

L A - 5 9

An Overview of Advanced Business Continuity (BC) Practices in the U.S:

An Insight into U.S. Private and Public Sector Cooperation

**Development Bank of Japan
Representative Office in Los Angeles Office
December 2005**

米国における防災マネジメントの実例

～ 公民連携の観点から ～

要旨

1. 2005年8月にニューオーリンズを中心とした米国南部を襲い千人以上の死者を出したハリケーン「カトリーナ」は、改めて自然災害の恐ろしさと防災対策を怠った代償の大きさを如実に示した。このことから、災害に対する事後の対処と同時に、継続的に災害に備える防災の重要性が指摘されている。
2. その意味では、1971年のサン・フェルナンド渓谷地震（死者65人）をきっかけにして地震対策が進んだカリフォルニア州における公民連携のあり方や、2001年の同時多発テロ以降進んだ米国企業の防災への取り組みに関して検証しなおす意義は大きい。
3. 防災に関する政府と企業との関係では、第一に企業に対して防災対策を義務付ける規制がある。政府としては、災害時における社会インフラ確保の観点から、銀行・証券などの金融機関、病院などの健康分野、などに対して規制をおこなっており、これらの規制を今後どの程度まで拡げていくかが検討課題である。
4. 次に、政府機関と企業、さらにコミュニティ（地域住民）の間における公民連携活動では、災害や災害対策に関する基本的情報の共有や防災対策に関する奨励事例の紹介などが重要な要素となっている。そのような活動の中では、1983年以降活動を続けているカリフォルニア州のBICEPP（The Business and Industry Council for Emergency Planning and Preparedness）の活動が好例である。
5. さらに企業による独自の対策としてはBCP（Business Continuity Planning）が注目されて久しいが、BCPを率先して導入した企業の中には、BCPをさらに一歩進めて、企業のリスクマネジメントの観点、また将来の企業価値増進といったマネジメントの観点から、防災マネジメントを実施している企業がでてきている。
6. 防災マネジメントのポイントは、(1)企業の事業活動を分析し、(2)各種災害に対するリスク評価を行い、(3)それらリスクが事業活動にどのようなインパクトを与えるのかを分析することからスタートする。しかし、インタビューした企業から共通して指摘されたポイントは、(1)企業幹部によるコミットメント等経営の関与、(2)業務の主要度の優先付け、データセンター等外部リソースの活用、(3)防災対策の不断の見直し、(4)システムに頼りながらも一方で従業員の継続的な防災対策トレーニングによって現場の浸透を図る姿勢、という点であった。つまり、どのような事態が発生するか予見しにくい防災対策においては、(1)できるだけ多くの情報をアップデートし、(2)万が一に備えて常に実行できるようにしておく、という基本的な姿勢が重要である。

（報告書執筆担当：Ellen Nishigaki、要旨担当：酒巻 弘）

なお、本調査実施に際しては、日本政策投資銀行「調査 No.80 防災マネジメントによる企業価値向上に向けて～防災 SRI（社会的責任投融資）の可能性～」をベースとし、調査方針の策定、インタビュー先の選定、インタビューの実施など、政策企画部と共同でおこなっている。また、インタビューの実施に際しては、Deloitte & Touche LLP Audit and Enterprise Risk Services の Ms. Kathleen McGrorty に大変お世話になったことを付言しておきたい。

Table of Contents

1. Introduction.....	1
2. An Advanced Approach to Business Continuity	4
3. An Overview of BC Trends in the U.S.	6
4. Overview of the Incident Command System (ICS)	11
5. Interview Summaries	13
BICEPP	13
Southern California Edison.....	15
Amgen.....	17
Company A.....	19
Washington Mutual, Inc	21
Westcorp.....	24
6. Conclusion	26
Appendix A: Federal Financial Institutions Examination Council (FFIEC) Regulatory Agencies.....	28
Appendix B: Disaster Recovery Institute International (DRII) – Subject Area Overview.....	31
Interviews.....	33
Works Cited.....	35

