on us.” Under guidance from the University of California Office of the President and the UCLA chancellor, Morabito and his fellow UCLA vice chancellors put a high priority on disaster readiness and business continuity preparations.

Awareness of the disaster risks at UCLA is not limited to the vice chancellors. Each of the executives interviewed for this case study not only acknowledged the risks but also noted that concerns about them are broadly shared on campus and that willingness to engage in mitigating them is enthusiastic and nearly unanimous. Because of the threat-rich environment at UCLA and the UC system’s extraordinary sense of responsibility for business continuity preparations, Morabito says, “At least for the initiatives we have in place now, funding is not the issue.” The development of campus policies and procedures has been challenged by the highly distributed nature of the UCLA IT structure. A culture of independence and autonomy in IT matters has been pervasive at the institution.

Potential obstacles have been circumvented in large part through the leadership of the Administrative Information Systems unit and the use of the campus IT governance processes. Business continuity planning was begun through AIS, which led the way with disaster recovery planning for the campus mainframe environment and sponsored an initial campus business impact analysis. For this analysis, AIS directly involved other units responsible for campus-wide IT functionality and thereby promoted a balanced, objective consultation addressing the broader campus application environment. The BIA was reviewed through the campus governance structure, through which the campus as a whole has reached a decision to commit to next steps and funding.

**Developing Specific Plans**

The threats to UCLA are not all seismic. In 1998, the first of a series of lengthy power outages in UCLA buildings brought business service continuity issues to the fore. That year the UCOP released Business & Finance
Bulletin IS-3, which dealt with IT security and specifically called for disaster recovery plans to be implemented for critical systems at each of the university system’s campuses. Soon thereafter, in parallel, the UCLA AIS and Corporate Financial Services (CFS) units began developing plans to implement IS-3 for payroll and financial aid functions. AIS acquired a copy of a disaster recovery planning template developed by the University of California at San Diego and engaged CFS in working toward a test of the payroll system on a mainframe computer housed at the president’s office in Oakland. That limited off-site test of the payroll system was conducted successfully in 2001.

In 2002 the UC system controllers pooled their energies in a second risk assessment exercise to identify four critical cash inflow and outflow functions on which to focus subsequent efforts: payroll, financial aid, accounts payable, and sponsored projects accounts receivable. The group subsequently developed a UC system-wide disaster planning template to document their plans. The owners of the four high-priority cash inflow and outflow functions used this template to develop detailed, site-specific business continuity plans, an effort completed in 2003.

In the context of this effort at UCLA, ties between the CFS, Student Affairs (financial aid), and AIS units were strengthened, and new partnerships developed. In particular, the payroll and accounts payable functional areas of CFS relied on the AIS Data Center Services group to develop robust post-disaster options for critical mainframe applications.

**Remote Warm Site**

As a critical element of its response to functional unit needs, and backed by campus funding, AIS accepted IBM’s bid to serve as UCLA’s partner in establishing a remote disaster recovery site for administrative mainframe computer functions. By April 2003, negotiations were complete and a contract for backup services was in place. An IBM facility in Colorado was selected as the location for the remote mainframe, which was to back up most of the core business processes identified by UCLA’s Business Continuity Planning Steering Committee and all of those identified by the controllers, as well as the principal student systems.

Unlike an expensive dedicated hot site, which would always be online, have up-to-date data loaded, and be available to UCLA on a moment’s notice, UCLA’s Colorado computing environment is a warm site. The required hardware is in place, but UCLA’s system software, applications, and data must be loaded before the site can be used.

UCLA’s contract with IBM includes provisions for replication of the UCLA mainframe environment in Colorado, production facilities from which UCLA systems staff can manage and use the mainframe, and an annual 48-hour test of the system. Financial details include an annual fee plus a per-day charge for mainframe use following a disaster. The contract imposes a six-week annual limit on UCLA’s use of the mainframe and production facility in the event of a disruption; usage beyond that point would be charged at a higher daily rate.

