COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

500 WEST TEMPLE STREET
493 HALL OF ADMINISTRATION
LOS ANGELES, CALIFORNIA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

TELEPHONE: (213) 974-2008
FACSIMILE: (213) 633-4733

February 18, 2003

To: Supervisor Yvonne Brathwaite Burke, Chair
Supervisor Don Knabe, Chair Pro Tem
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Michael D. Antonovich

From: Jon W. Fullinwider
Chief Information Officer

David E. Janssen
Chief Administration Officer

Joan Ouderkirk, Director
Internal Services Department

J. Tyler McCauley
Auditor-Controller

Subject: **BUSINESS CONTINUITY PROGRAM FEASIBILITY STUDY**

On July 2, 2002, the Board of Supervisors (Board) directed my office, together with the Chief Administrative Office/Office of Emergency Management (CAO/OEM), Internal Services Department (ISD), and the Auditor-Controller (A-C) to prepare scope, time, and cost estimates required for development of a Countywide Business Continuity Planning (BCP) Program. Attached is a BCP Program Feasibility Study, which addresses the elements of your Board's motion and provides recommendations for moving forward.

Below is a brief summary of the background, findings, and recommendations in this report. These findings and recommendations are based on a survey of departments, review of pertinent documentation, and our analysis of industry trends and best practices. We also took into consideration the County's ability to respond to the recommendations given its current and projected fiscal condition. In this context, we sought to provide realistic, cost effective and achievable solutions leading to the restoration of critical services in the event of a significant disaster.

BACKGROUND

BCP provides a structured approach to deal with the consequences of the loss of critical services, facilities, resources, or operational processes in the event of intermittent outages or catastrophic disasters. It is a compilation of individual recovery or contingency plans, coordinated through a comprehensive management plan. Simply put, BCP describes how an organization will continue to function and provide critical services until normal facilities and resources are restored after a disruptive event.

The County is located in one of the most disaster prone areas in the United States and led the nation in federal disaster declarations in the decade of the 1990s, with nine declared disasters, including earthquakes, floods, wild fires, and civil unrest. It is located in one of the world's most seismically active areas, with a historical record of frequent disruptive earthquakes. The County's risk to these known threats coupled with the terrorist attacks on September 11, 2001, has raised awareness to the importance of developing a countywide business continuity plan.

The need for a comprehensive BCP Program has been identified by your Board as well as by the County's cyber-terrorism working group and Auditor-Controller reports. In addition, proposed regulatory requirements under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 call for the development of business continuity/disaster recovery plans.

FINDINGS

Business recovery planning is currently conducted individually by each department with no coordinated effort at the countywide level. No clear recovery priorities are in place to coordinate the County and departments' recovery related activities and to guide the orderly restoration of County services and processes. As a result of these and other issues, the County may not be able to restore operations within identified recovery timeframes following a large disruption.

An analysis of the County's business continuity preparedness identified the following issues related to efforts to recover critical, time-sensitive business processes and functions following a disaster.

- **Lack of comprehensive disaster recovery and business continuity plans.** A significant number of departments had no documented plans and of those in place, the majority of respondents deemed them insufficient. Moreover, findings in audits by the A-C and KPMG LLP noted that the County lacked comprehensive plans to recover and restore critical systems in the event of a disaster.
- **Insufficient testing of existing plans.** Many departments reported that their plans were not tested regularly to ensure that recovery of services and critical data were achievable.
- **Existing plans focused only on recovery of information technology (I/T) assets.** Many plans are focused on recovery of technology assets and had not included recovery of critical programmatic and business work processes.
- **Existing disaster recovery planning is narrowly focused.** The County's disaster recovery activities have traditionally focused largely on restoration of mainframe resources

at the central data center. Critical data on midrange computing resources at the County's central data center and distributed systems hosted by departments may be largely irretrievable if facilities were destroyed, thus impairing restoration of data and services to constituents.

- **Loss of services could have significant consequences.** The loss of County services could have life and safety implications and possible legal and financial exposure if they were unavailable for a long period of time or impacted due to a major disaster.
- **Existing County emergency management planning has focused chiefly on disaster response and early recovery.** Past planning has focused on emergency response and early recovery, and has not adequately addressed recovery of County services and processes that are not essential to a disaster response. CAO/OEM has taken steps to address this weakness, but more actions need to be taken to provide coordinated business recovery of County services and processes.
- **Lack of recovery priorities and shared disaster recovery resources.** County recovery priorities were developed after the Northridge Earthquake for prioritization of building inspections and reconstruction, however, the County lacks clear recovery priorities to ensure the orderly restoration of services that complicates recovery from a disaster. Also, no shared disaster recovery resources (e.g., alternate work locations, alternate I/T sites, off-site storage) are available to assist department recovery efforts.
- **The County's exposure to potential threats is increasing.** The September 11, 2001, terrorist attacks demonstrated how vulnerable organizations can be even to the most unthinkable events.
- **Regulatory mandates will necessitate a commitment to BCP.** Proposed HIPAA security regulations will mandate a commitment to BCP.

Of interest in reviewing departmental plans was their focus on recovery of I/T related assets, however, there was no relationship to the identification or resumption of services. While I/T may be important, it is only an enabler for the delivery of services. The concept of a service centric BCP is a critical redefinition of how the County responds in the event of a significant/extended outage.

RECOMMENDATIONS

A single major event can jeopardize the delivery of critical services to the County's residents. Recognizing the need to continue delivery of these services, the County must establish a Countywide BCP Program to provide for the identification and timely restoration of critical services in the event of catastrophic disaster.

While we undertook efforts identifying costs to hire a consulting firm to assist in coordinating and implementing a comprehensive BCP program, we are recommending an internally staffed effort using only selective consultative assistance to augment current County expertise. This approach will ensure that BCP becomes a department responsibility and that plans are developed and in place that will enable the recovery of critical services within established timeframes.

As the County moves forward to implement a BCP Program, it must have a strong commitment and support from the Board and County executive management. Additionally, an established organizational structure must be put in place to implement and maintain the BCP Program. This organization structure would build on the County's existing emergency management organization.

The following are recommended initial actions that the County should take to implement an effective Countywide BCP program.

- Direct each department to participate in the development of their component of a Countywide BCP Program. Further, it is recommended that once the BCP is developed, it should be tested and validated annually.
- Establish a County BCP Steering Committee to oversee the development, implementation and maintenance of the program. The BCP Committee would be chaired by CAO/OEM with support from the CIO, ISD and A-C.
- Approve the acquisition or internal development of software to facilitate the management and maintenance of departmental plans. This will allow for improved visibility leading to the identification and maximization of potential shared resources.
- Secure a consultant to assist in the development of a formal framework for documenting and maintaining a department and Countywide BCP Program.

FISCAL IMPACT

We estimate that $400,000 in funding is required to cover the acquisition or internal development of BCP software and consulting services to assist in the development of a formal framework. The acquisition of BCP software tools and the recommended consulting engagement will require a separate solicitation or procurement apart from the BCP Request for Information (RFI) discussed in this report. The RFI was issued solely for informational and planning purposes.

This initiative will be funded with budgeted appropriation for County information security or the Information Technology Fund (ITF). The expenditure of ITF funds in amounts greater than $100,000 requires formal approval by the Board. It should be noted that there might be additional costs as technology-based infrastructure is identified to support the actual implementation of BCP recovery solutions.

We anticipate that approximately two months is required to obtain a consultant to assist in the development of a workable BCP framework and between four to six months to acquire or develop a software solution for the management and maintenance of departmental BCP data. For planning purposes, we project the implementation of a Countywide BCP Program within 18 months. However, testing, validation, and refinement of plans will be an ongoing task.