1. Introduction

Business continuity (BC), optimizing the availability of all mission and business critical assets – people, processes, data, technology, and facilities, among others to resume business operations in the wake of potential threats, is increasingly becoming a reality check for organizations of all sizes. Today’s generation of vulnerabilities in the business environment not only includes the day-to-day interruptions such as IT security breaches and power outages, but also catastrophic events such as Hurricane Katrina’s devastation to the Gulf Coast in August 2005, the London bombings in July 2005, the Indian Ocean earthquake/tsunami in December 2004, and the 9/11 terrorist attacks, among others. With the frequency and impact of recent events, businesses are reexamining and enhancing the quality of their BC strategies.

However, in a society driven by unpredictable events, experts have seen a consistent decline in the government’s attention to natural hazards. In particular, 9/11 has had many implications for preparedness, mitigation, response and recovery planning in the event of a natural disaster. Critics say many issues are attributed to the creation of the U.S. Department of Homeland Security (DHS) in January 2003 and the incorporation of the Federal Emergency Management Agency (FEMA) in March 2003. There is currently a debate over whether the Bush administration is undermining FEMA’s effectiveness by downgrading it from an agency that managed federal mitigation and response efforts to primarily a response and recovery agency. With government funding moving toward grant applications for homeland security issues, the nation’s priorities have become more focused on defense and national and international security. According to congressional figures, FEMA, which also supports state and local emergency management preparation and response, has lost control of more than \$800 million in grant money since 2003 to the Office for Domestic Preparedness responsible for preparation and planning functions.¹ Clearly, the government’s emphasis on terrorism is affecting its readiness for other catastrophes leaving the nation’s disaster/emergency management inadequate. One suggestion may be to liberate FEMA from DHS and restore its Cabinet-level agency status.

A director of the King County Office of Emergency Management in Washington state reported to the Los Angeles Times that, “Prior to 9/11, we were spending 75% of our time planning, training and exercising for natural hazards,” mostly earthquakes, he said. “Today, that’s down to 25%. The rest of the time is spent administering Homeland Security grants.”²

Clearly, the federal government requires a more consistent and balanced agenda in allocating its resources to deal with natural, man-made and accidental disasters including earthquakes, terrorist attacks, computer viruses and power failure that occur on a continual basis. Historically, the nation’s political system focused on how to react to

1 David Rogers and Gary Fields. The Wall Street Journal. “Already Under Scrutiny, FEMA Is Now In The Spotlight”. August 31, 2005.

2 Nicole Gaouette. September 1, 2005. “A Diminished FEMA Scrambles to the Rescue”. Los Angeles Times. listed at <http://www.latimes.com/news/nationworld/politics/la-na-fema1sep01.1.7749651.story?coll=la-news-politics-national>

rather than plan for catastrophes. Jim Goltz, outreach manager for the California Integrated Seismic Network of the Governor's Office of Emergency Services and a board member of the Business and Industry Council for Emergency Planning and Preparedness (BICEPP) pointed out that several years ago, a guest speaker from Johns Hopkins University noted that major public policy changes related to earthquake disasters in the U.S. were all in response to a specific event. For instance, after the 1971 San Fernando earthquake damaged major hospitals, in 1973, the Hospital Act was enacted and required hospitals to be built to higher seismic standards. Many experts are in consensus that the greatest challenge is maintaining strategies for disaster/emergency planning that must be continually reassessed in light of evolving risks.

BC is an ongoing process that involves the development and implementation of policies and procedures necessary to keep critical business operations available from the potential socio-economic, political and environmental impact of natural disasters and other unanticipated disruptive events. While this practice has traditionally been a low-profile company initiative, critical stakeholder players: government, investors, customers, suppliers, competitors, employees, academia and community are increasingly evaluating the company's viability and reputation in today's risky environment. From this perspective, BC clearly falls within the realm of corporate governance. BC has a trickle-down effect through company A and its stakeholders affecting the bottom line, the shareholder value and reputation of the organization.