To enable its functional office staff to access the Colorado backup mainframe without an 800-mile physical relocation, UCLA has arranged for the temporary use of a cluster of networked end-user workstations at a site 50 miles from the campus.

AIS conducts full-volume backups of mainframe data each day and stores them off site. On a regular schedule, full-volume mainframe backups are archived at an out-of-state facility. In the event of an emergency (or a test of the backup system), the Colorado facility has access to the most recent of these mainframe data archives.

In addition to these remote-site-oriented activities, UCLA is now conducting upgrades
to its data center’s environmental and physical security systems that will total in excess of $2 million over four years. These upgrades will enhance business continuity by providing full redundancy of support systems and eliminating single points of failure.

Testing

In 2004, UCLA began a series of three tests to confirm that the high-priority cash inflow and outflow functions identified by the UC system controllers could be carried out using the Colorado mainframe warm site. The tests spanned 18 months.

Initially, UCLA’s remote business continuity site proved more difficult than anticipated to bring up. During the first test, in November 2004, operating system functionality and network connectivity were restored, but the mainframe application functions were not. The resolution of hardware compatibility issues and address space availability consumed too much of the 48-hour test window, and so the test had to be terminated before the applications could be launched.

A second test, conducted in April 2005, was more successful, resulting in restoration of all essential mainframe applications within nine hours. Later in the 48-hour test window, functional users ran business processes related to both payroll and financial aid. Test data were dispatched to participating financial institutions with full success.

The third test, in May 2006, resulted in full system functionality being restored in just four hours, followed by successful application tests. This test involved the disbursement functions from the prior tests and the addition of transcript production. The experience of Louisiana universities following August 2005’s Hurricane Katrina suggested that a disaster whose impact was sufficient to close the university for a semester would make transcript production a high-demand service.

In both of the early tests, UCLA engineers were on site in Colorado, working with IBM to bring the mainframe up. Operationally, the third test was conducted entirely by IBM engineers, with the UCLA disaster recovery team “looking over their shoulders.” Don Worth, AIS executive director, explains, “In an actual regional disaster we’re looking at the fact that we may have staff who can’t go to Colorado because they’re dealing with their families and those kinds of things. So that’s been our more recent focus with the IBM contract, setting it up so that IBM can act in our stead.” The success of that exercise suggests to UCLA that their mainframe environment can be brought up in the future without requiring a UCLA presence at the warm-site facility. Even if UCLA staff were available to travel to Colorado in the event of a real disaster, having IBM begin the process could cut several crucial hours off the total recovery time.

The results of the testing events outlined above suggest that an untested business continuity plan may be a liability because of the false sense of security it instills. For UCLA, testing proved essential to understanding the full complexity of the testing regime and to achieving a quick resumption of business processes that doesn’t depend on a UCLA presence.

Business Continuity Versus Distributed Computing

In UCLA’s highly distributed computing environment, the mainframe hosts a relatively small proportion, numerically, of the applications in daily use at the campus. Several administrative applications important to the university’s business processes run on separate servers, as do many additional instructional, research, and auxiliary enterprise systems. Central systems staff directly manage about 250 servers and estimate that two to three times that number are located in additional data centers around the campus, supporting other campus-wide systems. In the words of Vice Chancellor Morabito, “On a campus as
large as this one, and as decentralized as it is, the big task for us is to establish the same level of IT resiliency across the campus, and that’s what we’re trying to do next.”

Ensuring the continuity of core business processes, in particular those related to cash inflows and outflows, was UCLA’s first priority. The livelihood of faculty, staff, and many students relies on the flow of cash from the university. As is true anywhere in academe, UCLA’s obligations under state and federal government regulation, as well as its contracts with its suppliers, require prompt payment of the university’s debts.