If you have questions, please contact Jon Fullinwider, CIO, at (213) 974-2008, or in his absence, your staff can contact Bill Butler, CAO/OEM, at (323) 980-2258 or Gregory Melendez, of the CIO, at (213) 974-1710.

JWF:JW:GM:ygd

Attachment

c: Sharon Harper, Chief Deputy, CAO
Constance Perett, Administrator, CAO/OEM
Chair, Information Systems Commission
BCP Program Working Group

P:\Final Documents\CIO\BCP\boardbcpreportcovermemovfinalversion_0218_03.doc
Created on 2/18/2003 11:54 AM

County of Los Angeles
Chief Information Office

Business Continuity Planning Program

Feasibility Study

Table of Contents

1.0 Introduction

A. Background

The County of Los Angeles (County) is located in one of the most disaster prone areas in the United States and led the nation in federal disaster declarations in the decade of the 1990s, with nine declared disasters, including earthquakes, floods, wild fires, and civil unrest. It is located in one of the world's most seismically active areas, with a historical record of frequent disruptive earthquakes. The County's risk to these known threats coupled with the terrorist attacks on September 11, 2001, has raised awareness to the importance of developing business continuity and recovery plans.

On July 2, 2002, the Board of Supervisors (Board) directed my office, together with the Chief Administrative Office/Office of Emergency Management (CAO/OEM), the Internal Services Department (ISD), and the Auditor-Controller (A-C) to prepare scope, time, and cost estimates required for development of a Countywide Business Continuity Planning (BCP) Program and report back to your Board within 120 days. The genesis of this Board motion was a June 2002 A-C report on ISD's plan for Disaster Recovery of the County's main data center assets. The report identified weaknesses in both ISD's and the County's ability to recover its operations during a disaster.

The need for a formal and comprehensive BCP Program has also been identified by:

- The CIO in leading the County's cyber-terrorism working group. This working group was formed after "Code Red", "Nimda" and the terrorist attacks of September 11, 2001, as part of an overall effort to educate and improve the County's ability to respond to cyber-terrorism. The group identified a business continuity program as an integral part of an overall countywide security program to respond to the increasing range of cyber threats.

- KPMG LLP was hired by the A-C to audit the County's general-purpose financial statements for the year ended June 30, 2001. In their April 30, 2002, management letter, they identified that the County lacks a formal organization-wide Disaster Recovery Plan for key systems throughout the County and network connectivity that could significantly impact the County's ability to recover its operations during a disaster.

In addition, the County as a healthcare and mental healthcare provider must comply with regulatory requirements under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that calls for development of business continuity/disaster recovery plans. Proposed HIPPA information technology (I/T) security provisions identify system security measures for the electronic transfer of patient records, and require that a disaster recovery and business continuity plan be in place. Under HIPAA, healthcare organizations are required to maintain business continuity policies, procedures and practices to achieve compliance. Additionally, they should evaluate their computer systems and network design to certify that the appropriate security measures have been implemented and to both guard and ensure data integrity, confidentiality and availability.

B. Study Activities

The County's BCP Program working group conducted the following tasks to assess the County's current environment and to collect relevant information to document scope, time and cost estimates for development of a Countywide BCP program. These tasks included:

❑ Developing and distributing a BCP questionnaire to County departments and related agencies to gather requisite information.

- ❑ Preparing and distributing a Request for Information (RFI) document to identify BCP practice methodologies and to gather cost and time estimates for implementing a comprehensive Countywide program.

- ❑ Developing a proposed BCP Program framework and recommendations for actions leading to a comprehensive Countywide program.

C. Organization

This document presents a status of the County's BCP efforts and recommends areas for improvement. It is organized in the following sections:

- A definition of BCP and its importance to the delivery of County services.

- A discussion of potential threats that can occur in the County.

- An analysis of BCP questionnaire results and discussion of findings.

- An analysis of the results of the RFI that was prepared and distributed to the vendor community to assess the time and cost of developing a Countywide program under the direction of a recognized BCP consultant.

- An identification of recommended next actions.

2.0 County Service Delivery and BCP

A. County Services

Citizens and families of Los Angeles County depend on the County for many important services. The County provides critical health, public health, mental health, and substance abuse services to indigents; provides emergency and fire services; prosecutes, jails, and supervises most criminals; operates libraries; works to protect children from abuse; maintains roads and dams; and serves its residents in many other ways.

Within the California governmental structure, the County functions in two roles, serving in place of a municipality by providing municipal services to its unincorporated areas and as an agent of the State in the administration of programs (e.g., health, social services, and criminal justice programs). In addition, the County serves 58 "contract cities", which rely on the County to provide municipal-type services on a contract basis. These include contracting for police protection, fire protection, public works, and library services.

For the purposes of this study, we asked County departments to identify "critical" services that they provide. This identification of critical services was made following an assessment of potential impacts to the public and County if the services were lost or interrupted in the event of a disaster or extended event.

Many of the critical services carried out by departments are directly tied to the availability of resources. In the event a major disaster causes a loss of these resources, the services may be unavailable or may not be delivered in a timely or effective manner causing significant consequences to citizens in need of those services[1]. These resources may include:

- **People** – both the County's staff and people external to the County that may be critical to delivery of the service.
- **Infrastructure** – buildings, communications, and other property used by the County to deliver its services.
- **Equipment and supplies** – assets, systems, and consumables that are used by County staff to deliver the services.

An important resource identified in this report is I/T. I/T was also the focus of the A-C audit, noted in the KPMG LLP management letter as well as federal HIPAA regulations. The department survey identified that the majority of essential services are directly tied to I/T and related resources. Beyond critical systems and their ability to be recovered in a timely manner, local services such as electronic mail (e-mail) and word processing applications were deemed critical to providing services and important communications.

I/T will become increasingly more important as the County seeks to implement the goals, strategies, and objectives identified in the County's Strategic Plan. The plan requires that County services and programs be more accessible, responsive and efficient. Additionally, it identifies the need for collaboration and sharing of information and solutions as a priority. The use of I/T will be a major enabler for County departments to achieve these outcomes.

B. Business Continuity Planning

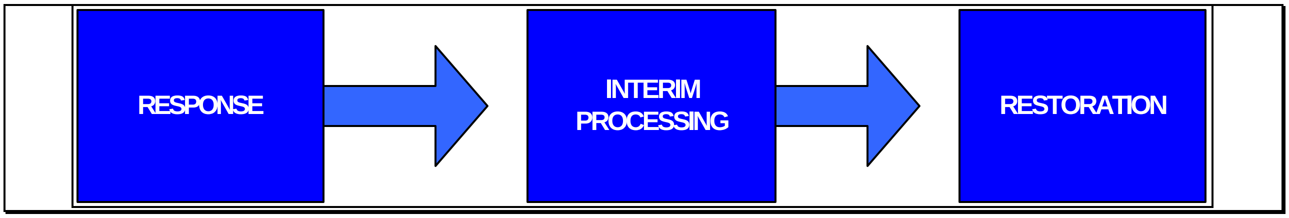
Business Continuity Planning provides a structured process and approach to deal with the consequences of the loss of critical facilities, resources, or operational processes in the event of intermittent outages or catastrophic/extended disasters. It is a compilation of individual recovery or contingency plans, brought together with an overarching management plan to coordinate the resumption of pre-identified services and processes. BCP describes how an organization will keep functioning until normal facilities and resources are restored after a disruptive event. It includes disaster response plans that are service area specific, operational recovery plans, as well as restoration and transfer of operations plans and guidelines, as appropriate.

BCP addresses the question "If the County's time sensitive services and business processes were to be interrupted, how fast could they resume?" It also enhances the County's ability to provide a minimum level of services in the event of failure to access key resources.

BCP identifies specific strategies to overcome disruptions needed to address the stages necessary for complete recovery. The stages of recovery are identified in Figure 1.