Still, a surprising number of companies continue to overlook the requirements of a sustainable long-term BC program, according to a recent survey commissioned by AT&T.³ About one-third of 1,200 respondents said they have no BC plan. About a quarter of companies surveyed said they have not revised their plans in the past 12 months, and nearly as many have not tested them during that time either. Seventeen percent said they have never tested their disaster recovery plans. "It's not the priority you would think it would be," an AT&T representative said.⁴ Those that shy away from protecting themselves from today's risks could lose long-term competitive advantage. The increasing realization that legislation alone cannot improve corporate governance creates healthy incentives such as BC for the best companies to try to stand out from the crowd.

A board-level focus on BC should not necessarily be driven solely by the need to comply with regulations. With the federal government's ill-prepared state of readiness toward unpredictable events, there is a strong indication that society needs to act on this awareness and learn to become self-sufficient and not rely too heavily on the government. This can be achieved through private-public partnerships and networking to ensure cooperation and solidarity among the government, private sector, organizations, community and academia.

³ Alorie Gilbert. September 5, 2005. "Data recovery firms slog through the post-Katrina Gulf Coast". Cnet News.com. listed at <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/09/05/BUGG0EHTR01.DTL&type=printable>

⁴ Ibid.

The purpose of this research is to explore the current trends of BC practices in the U.S. Research was conducted through interviews with public and private sector organizations preserving the anonymity of several interview participants by not identifying their names and organizations. Quotes may not reflect the organization's views but are based on the experiences of the interviewees. Additional findings were taken from general media sources. The diversity of the participants' industries resulted in a wide range of feedback demonstrating different levels of experience in BC ranging from programs that are currently developing BC plans to those with advanced practices.

2. An Advanced Approach to Business Continuity

Deloitte & Touche LLP's Business Continuity Management (BCM) practice, which is one element of an entire suite of risk management service offerings, has evolved over the past 30-35 years. It is capable of serving clients globally, with professionals based throughout the U.S. and abroad. Deloitte & Touche's consultants are certified through the U.S.-based Disaster Recovery Institute International (DRII)⁵, an internationally recognized body that sets common guidelines and standards. Its counterpart is BCI Institute (BCI) based in the United Kingdom.

This section highlights Deloitte & Touche's approach to a comprehensive BCM program tailored to an organization's business objectives, requirements and risks. BCM encompasses the planning, anticipating and mitigating strategies in the event of a business interruption. A sustainable and dynamic BCM program involves the following action stages:

Analyze

- **Current State Assessment:** The organization's current state of preparedness to adverse circumstances. For instance, characteristics of leading-edge programs include active executive involvement, third-party continuity contracts, integrated testing between business units, IT, facilities, and external parties.
- **Risk Assessment:** Potential threats to continuity of business operations affecting people, processes, IT, records and facilities, among others.
- **Business Impact Analysis (BIA):** The financial, operational and regulatory effects from extended business interruptions with varying downtimes.

Develop

- **Governance:** Executive management takes an active leadership role in identifying, assessing, prioritizing, managing and controlling risks. Responsibilities include setting policy, prioritizing critical business activities, allocating sufficient resources and personnel, providing oversight, approving plans and reviewing test results.
- **Availability/Recoverability Strategies:** Strategies are developed to anticipate disruptions, mitigate consequences and expedite the recovery of critical operations. Plans are designed to reduce the downtime and restore conditions to a state of business as usual. To minimize geographical-concentration risk, primary and alternate teams, dual purpose facilities incorporating ongoing business functions, distributed recovery capabilities, rather than "dark sites" with recovery capability only, redundant services and back-up capabilities are identified.
- **Procedures:** Documents are prepared to reflect the roles, responsibilities and actions of personnel. Plans are developed and continuously maintained for recovery of facilities, processes, people and technology.