But UCLA officials also realized that while disbursement processes are necessary, they are not entirely sufficient for the continuity of the university enterprise. This issue was brought to the fore not just by the example of Hurricane Katrina but also by a lengthy power outage at UCLA in 2005 that exceeded the capacity of the uninterruptible power supplies sustaining the mainframe and several servers. AIS system engineers were forced to decide, without benefit of written guidelines, which systems to bring down and which to keep running, a situation uncomfortable for both them and AIS.

**Business Impact Analysis**

To help provide guidelines and priorities for the system engineers and, at a higher level, to supplement the risk analyses conducted previously and take another step along the sequence of business continuity preparation, UCLA launched a campus-wide business impact analysis. In December 2005, AIS issued a request for proposals for facilitation of such a process. IBM Global Technology Services was the successful bidder, and AIS provided funding for the project. The intent of the BIA was to involve nonexecutive leaders from campus functional offices as well as the providers of central IT services (see the sidebar “UCLA Business Impact Analysis Participants”) in extending business continuity preparation campus-wide. According to AIS Executive Director Don Worth, “Participants were chosen on the basis of their ownership of automated business processes that affect the entire campus.”

The immediate purpose of the BIA was for UCLA’s business function leaders to explore the potential impacts on the university of various disasters, physical and otherwise, and to reach consensus on acceptable durations of unavailability for key operational processes. The overarching goal was to help balance the risks and impacts of disasters with the costs of mitigation efforts.

In a complex and decentralized environment like UCLA’s, there exist many serious obstacles to the successful completion of a BIA. These include:

- **Coordination.** Often a wide range of departments has systems with potentially campus-wide impact. It becomes a complex problem to identify the right participants, find times to bring them all together, and follow up to ensure that “homework” is completed on time.

- **Leadership.** Because priorities and attitudes vary from department to department, it may require extraordinary leadership to get everyone on the same page, all taking the exercise seriously.

- **Prioritization.** In the early stages of a BIA process, many departments’ representatives may think their issues alone have top priority. It consumes everyone’s time—and often their patience—to describe the range of institutional business and IT services and place them into a shared institutional perspective.

- **Enterprise vision.** Most institutions that conduct BIAs find that the providers of distributed systems are only partially aware of the full web of interdependencies among the many elements of the
campus IT infrastructure and the application suite. The establishment of final priorities must take this into account.

UCLA’s approach to this daunting task capitalized on the successes of the business continuity partnership between AIS, Corporate Financial Services, and Student Affairs. It was aided as well by the strategic positioning of the Office of the Chief Information Officer between the academic and administrative vice chancellors, and at the center of UCLA’s IT governance web. This positioning, and the personal leadership provided by CIO Jim Davis, was instrumental in getting all the disparate parties to the same table. Top-level executive support—and expectations—contributed essential credibility, momentum, and financial support.

UCLA’s BIA process began with a kickoff meeting involving all participants and continued with the distribution of a detailed survey to the participating functional areas. The completed surveys were then used as the basis for IBM-facilitated interviews to validate and expand on the responses. The surveys posed specific questions in the four key areas described above under “The Planning Process”: recovery time objectives, recovery point objectives, financial and intangible impacts, and application dependencies.

The next step was a group meeting in which all participants shared their survey responses. With the help of an outside facilitator, participants compared RTOs and discussed application dependencies. Of this open discussion Worth observed, “It was interesting to see the peer pressure at work. One of the units said they wanted a recovery point objective of 4 hours for some of their data. They were the only ones who had that requirement; everyone else had asked for 24 hours. So we’re all sitting at this big table, and when the facilitator came to that unit’s slide, where the RPO was so out of line with the others, that unit said, ‘Well, maybe we could get by with 24 hours after all.’”

Participation in UCLA’s BIA exercise was broad and enthusiastic. As summed up by Karen Melick, AIS director for Systems, Network, Architecture, and Planning, “From the big 1994 Northridge earthquake and 9/11, people developed a fear of disaster impacts, but they didn’t know how to approach preparedness. IBM supplied a methodology and an approach, and we got very good cooperation.”