[1] The County has mutual aid agreements in place to supplement existing emergency police, fire and public works services following a major disaster.

FIGURE 1
STAGES IN RECOVERY OF BUSINESS OPERATIONS



Each phase is defined as follows:

- **RESPONSE** – the period of time from the disaster declaration until critical services and processes have been re-established using strategies documented in the business continuity plan.
- **INTERIM PROCESSING** – the period of time that services are provided via alternate processes and resources.
- **RESTORATION** – the period of time it takes the organization to return to its normal operation from using alternate processes and resources.

Gartner Group, a leading I/T research and consultancy firm, defines BCP (See Figure 2) as a process with five essential components:

- **Disaster Recovery** – Plans for the orderly restoration of computing and telecommunication services.
- **Business Resumption** – Provides workaround procedures for recovering business operations, used until the processes are recovered.
- **Business Recovery** – Plans complete recovery of business operations, including the people, workspace, non-I/T equipment and facilities.
- **Contingency Planning** – Planning for how to respond to various external events.
- **Crisis Management** – The overall coordination of an organization's response to a crisis to avoid or minimize damage to its ability to operate.

FIGURE 2
BCP COMPONENTS

	Disaster Recovery	**Business Resumption**	**Business Recovery**	**Contingency Planning**
Objective	Mission-critical applications	Business process workarounds	Mission critical business processing	External event
Focus	Site or component outage (external)	Application outage (internal)	Site outage (external)	External event forcing change internally
Deliverable	Disaster recovery plan	Alternate processing plan	Business recovery plan	Business contingency plan
Sample Event(s)	Fire at data center, server failure	Payroll system down	Electrical outage in building	Main supplier cannot ship due to its own problem
Sample Solution	Recovery site at a different location	Manual procedure	Recovery site in different power grid	25 percent of backup of vital products; backup supplier
Crisis Management				
Overall coordination of the organization's response				

Source: Gartner Group

The following section will describe the potential threats the County faces that could impact the delivery of services.

3.0 Potential Threats Facing the County

A. Discussion of Potential Threats Facing the County

There is no scientific measurement method that can provide the precise probability of experiencing a disaster that could cause a loss in the delivery of County services and functions. However, the County, with its varying topography and geographic location, is vulnerable to a wide range of natural threats. The County is also vulnerable to human threats and damage to infrastructure.

In the 1990s, nine major disasters were declared for various kinds of events: floods, earthquakes, wildfires and civil disturbances. These incidents include:

- El Nino Flood in February 1998;
- Calabasas Fires in October 1996;
- California Winter Storms in March 1995;
- Northridge Earthquake, 6.7 on the Richter Scale, in January 1994;
- Southern California Fire Storms in October 1993;
- Los Angeles Civil Unrest in April 1992; and
- Winter Storms in February 1992.

New realities from the September 11, 2001, terrorist attacks in New York City, Pennsylvania, Washington, D.C., as well as from less physically destructive but economically significant cyber attacks, such as Code Red and NIMDA[2], and the recent SLAMMER Worm, have added to potential threats facing the County.

For the purposes of this report, we have classified the types of potential threats to the County as natural, human and technical threats. Figure 3 identifies a list of potential types of exposures.

[2] Code Red infected 150,000 computer systems in 14 hours, causing billions of dollars in losses. NIMDA ("ADMIN" spelled backwards) attacked an estimated 86,000 computers causing significant problems in well-protected industries, forcing firms offline, shutting down customer access, and requiring some firms to rebuild systems entirely. The actual financial cost of the NIMDA attack is unknown because there is no consistent method to track such damage. The number of attacks has increased: Carnegie Mellon University's Computer Emergency Response Team's [CERT] Coordination Center reported approximately 3,700 attacks in 1998 and reported over 82,000 attacks in 2002.

FIGURE 3
POTENTIAL TYPES OF EXPOSURE

Natural Threats	Human Threats	Technical Threats
• Seismic Event	• Improper handling of sensitive data	• Cyber terrorism
• Fire	• Unauthorized physical access or unauthorized access to data or theft of data	• Computer crime
• Flooding	• Malicious damage or destruction of physical assets, software or data	• Power failure/fluctuation
• Extreme Weather	• Bomb threats	• Heating, ventilation, plumbing or air conditioning failure
• Tsunami	• Civil disturbance	• Failure of system hardware and/or application software
	• Sabotage	• Telecommunications failure
	• Biological or chemical contamination	• Loss of physical access to resources
	• Radiation contamination	• Gas leaks
	• Terrorist acts	• Communications failure – internal/external

The County is exposed to various threats and vulnerabilities described above. Some of them come without warning. Most of them may never happen. The key is to be prepared and to be able to respond to the event when it does happen.

The next section will discuss how well the County is currently positioned to resume operations following a disruptive event.

4.0 BCP Questionnaire Results and Findings

A. Background

A BCP questionnaire was prepared and distributed to all County departments as well as Community Development Commission, the Los Angeles County Employees Retirement Association and the Unified Court on August 27, 2002.

The information requested from departments and agencies included:

- Identification and classification of key services and processes.
- Impacts resulting from the inability to conduct operations for a prolonged period of time.
- Current state of preparedness to resume business operations following a disruptive event.
- Dependent I/T support for resumption of time-sensitive services.

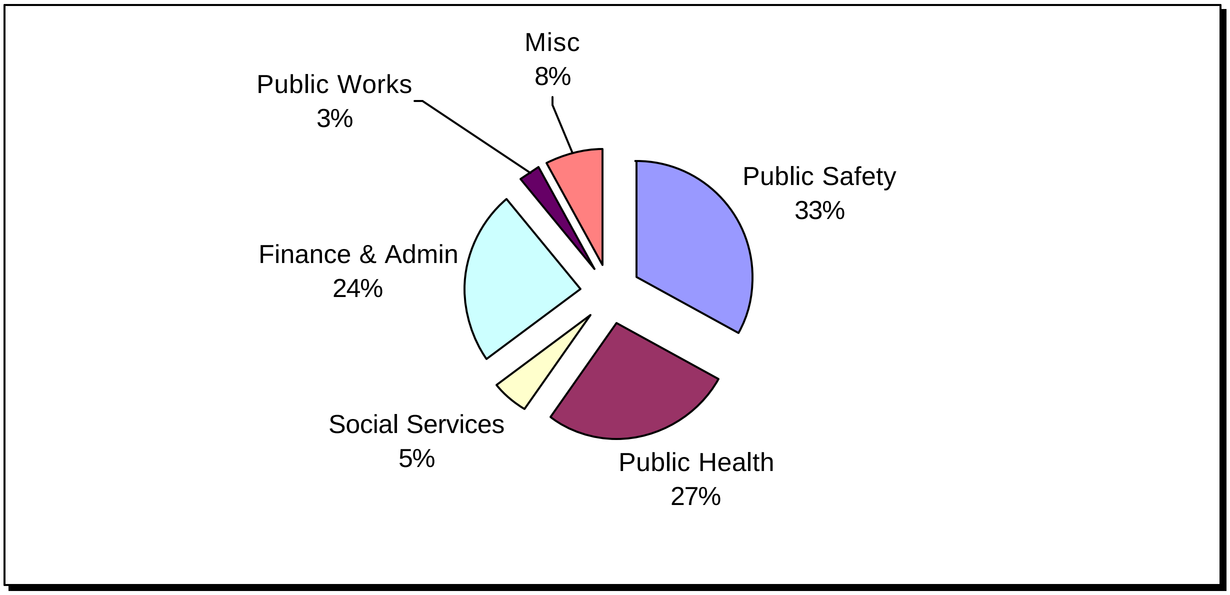
BCP questionnaires were distributed to 40 County departments and agencies. Thirty-nine of the responses were received and used in developing the following information.