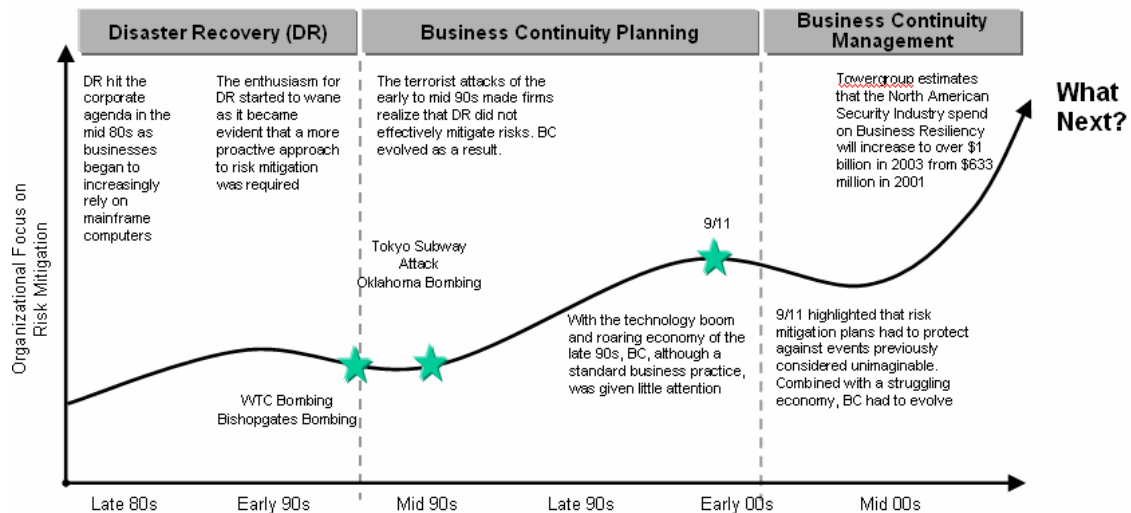
⁵ See Appendix Appendix B.

Implement

- **Resource, Acquisition & Implementation:** The extended enterprise – external resources, third-party services, business partners, public sector, and so on are integrated into BCM plans.
- **Training & Testing:** People are trained and educated organization-wide and plans are integrated and exercised, tested and revised routinely to ensure effectiveness.
- **Maintenance:** BCM capabilities are reviewed and refined to ensure business, organizational and information system changes reflect the current business environment and risks.

3. An Overview of BC Trends in the U.S.

The Evolution of Business Continuity



Preparations for crises have evolved from disaster recovery and business continuity planning into a more comprehensive approach called Business Continuity Management. Source: Copyright 2005 Deloitte & Touche LLP

In today's risky intense global environment, the frequency, magnitude and costs of many business disruptions have affected organizations' strategies in dealing with crises of all sizes. Planning for unanticipated events has expanded beyond an IT-focused, recovery approach to a comprehensive one that maximizes business resiliency involving preparedness, mitigation and recovery of business and mission critical assets including people, operations, technology, buildings, infrastructure, and interdependent entities including partners, vendors and suppliers. The risk management culture in response to eventualities is changing from a reactive and short-term strategy to a proactive and long-term one.

Kathleen McGrorty, a Senior Manager with Deloitte & Touche LLP's Audit and Enterprise Risk Services practice explained, "Our approach takes into consideration the way the U.S. is approaching BC. If you look at the way our government has started to regulate or increase regulation, especially in financial services but also in energy, telecommunications and transportation, there are more regulations that are *specific* to BC". McGrorty added, "What keeps the U.S. running is its critical core processes: financial services, transportation, energy and telecommunications. Whereas the largest corporations dominated the BC preparedness arena five years ago, McGrorty is finding more small and mid-sized companies are focusing on developing more detailed recovery strategies.