Among the findings in the BIA report, the following emerged as most significant:

- **Recovery time objectives.** Of 132 processes analyzed, more than half were assigned RTOs of seven days or longer. At the other extreme, 16 percent were assigned RTOs of 24 hours or less. Most of the rest were assigned 72-hour RTOs. The most critical processes involved restoration of utilities (gas, electric, water) and services related to health, safety, and communication. Payroll and financial activities in support of contractual obligations were also high priorities.
Recovery point objectives. The process judged most sensitive to data loss was student enrollment at peak periods of registration; there the impacts on revenue and student satisfaction are clear. About two-thirds of the processes studied would be sustainable in the event of a 24-hour loss of data. Longer than that, and data integrity would be seriously impacted. About a third of processes could survive data losses ranging from 72 hours to 14 days.

Financial and intangible impact. While participants identified many potential financial impacts, they strongly agreed that the most serious impacts to the campus would be intangible, including safety and security, the quality of instruction and research, and university image, among others. The most serious financial impacts would derive from long-term interruptions in classroom and dormitory usability and from fines, penalties, and lost interest income if the campus’s computer-based finance system were unavailable. Participants broadly acknowledged that the costs of resuming normal business activities—catching up—would also be substantial.

Application dependencies. Participants widely regarded the university mainframe computer as the most critical IT system because so many campus functions rely on its databases and applications directly or indirectly.

While UCLA’s 2006 BIA met its goals, the campus acknowledges that much remains to be done. To Sue Abeles, assistant vice chancellor and controller, the disparities between various campus units’ RTOs and RPOs for highly interdependent systems suggest the need for a more collaborative, interdepartmental vetting of these key building blocks of UCLA’s strategy. “We need to have some additional conversations about people’s assumptions,” she noted. “Some units said they needed everything in four hours—and there are costs! You have to look at the risks and the cost trade-offs.” Abeles also suggested that greater executive-level participation in the BIA process could help reconcile differing points of view and establish the real campus priorities.

Included in UCLA’s BIA summary report is the following statement: “The decentralization of UCLA’s IT resources adds significant challenges and risk for implementing a consistent set of business continuity standards.” This has encouraged all units involved with campus-wide applications to commit to a campus planning effort and to seek additional resources and support for these initiatives from high-level institutional governance and leadership bodies. This commitment of resources has been made (see the “Future Directions” section). UCLA hopes to address the decentralization challenge at its source through a long-term project to reposition IT (see the sidebar “Repositioning IT”). The project’s aim is to rethink the outdated IT service dichotomy between “central” and “distributed” service models and to restructure the provision and management of IT services to reap the benefits of both models.

Gap Analysis

UCLA’s BIA exercise enabled most campus providers of automated information processes to come to consensus on application recovery priorities that acknowledged both criticality and interdependence. While the process is nearly complete, a few other campus units need to be brought into the BIA process (such as UCLA Extension, Associated Students UCLA, and Academic Planning and Budget), and the UCLA Medical Enterprise is working to refresh a previously conducted BIA.

For the future, Worth points out the need to take the institution’s business continuity planning to yet a higher level. Through its BIA, UCLA established a set of aspirational
Repositioning IT

Inspired in part by business continuity concerns, UCLA has begun a campus-wide initiative it calls Repositioning IT/Technology Infrastructure for Education and Research (RIT/TIER). RIT refers to those aspects that involve consolidation for efficiency and performance. TIER refers to those aspects that are optimized for strategic value, especially with respect to the front lines of research and instruction. This initiative is separate from the business continuity initiative described in this case study, but the two are complementary. As described by CIO Jim Davis, RIT/TIER is a funded, chancellor-level initiative intended to restructure campus networks, data centers, and communications for competitiveness, efficiency, and security in UCLA’s highly distributed IT environment. “Disaster recovery and business continuity are embedded no matter how you look at it,” Davis says. “Our disaster recovery and business continuity initiative defines what is needed and defines the approach. RIT/TIER offers an initiative to deal with structural and operational alignment to accommodate disaster recovery and business continuity goals.”