B. Questionnaire Results

Respondents identified 623 mission critical services and processes that would have significant impact to the public and the County if they were interrupted or unavailable for varying periods of time.

Figure 4 illustrates these critical services by functional category. Of the services identified, the majority of the services were related to public safety (33 percent) and public health (27 percent) followed by finance and administration (24 percent), miscellaneous (8 percent), social services (5 percent) and public works (3 percent).

FIGURE 4
DISTRIBUTION OF CRITICAL SERVICES BY FUNCTIONAL CATEGORY



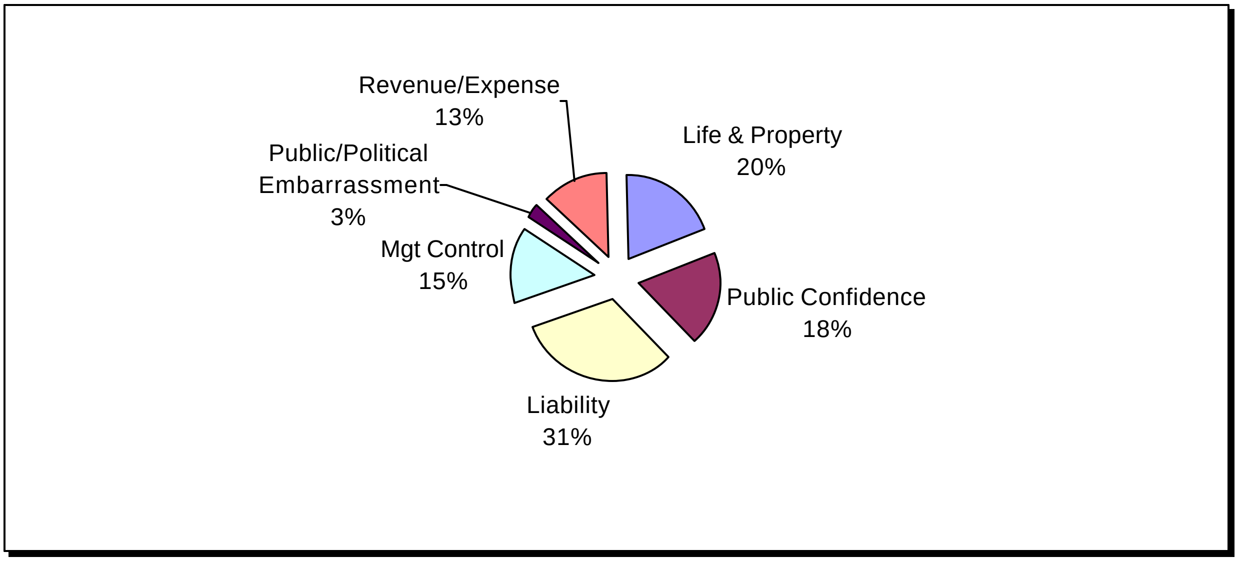
Departments were asked to evaluate the potential implications of the loss of these critical services and processes. This assessment required departments to evaluate how vital the service/process was to the public and the department, as well as the operational impact to the County.

Their responses included:

- Whether the loss could impact life and property.
- Whether it could have financial impact through either revenue loss or increased expense.
- Whether its loss could result in violation of regulatory requirements, any contractual liabilities, or whether it could create any legal issues.
- Whether it could affect the confidence of citizens.
- Whether it could result in loss of management control.
- Whether it could result in public or political embarrassment.

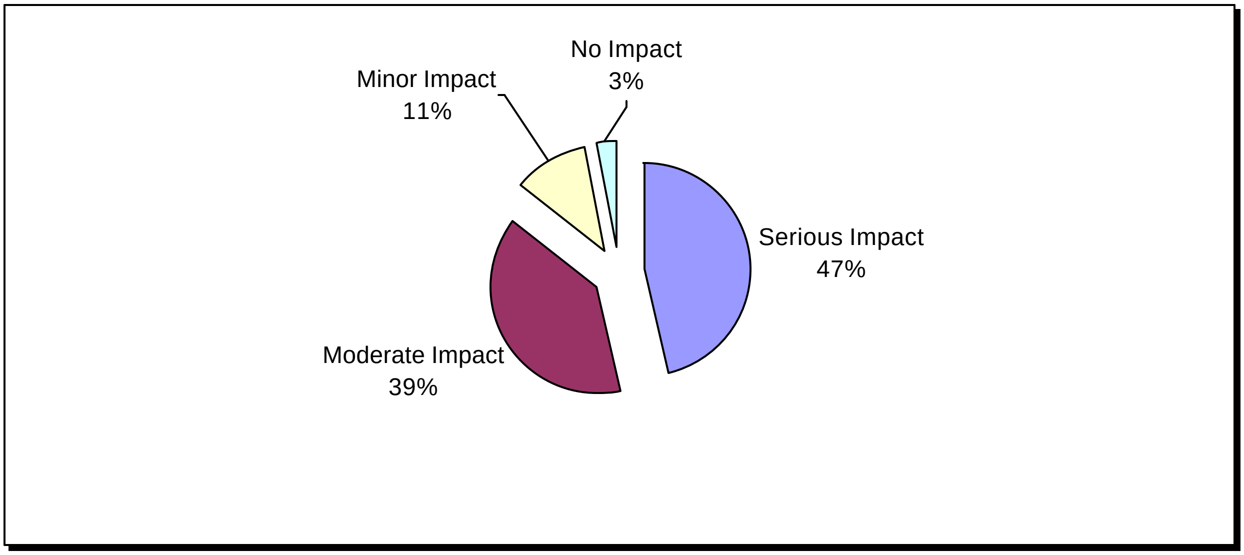
Figure 5 depicts the assessment of potential effects if these critical services were not available. Departments reported the major impact would be potential regulatory, statutory or contractual liability (31 percent), followed by loss of life and property (20 percent) and loss of public confidence (18 percent). Other potential impacts included loss of management control (15 percent), loss of revenue or increased expense (13 percent) and public or political embarrassment (3 percent).

FIGURE 5
POTENTIAL IMPACT FROM LOSS OF CRITICAL SERVICES



When departments were asked to rank the potential impact of the loss of these critical services to the public. More than three-fourths of the services identified would have serious to moderate impact on the public if the services were lost or disrupted (See Figure 6).