Differences of Approach, Differences of Intent

	Disaster Recovery	Business Continuity Planning	Business Continuity Management
Approach	<ul style="list-style-type: none"> ▶ Recovery of data and provision of alternate equipment to operate applications in an emergency ▶ Restoration of operating facilities after a crisis 	<ul style="list-style-type: none"> ▶ Single risk management solution that relies on redundant facilities ▶ Applied in a similar manner to all businesses in a "one size fits all" solution ▶ Broader scope than DR, includes business operations 	<ul style="list-style-type: none"> ▶ Outages and interruptions are anticipated and mitigated before they occur ▶ Considers such factors as the level of risk mitigation required, actual risks faced, and the cost to mitigate risk ▶ Aligns the appropriate resiliency solution with the appropriate businesses ▶ Menu of risk mitigation solutions of which traditional continuity is just one option

Simply planning for a disaster assumes that it is something that happens so rarely that an organization should only be prepared to recover when and if an event occurs. Managing the risk of business interruption implies accepting that disasters, though unpredictable, do occur and that the ability to respond and continue activities should be a process of design and management.

Source: Copyright 2005 Deloitte & Touche LLP

Prompted by market forces, regulations and industry compliance requirements, the financial services industry serves as the bellwether for BC trends in leading the way through a series of initiatives among financial organizations to improve the BC plans of their critical service providers and other interdependent entities. According to David Sarabacha, a Senior Manager with Deloitte and Touche LLP's Audit and Enterprise Risk Management practice, "In the U.S., BC initiated through the financial industry, has moved into healthcare through HIPPA and is slowly making its way through other industries. However, with Sarbanes-Oxley (SOX) Act of 2002 excluding BC from its scope, I believe that has somewhat slowed the process." The recent wave of regulations including SOX, which was enacted to help re-establish investor confidence in the financial markets requiring accountability measures to be in place to validate internal controls and regular reporting to shareholders, has placed BC issues firmly on the boardroom agenda.

Eric Beck, a Senior Manager with Deloitte & Touche's Security Services Group added, "HIPPA⁶ has brought attention in the healthcare industry that there is a need to look at BC initiatives. Disaster recovery is fairly well covered from a technology perspective at most pharmaceutical firms." While most hospitals have a disaster recovery plan, it will be compulsory for all hospitals to have a plan in place based on the HIPPA requirement. In

⁶ Health Insurance Portability and Accountability Act of 1996 (HIPPA) is designed to force the health care infrastructure to comply with security and privacy standards to protect personal health information. HIPPA requires BC plans to include a process that restores any loss of data in an unexpected event.

addition, he noted that in retail – large, enterprise-level, national chains – all have a commitment to practicing BC to some level.

NASD 3510, which was issued in August 2004, requires brokers, security firms and other investment advisors to have a current plan to prepare for business interruptions. According to Beck, it mandates that a formal BC plan must “address mission critical systems – basically the 10 key processes of transactions recorded in a trade.”

Among other industries, the practice of BC is considered just good business at this point. Sarabacha commented, “We’ve done some work for oil exploration organizations and some initial conversations with several of them, but nothing is coming across as a mandate.”

Emerging Trends in Business Continuity and Disaster Recovery		
	Traditional	New Reality
Management Disposition	Due-diligence	Active commitment
Organizational Positioning	Middle Management	Executive
Basis For Measurement	Historical, experience-based	Unknown potential and frequency
Requirements	Recovery-minutes, hours, days...	Continuous availability
Awareness	Low	High/Acute (may diminish over time)
Priority	Low: after-thought	Higher-design consideration
Focus	Technology	People, Process & Technology
Plans/Process	Reactive: post-event	Integrated-anticipative
Cost	Distinguishable, minimized	Embedded
Service Providers/Suppliers	Inherent trust	Trust, but verify
Insurance	Open-ended policies, low premiums	Coverage restrictions, higher deductibles and premiums
Source: Copyright 2005 Deloitte & Touche LLP		

On the same topic of BC drivers, McGrorty explained, “There is a hairline difference between the financial impact of an outage of a particular process and, let’s say, the brand image impact. Considering major brands are critical when performing risk assessments, it’s not just about the finances that keep a company viable. The folks with the biggest logos and the most international recognition know this and invest in protecting their brand’s reputation as part of their BC program.” Reputational risk or brand equity has climbed up the boardroom agenda. As the collapse of Enron has showed, repercussions can affect an organization’s entire operations.