Davis is quick to point out that RIT/TIER is not a recentralization effort but rather a move in the direction of what he calls “coordinated autonomy.” “Our decentralization has given the community some opportunities it might not otherwise have had,” Davis says. “Our goal is not to build a central IT organization but to optimize institutional and local capabilities and capacities. We refer to this as building institutional layers of infrastructure, service, and accountability. At UCLA, the term centralized means central systems, provisioning, operations, and support, which excludes the capabilities of the distributed units. The term decentralized suggests that anything central is excluded, so there are two polarized ends. We’ve been looking for terminology that gets us out of that discussion, and institutional layers is the term we’ve settled on.”

In the context of enterprise messaging (EM), for example, this means putting together operational structures in which the staff in the various units have direct management authority and accountability for a number of aspects of a centrally provisioned system. RIT/TIER began with e-mail systems. Last year, Davis says, UCLA had about 50 disparate e-mail services. That number shrank by 30 percent this year, as a number of administrative and academic units joined the institutional EM service. A number of other units are poised for or considering participation.

Given the campus’s identification of e-mail as one of the systems that must be made available almost instantaneously in the wake of a disaster, systems consolidation makes sense. A few e-mail systems will be much easier to back up and restore than a large number, particularly if the disaster decreases the number of technical staff available to do the work. Similarly, a centrally maintained directory service will simplify the regular updating of user authentication information on the backup e-mail server, a key to seamless service restoration following a disruption.

Institutional layering has been applied so far to enterprise messaging, procurement, IT policy and practice, and grid computing infrastructure. It is now being applied to next-generation networking, with an emphasis on new campus buildings and remodeling projects, data center consolidation, the campus security program, and a common collaboration and learning environment.

Says Davis, “We’re being very careful not to build out these new support structures in a traditional, centralized fashion. Working from the starting point of our highly decentralized IT structure, we’ve been able to shift toward these layered services with structures that are based on both institutional and local involvement and accountability.”
process then may result in additional funding, reallocation of existing resources, and revision or reprioritization of the aspirational RTOs and RPOs.

In 2005, such a gap analysis was completed for the portfolio of applications managed by AIS. It led to the adoption of strategies associated with the warm backup mainframe installation in Colorado; the installation of an emergency generator to provide an uninterrupted power source to the UCLA Wilshire Center, where most of the central financial personnel and other key administrative personnel are housed; and the upgrade of the emergency generator for the primary campus data center, among other steps. In the next stage of gap analysis, UCLA will need to develop strategies for maintaining the continuity of many other key systems serving business functions, instruction, and research. A request for proposals has been released for the facilitation of that gap analysis and strategic planning exercise.

**Steps Forward—Facilities**

Despite all its business continuity planning activities, UCLA is actively avoiding “paralysis by analysis.” Says Melick, “We’re not waiting for the strategy to move forward in what we’re doing for our ultracritical servers. We’re already moving forward.” These steps include establishing with other campus entities local, reciprocal agreements for hot-site placement or for server and network resource sharing, with the goal of providing server capacity following a local disaster.

For example, UCLA’s campus data center is working with the hospital data center to arrange reciprocal server backup facilities. As an example of a wider-scale initiative, a reciprocal agreement has been put in place between UCLA and another, distant campus in the UC system to ensure that essential functions such as domain name service and emergency campus Web sites can be hosted at either location if the other experiences a disaster. Ultimately, the functions of 10 to 20 servers will need to be replicated in this way.