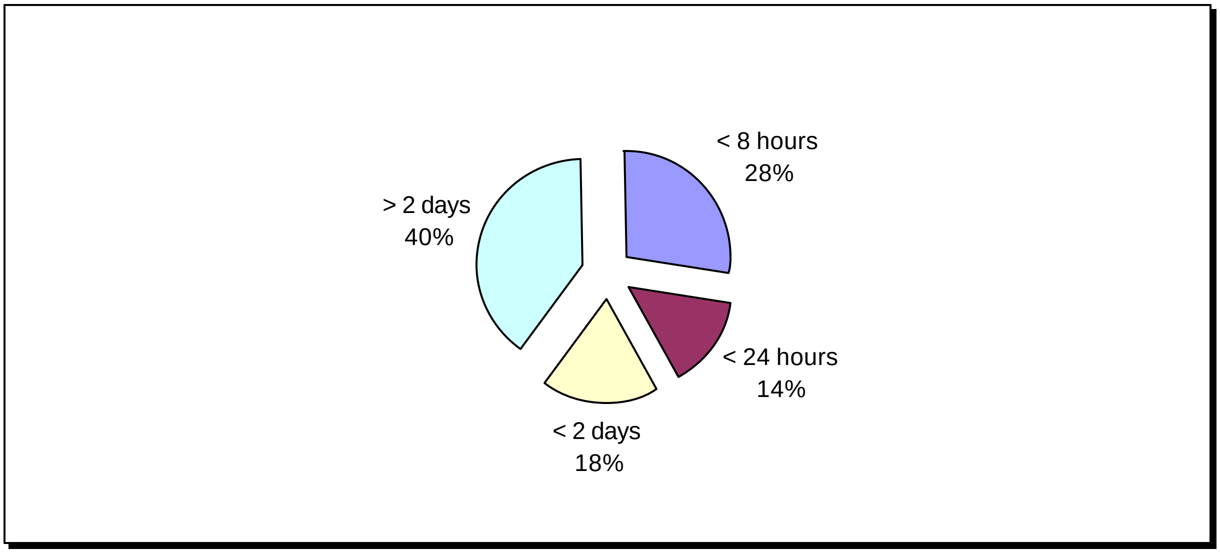
FIGURE 6
POTENTIAL IMPACT TO THE PUBLIC FROM LOSS OF CRITICAL SERVICES



Following an outage or extended event, departments can often operate and deliver services for a short period of time using fewer resources than would be available under normal operating conditions. However, at some point a full compliment of resources (i.e., staffing, equipment, supply configurations, etc.) will become necessary requiring recovery procedures to be invoked. This point of time is referred to as critical recovery time (CRT).

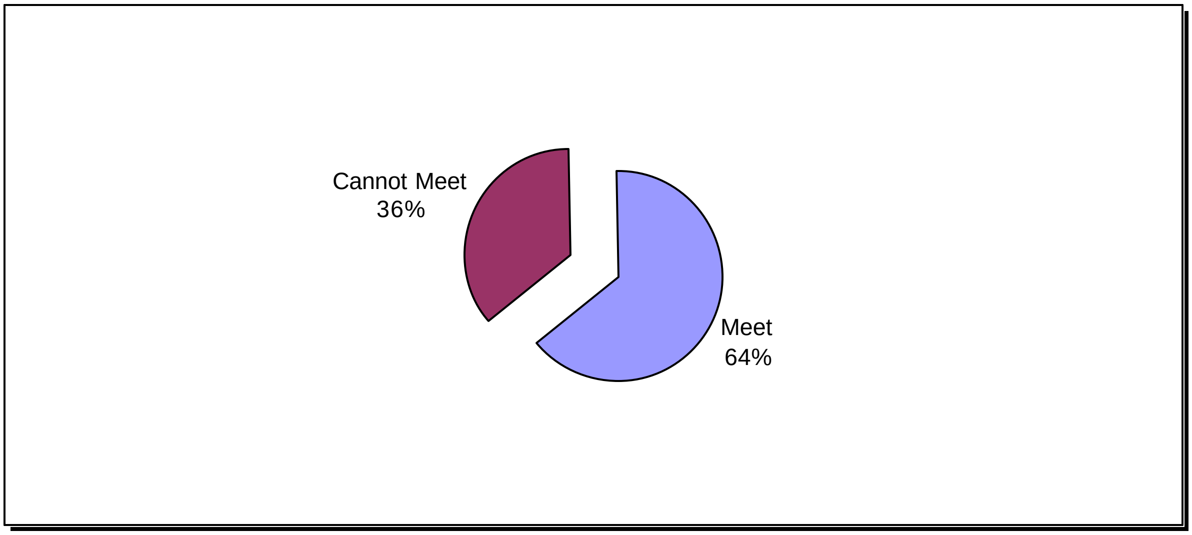
Departments were asked to determine CRTs for their identified services or processes. This assessment was based on the overall impact of the loss of the service/process and impact of the loss of corresponding activities and resources to support the process. Departments indicated that 42 percent of their services needed be to recovered in less than 24 hours with 60 percent requiring restoration within 48 hours. The remaining 40 percent of departmental services could be recovered in a time period greater than 48 hours (See Figure 7). Of particular concern was the identification that 28 percent of departmental critical services and processes had CRTs of eight hours or less.

FIGURE 7
CRITICAL RECOVERY TIMES FOR SERVICES



When departments were asked about their ability to meet the CRTs identified for their services or business processes, only 64 percent indicated that they could meet the recovery times (See Figure 8).

FIGURE 8
ABILITY TO MEET CRITICAL RECOVERY TIMES

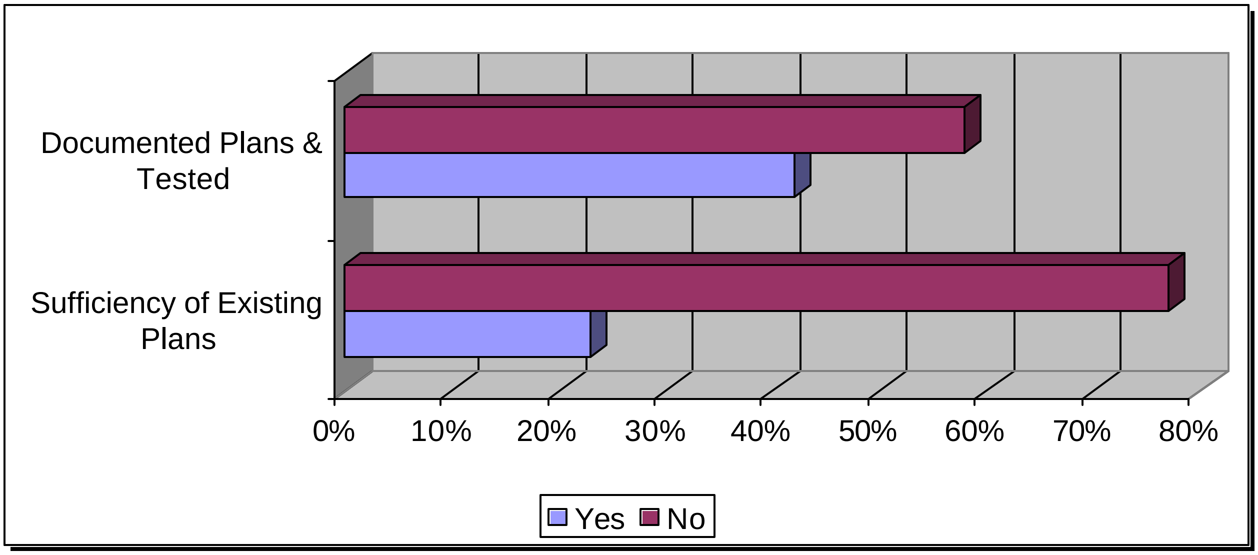


One of the major lessons learned from the September 11, 2001, terrorist attacks was that many business continuity and disaster recovery plans were inadequate. The principal inadequacies of the plans included:

- Not updated to reflect current configurations, applications, processes, and capacity needs.
- Dependence on personal knowledge of experienced staff members.
- Inadequate links between business units and the corporate organization, and with customers, suppliers, and business partners.
- Not tested recently, or sometimes not at all.

To get an overall understanding of the current status of BCP in the County, departments were asked a series of questions regarding their current plans in addressing a potential catastrophic outage. When asked if they had documented resumption, recovery and contingency plans in place that were maintained and tested regularly (within the last year), only 42 percent of the departments responded that plans were in place and tested. When queried about the sufficiency of their existing plans in the event of a significant outage, only 24 percent considered them sufficient (See Figure 9).