According to Worth, UCLA’s mainframe environment for central business applications has “made it really easy to pick up the whole environment and move it to Colorado in one piece. We don’t have that now on the central and departmental server side.” The lesson embedded in that fact has not been lost on the stewards of decentralized applications. In our discussions, Melick referred to a department at UCLA that is even now actively considering the migration of its applications from a server to the mainframe, purely for business continuity reasons. “They want their application to come up as soon as possible after a disaster, and they realize that we’re not going to get 200 servers back up in the first 24 hours,” Melick says. While it may seem like a step backward, this revival of interest in mainframe technology demonstrates the priority that business continuity issues have taken, relative to campus interest in independence and autonomy.

Another compromise between technology and business continuity expedience involves tape backup technologies. Jack Ewart, AIS’s director of Data Center Services, says, “On the data recovery side, we’re using older tape technology because with it we can spread out 14 or 15 tapes across 14 or 15 tape drives and in three or four hours assemble a data archive for transport to our remote storage site. If we used a single terabyte-scale tape, recovery would take much longer.”

On the other hand, AIS is also using state-of-the-art technology to make its distributed environment more conducive to business continuity preparedness. “On the distributed server side,” Melick says, “disaster recovery issues are really helping us move to virtualized servers because that makes recovery a lot easier using VMware. From an efficiency standpoint we’ve always wanted to put multiple applications on a server, but the
problem was that, for example, one application owner might need to upgrade SQL Server before another user. In a shared environment, that’s difficult. But with VMware you don’t have that issue because you have separate virtual environments. Using VMware has really helped us with disaster recovery because the hardware configurations of our primary and backup servers don’t have to exactly match anymore.”

**Steps Forward—Applications**

The UC System Joint Data Center Managers Group meets regularly to discuss IT issues common to the university system campuses and has identified three critical functions that must be kept available for each campus in the immediate aftermath of a disaster:

- authentication,
- an emergency Web site, and
- a people-registration system.

The latter, also called a people locater, is a Web-based application allowing campus personnel to record their post-disaster status and contact information. Many institutions that weathered Hurricane Katrina found such a system invaluable; those that had not deployed one wished they had. UC Berkeley is currently developing a people locater application that any UC campus can adapt and deploy.

This group also identified a backup e-mail system as an essential business continuity asset. The system must be prepopulated with, at minimum, all current campus usernames and passwords to enable the free flow of communication as the institution responds to and recovers from a disaster. In such a scenario, synchronization of account information is the big issue, Melick warns. The UC system is exploring several alternatives for such a system, including homegrown systems and innovative applications of Microsoft’s Windows Live @ edu program or a similar offering from Google.

**Future Directions**

While UCLA is well on its way to developing a comprehensive business continuity strategy, university leaders realize that there is still work to be done.

An immediate next step will be to continue current consulting engagements to complete the process begun with risk assessment and business impact analysis. As mentioned above, a gap analysis must occur to reconcile aspirational response time objectives and recovery point objectives with available resources and expertise. Top UCLA executives expect this work to be completed by the end of AY2007.

This is no small task and must be grounded firmly in institutional realities. When gaps are identified, a set of strategic plans must be developed to address them, either by compromising where possible and accepting an imperfect situation, or by taking the necessary—and sometimes difficult—steps to achieve campus aspirations.

Worth, his AIS colleagues, and representatives of other campus entities plan to form a technical group to identify and share best practices in applying business continuity principles. Campus funding has been committed to support this group of skilled technical staff from across the campus in developing strategies to plug the gaps likely to emerge in UCLA’s preparedness. Early candidates for further development are strategies for shared storage on campus and for expansion of agreements among campus and university system partners to provide reciprocal backup hardware facilities, especially for UCLA’s server-based systems. While another UC campus has placed about 10 backup servers into UCLA’s AIS machine room, UCLA itself has not yet deployed backup servers to that campus. Such activities will take priority in the coming year.