FIGURE 9
ASSESSMENT OF EXISTING PLANS

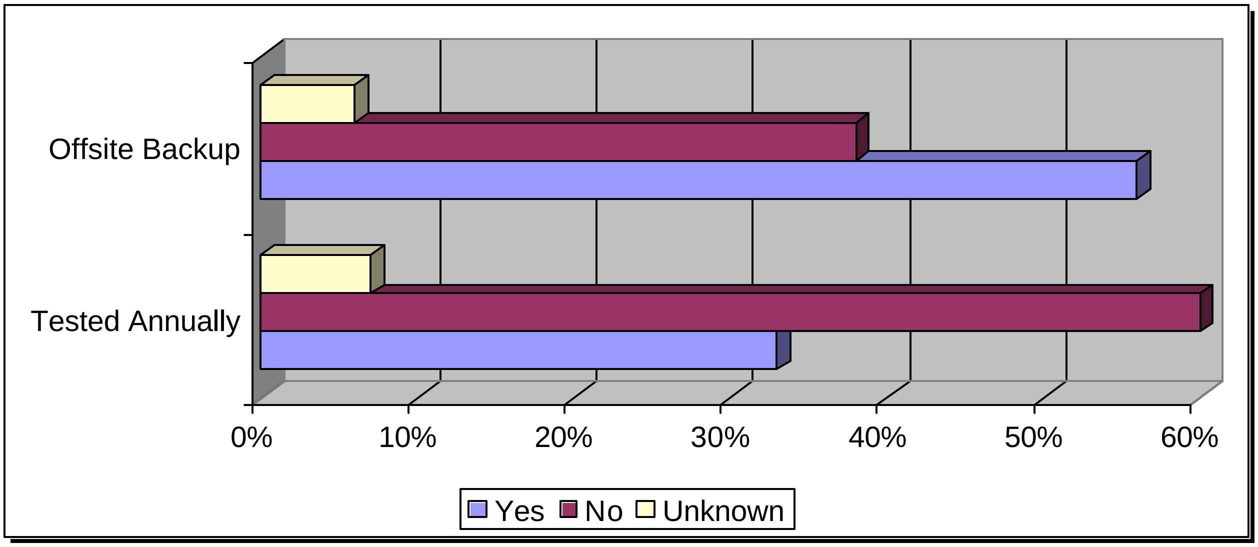


The majority of the services and processes identified by departments are heavily reliant on I/T to meet programmatic and business objectives. Respondents identified approximately 569 supporting I/T applications and systems. Many of these applications/systems are distributed systems hosted and operated by departments outside of the County's main data center.

Another lesson learned from the September 11, 2001, terrorist attacks was that most damage and loss of data and applications occurred in distributed systems. Many were inconsistently backed up and lacked operational documentation. Often, primary and backup servers were in the same room along with backup tapes from the previous day locked in file cabinets rather than being transported to offsite storage facilities. Insufficient testing of backup and recovery procedures was also a common shortfall. Many applications were not regularly tested to ensure that data could effectively be reassembled. Bottom line, many companies residing in the World Trade Center and surrounding areas were not able to recover critical information or data assets, resulting in loss of revenues and their inability to return to providing customer-based services.

When departments were asked if their I/T applications and systems had established (formal) backup and recovery procedures, approximately 56 percent indicated they had system data and software backed-up and stored offsite far enough away to reduce the likelihood that both sites would be affected by the same outage. When asked if backup and recovery procedures had been tested within the last year to ensure that system recovery was achievable, only 33 percent of the departments indicated their systems and applications were tested annually (See Figure 10).

FIGURE 10
I/T BACKUP AND RECOVERY PLANS



C. Summary of Findings

Based on the survey results as well as the A-C audits and other pertinent documentation, the County may not be able to restore operations within identified recovery time frames following a large regional event. The following are issues currently facing the County:

- **Lack of comprehensive disaster recovery and business continuity plans**. Survey results indicated a significant number of departments had no documented plans and of those in place the majority of respondents deemed them insufficient. Moreover, findings in audits by the A-C and KPMG LLP noted that the County lacked comprehensive plans to recover and restore critical systems in the event of a disaster.
- **Insufficient testing of existing plans.** Many departments reported that their plans were not tested regularly to ensure that recovery services and critical data were achievable.
- **Existing plans focused only on recovery of I/T assets**. Many plans are focused on recovery of technology assets and had not included recovery of critical programmatic and business work processes.
- **Existing disaster recovery planning is narrowly focused**. The County's disaster recovery activities have traditionally focused largely on restoration of mainframe resources at the central data center. Critical data on midrange computing resources at the County's central data center and distributed systems hosted by departments may be largely irretrievable if facilities were destroyed, possibly impairing restoration of data and thus services to constituents.
- **Loss of services could have significant consequences**. The survey results indicated life and safety implications and possible legal and financial exposure if County services were unavailable due to a major disaster.

- **Existing County emergency management planning has focused chiefly on disaster response and early recovery.** Past planning has focused on emergency response and early recovery, and has not adequately addressed recovery of County services and processes that are not essential to disaster response. CAO/OEM has taken steps to address this weakness but more actions need to be taken to provide coordinated business recovery of County services and processes.
- **Lack of recovery priorities and shared disaster recovery resources**. County recovery priorities were developed after the Northridge Earthquake for prioritization of building inspections and reconstruction, however, the County lacks clear recovery priorities to ensure the orderly restoration of services that complicates recovery from a disaster. Also, no shared disaster recovery resources (e.g., alternate work locations, alternate I/T sites, off-site storage) are available to assist department recovery efforts.
- **County exposure to potential threats is increasing.** The September 11, 2001, terrorist attacks demonstrated how vulnerable organizations can be even to the most unthinkable devastation.
- **Regulatory mandates will necessitate a commitment to BCP**. Proposed HIPAA security regulations will mandate a commitment to BCP.

The previous discussion has clearly articulated the need for an effective Countywide BCP program. The following sections will discuss the RFI that was prepared and distributed to identify the cost and scope of implementing a program under the direction of a consulting engagement.

5.0 BCP RFI Results and Findings

A. Background

An RFI was prepared and distributed to the vendor community on November 12, 2002. The purpose of the RFI was to identify proven BCP methodologies, to identify scope and cost information requested by the Board, and to assist the County in developing a Countywide BCP program. We issued the RFI solely for informational and planning purposes. Any County decision to engage consulting assistance or acquire software will require a separate solicitation or procurement.

Recognizing the scale and complexity of the County organization and the magnitude of the effort, we assumed for the RFI that the County's strategy would be to implement a BCP program using a phased approach that follows generally accepted BCP planning practices. Consultants were asked to describe how their BCP methodology would address the proposed RFI Scope of Work (SOW). The RFI SOW identified three major deliverables: (1) a risk assessment identifying corrective measures and safeguards required for reducing or eliminating identified risks; (2) a business impact analysis identifying the financial exposures and operational impacts from a major disruption of County services to establish the parameters of resumption, recovery and restoration-related decisions; (3) an analysis of alternative strategies to recover critical services/processes within the identified time frames; and (4) knowledge transfer strategy to enable the County to build internal competencies to develop and maintain a comprehensive BCP Program.

B. RFI Results

The County received 19 responses to the RFI. Five responses were considered to be the most credible based on the following criteria:

- Understanding of the "overall" project and the scope of work proposed.
- Proposed business continuity planning/disaster recovery planning methodology including use of automated tools.
- Proposed time and cost estimates to complete the project.

A review of all the vendor proposals determined that the project duration would range from 14 to 53 weeks. Aggregate cost estimates for the project ranged from $205,000 to $9,700,000 (See Figure 11).

FIGURE 11
RFI TIME AND COST ESTIMATES

Description	Estimate
Estimated Project duration	14 – 53 weeks
Estimated cost for assessment and strategy development.	$205,000 - $9,700,000
Estimated cost for knowledge transfer/training	$18,000 - $800,000
Cost for BCP software	$15,000 - $300,000 site license/$7,000 - $45,000 annual maintenance

C. RFI Analysis

Using consulting and planning assistance can significantly reduce the time and effort to develop, test and implement a BCP Program. Consultants can reveal pitfalls in the planning process, assist the County in establishing its goals and objectives, and provide the means for accomplishing these plans.