To date, much of UCLA’s progress in business continuity has been made “on the margin,” without benefit of full-time staff dedicated to those processes. To reduce the
burden of business continuity activities on existing staff, the campus has committed the resources necessary to add staff who will focus exclusively on this critical area. The university administration has asked functional area administrators to fund release time for their IT staff to participate more fully in institution-wide business continuity efforts.

UCLA sees the Colorado warm site for protection of its mainframe environment and applications as Phase I of its current business continuity efforts and considers it essentially complete. Phase II is the development of plans and processes for the protection of central and distributed server-based applications that serve whole-campus needs. By extension, a third phase would focus on protecting the many systems related to the university’s mammoth research enterprise. Individual research teams take responsibility for protection of their applications and data, but the intensity of the effort is highly variable and at present is not organized. A variety of internal and external drivers is encouraging the university to hasten the beginning of Phase III.

Lessons Learned

While UCLA’s development of a comprehensive set of business continuity practices is not complete, a solid foundation for future action is in place, and many of the difficult issues that bedevil such initiatives have been resolved. Campus IT leaders point to several factors that have enabled the institution’s success:

♦ **High-level executive support.** Both the UC president and the UCLA chancellor have provided consistent direction to the campus by setting the expectation that UCLA’s core IT systems will survive a disaster and that the university’s activities will not be long interrupted by foreseeable catastrophes. Their offices and those of the vice chancellors have provided funding to meet those goals.

♦ **Campus consensus.** Members of the UCLA community face in common the natural disasters endemic to the Southern California landscape and the anthropogenic disasters that loom over any large urban area. To an uncommon degree, UCLA has faced those threats head on, and its IT governance bodies have both acknowledged them and agreed that preparing the university for them carries a high priority. Intramural conflict and apathy proved to be less of an obstacle than some might have feared.

♦ **Peer leadership.** From its position at the hub of UCLA’s administrative IT services, the AIS unit had a unique perspective on the value and priority of BC planning. This perspective, along with the vision and energy of its key staff, made AIS the logical department to lead that effort. AIS has been the aggregator of planning strategies and logistics and has contributed generously to essential BC activities from its own budget while also funneling additional central budget monies into the project.

♦ **Personal commitment.** Much of UCLA’s BC effort has been taken on by individuals who had full-time jobs to begin with, and with support from budgets that were already overcommitted. The success of these efforts owes much to the individual and joint commitments of staff in IT and in functional areas.

♦ **Partners.** UCLA has been fortunate in finding consulting firms and facilitation services that could bring knowledge and experience to campus BC efforts. In addition, other UC system members, through the UC Office of the President, the former Business Continuity Planning Steering Committee, the IT Leadership Council, and the current Joint Data Center Managers Group, have
inspired UCLA’s efforts and provided material assistance in various ways.

- **Governance structure and processes.**
  UCLA has a well-defined governance structure and a set of processes for reviewing and endorsing campus-wide IT initiatives and committing the necessary resources. The campus has acknowledged and agreed to the roles of these governance entities and the related processes. Decisions about scope, approach, and resource commitments to address BC were made through this process. In the UCLA environment, the existence of this governance structure and its established practices was essential in establishing buy-in and commitment to proceed.

**Conclusion**

While UCLA faces an unusual number of very real and very present dangers, it is certainly not alone in that. Colleges and universities in Manhattan, as well as those in New Orleans and vicinity, have learned recently in tragic ways that while the potential for disaster may be a matter of probability—a roll of the dice—there is nothing gamelike about it when it occurs. The globalization of economies and the growing web of interdependencies among countries, institutions, and academic collaborators have put all academic institutions within a few degrees of separation from each other’s fate. By looking inward to its own business frameworks and practices, and by reaching outward to sister institutions and commercial sector partners, UCLA has extended and reinforced the connections it will need to be flexible and resilient under challenging circumstances. In this way, UCLA has provided for the rest of academe an example worthy of emulation.

**References**