A review of the RFI responses revealed that although planning methodologies may vary, there are common process components. These components are sequential in nature and include the following:

INITIATION

This step involves obtaining support and commitment from management and all the stakeholders for the BCP plan. The initiation process includes:

- Identifying an executive sponsor to facilitate the establishment of recovery priorities, define the level of program commitment and allocate sufficient project resources.
- Establishing a governance and planning organization to oversee development, implementation, and maintenance of the planning process. This organization gives the BCP process continuous focus, credibility, and management.
- Identifying a business continuity manager to manage day-to-day responsibilities. This business continuity manager is the single point of responsibility and coordination for the BCP Program.

BUSINESS IMPACT ANALYSIS

Business Impact Analysis (BIA) is the process of identifying critical business functions and the losses or effects if these functions are not available. The results of the BIA establish the parameters of an organization's resumption, recovery and restoration-related decisions.

It involves analyzing and documenting the business functions in order to assess impact and recovery requirements. The BIA includes:

- Documenting key time-sensitive services and business processes, supporting activities and resources, and interdependencies.
- Analyzing financial exposures and operational impacts associated with the loss of time-sensitive critical services/processes.
- Establishing time frames in which time-sensitive services/processes must resume after an outage or interruption.
- Facilitating the establishment of a priority ranking of the time-sensitive services/processes for restoration/recovery.

STRATEGY DEVELOPMENT

This step involves identifying, evaluating, and recommending business continuity/disaster recovery strategies that will enable each critical service/process to be recovered within the time frame identified by the BIA.

Strategy development includes:

- Identifying and evaluating both self-reliant (internal) and commercially available continuity/disaster recovery solutions for recovery appropriate to the organization.
- Developing cost/benefit information for consideration by the organization in selecting optimal and cost-effective solutions. This information details the benefits and estimated costs of acquiring, deploying, and testing the various strategies analyzed and the recommendations.

PLAN DEVELOPMENT/IMPLEMENTATION

This step involves the documentation of procedures associated with the selected recovery strategies necessary to restore critical business processes within the required time frame as defined by the BIA. Plan strategies include detailed procedures for managing crisis situations, mobilizing recovery personnel and resources, establishing command and control, coordinating logistics of the recovery operations, and ensuring the life/safety of employees.

TESTING/TRAINING

Training and testing ensures that plan personnel are trained in the detailed provisions of the recovery program. This phase includes:

- Developing and conducting plan exercises;
- Establishing training requirements; and
- Updating and refining the plan regularly.

Some of the more established BCP consultants offer software based planning tools that provide structured methodologies to assist organizations in creating plans and coordinating business continuity activities. They also can automate the communication, implementation, and maintenance of plans.

Business continuity plans require continual review, revision and testing to ensure that they will meet an organization’s needs. Changes in services and processes and new system developments require frequent plan updates. BCP tools can automate updates and ensure ease of work in maintaining the currency of plans.

The previous section discussed the results and analysis of responses to the RFI. The following section identifies recommendations to begin the development and implementation of a County BCP Program.

6.0 Recommendations

Any number of threats can strike the County and its departments. In the decade of the 1990s, the County suffered nine declared disasters, including earthquakes, floods, wild fires, and civil unrest. It is located within one of the world’s most seismically active areas, with a historical record of major earthquakes occurring about seven times each century. A single major event can jeopardize the delivery of critical services to the County’s residents.

Citizens and families of Los Angeles County depend on the County for the sustained delivery of important services. These include social support activities as well as critical public safety functions, such as law enforcement, fire and emergency response services. Recognizing the need to continue delivery of these services, the County should establish a Countywide BCP Program to provide for their timely recovery in the event of catastrophic disaster. Additionally, new federal regulatory requirements stemming from HIPAA and Homeland Defense will necessitate an increased County commitment to business continuity.

This study has found that the County would be at risk to restore the delivery of services and operations within identified recovery timeframes following a large disruption. An assessment of the current BCP efforts revealed a number of issues that would impact County efforts in the timely restoration of critical business processes and functions.

While we undertook efforts identifying costs to hire a consulting firm to assist in coordinating and implementing a comprehensive BCP program, we are recommending an internally staffed effort using only selective consultative assistance to augment current County expertise. This approach will ensure that BCP becomes a department responsibility and that plans are developed and in place that will enable the recovery of critical services within established timeframes.

As the County moves forward to implement a BCP Program, it must have a strong commitment and support from the Board and County executive management. Additionally, an established organizational structure must be put in place to implement and maintain the BCP Program. This organizational structure would build on the County's existing emergency management organization.

The following are recommended initial actions that the County should take to implement an effective Countywide BCP program.

- Direct each department to participate in the development of their component of a Countywide BCP Program. Further, it is recommended that once the BCP is developed, it should be tested and validated annually.

- Establish a County BCP Steering Committee to oversee the development, implementation and maintenance of the program. The BCP Committee would be chaired by CAO/OEM with support provided by the CIO, ISD and A-C.

- Approve the acquisition or internal development of software to facilitate the management and maintenance of departmental plans. This will allow for improved visibility leading to the identification and maximization of potential shared resources.

- Secure a consultant to assist in the development of a formal framework for documenting and maintaining a department and Countywide BCP Program.

We estimate that $400,000 in funding is required to cover the acquisition or internal development of BCP software and consulting services to assist in the development of a formal framework. The acquisition of BCP software tools and the recommended consulting engagement will require a separate solicitation or procurement apart from the BCP RFI discussed in this report. The RFI was issued solely for informational and planning purposes.

This initiative will be funded with budgeted appropriation for County information security or the Information Technology Fund (ITF). The expenditure of ITF funds in amounts greater than $100,000 requires formal approval of the Board. It should be noted that there may be additional costs as technology-based infrastructure is identified to support the actual implementation of BCP recovery solutions.

We anticipate that approximately two months is required to obtain a consultant to assist in the development of a workable BCP framework, and between four to six months to acquire or develop a software solution for the management and maintenance of departmental BCP data. For planning purposes, we project the implementation of a Countywide BCP Program within 18 months. However, testing, validation, and refinement of plans will be an ongoing task.

P:\Drafts\countybcpreportfinalversion_feb18_03.doc
Created on 2/18/2003 11:40 AM

APPENDIX A

SURVEY RESULTS BY DEPARTMENT

	DEPARTMENT	SVCS		CRT					MEET CRT-SVCS		PUBLIC IMPACT				BCP PLANS		IT-SYS	B/UP Offsite			Testing					Meet CRT-IT		
				<8 hrs	<1 day	< 2 days	> 2 days		YES	NO	Serious	Moderate	Minor	None	YES	NO		YES	NO	UNK	YES	NO	UNK			YES	NO	UNK
1	**Affirmative Action**	1				1			1				1		0	5	9	0	5	4	5	0	4			5	0	4
2	**Agriculture Wts & Meas**	22			4	5	13		20	2	4	7	7	4	5	0	27	0	27	0	27	0	0			27	0	0
3	**Alternate Public Defender**	1					1		1		1				3	2	9	0	4	5	3	1	5			1	3	5
4	**Animal Care & Control**	5		3	2					5	3	2			2	3	7	3	4	0	0	7	0			0	7	0
5	**Assessor**	44				1	43		****	****	15	29			0	5	61	42	19	0	0	61	0			0	61	0
6	**Auditor-Controller**	41		3	12	9	17		4	37	19	22			0	5	72	44	0	28	0	72	0			50	22	0
7	**Beaches and Harbors**	8		7	1				7	1	8	4			2	3	1	1	0	0	1	0	0			0	1	0
8	**Board of Supervisors**	9		****	****	****	****		****	****	2	5	2		1	4	3	3	0	0	3	0	0			3	0	0
9	**Chief Administrative Office**	6					6		6			4	2		5	0	6	6	0	0	6	0	0			6	0	0
10	**Child Support Services**	3					3		****	****		3			4	1	15	0	15	0	15	0	0			15	0	0
11	**Chidren and Family Services**	0	**NR**																									
12	**Community Dev Comm**	3			1	2			1	2	1		2		0	5	16	15	1	0	16	0	0			7	9	0
13	**Community Senior Svcs**	20		4	1	1	14			15	17	3			0	5	10	3	5	1	1	8	1			4	5	1
14	**Consumers Affairs**	5					5			5		5			0	5	7	3	4	0	0	4	0			0	4	0
15	**Coroner**	27		9	5	4	9		***	***	17	10			0	5	55	52	3	0	53	2	0			52	3	0
16	**County Counsel**	2			1		1		2		1	1			3	2	8	8	0	0	0	6	2			6	2	0
17	**District Attorney**	5		2	1	1	1		0	5	3	2			3	2	20	0	5	15	4	1	15			0	5	15
18	**Fire**	1		1					0	1	1				3	2	7	7	0	0	7	0	0			5	2	0
19	**Health Services**																											
19a	**Health Services Admin**	36	**NR**	****	****	****	****	**	****	****	****	****	****	****	-	-	****	****	****	****	****	****	****	***	***	****	****	****
	Health Services Admin	13		9	2	2			13		5	4	4		5	0	5	4	1	0	5	0	0			5	0	0
	Data Collection & Anaysis	**2**	**NR**	****	****	****	****	**	****	****	1	1			5	0	1	1	0	0	1	0	0			1	0	0
	Emergency Medical Svcs	17	**NR**	****	****	****	****	**	****	****	****	****	****	****	-	-	****	****	****	****	****	****	****	***	***	****	****	****
19b	**Personal Health**														-	-												
	Martin Luther King/Drew	42		18	6	2	16		42	0	9	15	10	8	2	3	38	8	30	0	1	37	0			1	37	0
	High Desert Hospital	32			1	26	5		****	****	9	22	1		2	3	7	7	0	0	7	0	0			7	0	0
	UCLA-Harbor Medical	29		18	1		10		****	****	19	10			3	2	154	151	3	0	34	120	0			0	154	0
	LAC + USC	27		9	7	6	5		15	12	25	2			3	2	23	10	13	0	9	14				9	14	
	Rancho Los Amigos	19					13		13	0		7	5	1	5	0	19	4	1	14	4	1	14			****	14	****
	Olive View	0	**NR**	****	****	****	****	**	****	****	****	****	****	****			****	****	****	****	****	****	****	***	***	****	****	****
19c	**Public Health**	5		1					4	1	2	3			-	-	4	2	2	0	0	4	0			2	2	0
	Public Health Info Systems	4		1	3				4	0	1	1	2		5	0	4	0	4	0	4	0	0			4	0	0
	Tuberculosis	1					1		1	0	1				0	5	1	1	0	0	1	0	0			1	0	0
	Tobacco	4					4		4	0			4		5	0	4	4	0	0	4	0	0			****	****	****
	Immunization	3				2	1		3	0		3			4	1	6	6	0	0	6	0	0			6	0	0
	HIV	1					1		0	1			1		0	5	5	0	5	0	0	5	0			0	5	0
	Alcohol	9		1		2	6		9	0		9			2	3	14	11	3	0	0	14	0			11	3	0
	Child-Lead Poisoning	2					2		2	0	1		1		4	1	1	1	0	0	1	0	0			1	0	0
	Sexually Transmitted Disease	4					4		4	0	4				1	4	4	4	0	0	4	0	0			4	0	0
20	**Human Relations Comm**	7		1	4	1	1		7		6		1		0	5	6	0	6	0	6	0	0			6	0	0
21	**Human Resources**	8		2	2		4		8		2	1	2	3	5	0	6	1	3	2	1	5	0			2	3	1
22	**ISD**	5		5					5		5				1	4	52	39	13	0	5	47	0			0	52	0
23	**LACERA**	18				18			18		18				5	0	22	22	0	0	22	0	0			15	0	7
24	**Mental Health**	7		4		2	1			7	10	4			1	4	14	10	3	1	13	0	1			11	2	1
25	**Military & Veteran Affairs**	2					2		2				2		0	5	12	1	0	0	1	0	0			1	0	0
26	**Museum of Art**	2		0	0	0	2		2	0			2		5	0	22	22	0	0	22	0	0			22	0	0
27	**Natural History Museum**	6					6		****	****		2	4		0	6	17	7	10	0	7	10	0			7	10	0
28	**Ombudsman**	1		1					****	****			1		0	3	4	4	0	0	4	0	0			4	0	0
29	**Probation**	37		29	3	2	3		37		17	17	3		1	4	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
30	**Park and Recreation**	3			3				2	1		1	2		5	0	73	20	53	0	25	23	25			11	60	2

APPENDIX A

SURVEY RESULTS BY DEPARTMENT

	DEPARTMENT	SVCS	CRT				MEET CRT-SVCS		PUBLIC IMPACT				BCP PLANS		IT-SYS	B/UP Offsite			Testing			Meet CRT-IT		
			<8 hrs	<1 day	< 2 days	> 2 days	YES	NO	Serious	Moderate	Minor	None	YES	NO		YES	NO	UNK	YES	NO	UNK	YES	NO	UNK
31	Public Defender	8	****	1	****	****	****	****			1		****	****	9	1	0	8	1	0	8	0	1	8
32	Public Library	6			2	4	2	4		6			0	5	8	7	1	0	8	0	0	13	5	0
33	Public Safety	8	1	4	3	0	0	8	2	5	0	1	1	4	7	8	0	0	6	2	0	0	8	0
34	Public Social Services	8			1	7	7	1	6			2	5	0	4	8	0	0	8	0	0	8	0	0
35	Public Works	19	6	1	3	9	4	15	8	6	5		0	5	134	8	126	0	11	123	0	107	27	0
36	Regional Planning	3				3	1	2		3			1	4	10	5	20	0	0	25	0	0	25	0
37	Registrar-Recorder/Clerk	5	2	1		2	5		4	1			0	5	12	12	0	0	8	4	0	1	11	0
38	Sheriff	6	2			4	3	3	2	3	1		0	5	25	6	19	0	10	15	0	17	8	
39	Superior Court	3				3	3	0	3				5	0	3	3	0	0	0	3	0	3	0	0
40	Treasurer/Tax Collector	8		2		6	1	7	5	1	2		0	5	13	13	0	0	6	7	0	0	13	0
	TOTALS =	**623**	**139**	**69**	**87**	**200**	**263**	**135**	**257**	**210**	**60**	**17**	**106**	**147**	**868**	**598**	**408**	**78**	**386**	**621**	**75**	**456**	**578**	**44**
	PERCENTAGES		**28**	**14**	**18**	**40**	**66**	**34**	**47**	**39**	**11**	**3**	**42**	**58**		**55**	**38**	**7**	**36**	**57**	**7**	**42**	**54**	**4**
														See #1		**38% = Not B/up & stored**			**57% = Not tested**			**54% = Not meet**		
	PERCENTAGE TOTALS		**60% = Less than 2 days**						**46% = Serious Impact**															
			28% = Less than 8 hours				**39 = Cannot CRT**		**39% = Moderate**															
NR -	**Non-responsive department**																							
CRT-	**Crtical Recovery time**																							
B/UP	**Backed-up and stored offsite**								**#1. Approximately 58.1% of BCP plan responses from departments indicated insufficient business recovery,**															
IT-SYS	**Information Technology Systems**								**resumption, emergency contingency plans and lack regular testing.**															
UNK-	**Unknown**								**#2. Approximately 76.92% (30 of 39) of reporting departments indicated partial and incomplete BCP plans.**															
********	**No response**																							