Similarly to Wall Street’s decision to shut down its operations for a period of time to allow companies to recover themselves after 9/11, advanced planning in the financial services industry starts with the business perspective according to McGrorty. “What are my business processes? What do I need to keep them running on a business as usual basis? What is the impact to my business if I cannot perform that process or function? How long will it take before there is significant impact – either financial or brand, quantitative or qualitative – to the viability of operations?” BC is business process-driven and the operational disciplines which support a business process typically include IT, human resources, facilities, finance, legal and so on. As McGrorty explained, “If I know *what* I do, the *how* I protect it follows.” For instance, most of the organizations with leading edge business continuity programs implement IT disaster recovery strategies *in response to business recovery requirements*.

Based on McGrorty’s experience in the marketplace, many clients find gaps that exist between business and IT operations. Often, business expectations and the IT recovery strategies that may have been implemented require adjustments to meet realistic recovery time objectives. Strategies developed by IT operations without knowing the precise business process recovery requirements almost always result in speculation about the proper level of investment. Business process owners and the respective IT professionals who support them should be intensely collaborative.

Disaster recovery experts say that strengthening infrastructure such as power and water, hospitals, and response-and-recovery capabilities will better prepare the nation for almost any contingency. While most leading practices include third-party continuity in their plans, it is the component frequently missing from an organization’s BC plan. However, there is speculation that in the near future, regulations will require BC to be built into the critical national infrastructure such as telecommunications, oil, gas, and power industries linking the respective industries to homeland security. To keep up with the mainstream, this suggests that small, medium and large organizations will adopt similar reciprocal contracts with third-party entities into their BC programs.

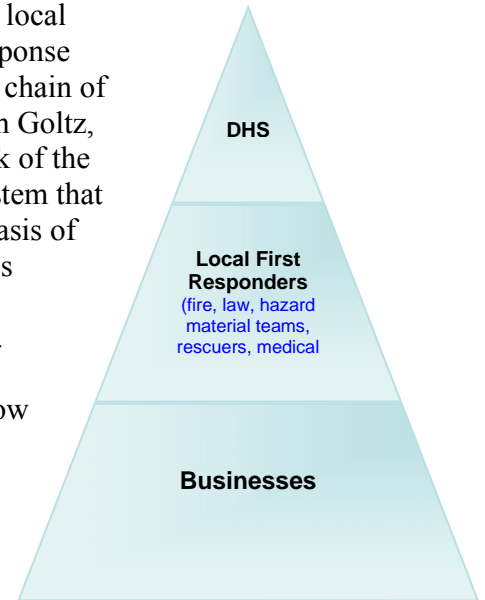
Rising investor and public expectations will drive organizations to use measures that incorporate exploring and managing uncertainty and crisis in the business world. The future direction of organizations will most certainly involve adopting a business model that integrates BC to protect them from today’s business risks – strategic, financial, operational, reputational and regulatory.

Looking forward, McGrorty speculates that there will be more dialogue asking: “What are the best BC regulations? What are the most equitable regulations?” Although partnership efforts are gaining ground, government entities may bear prime responsibility for creating a climate that promotes BC awareness. Furthermore, the private sector plays a key role in supplementing government-led efforts. While most organizations do not desire to be hampered by the government, regulations may be necessary to stimulate BC commitment to action.

3. An Overview of the Incident Command System (ICS)

In the early 1970s, the Incident Command System (ICS) was developed in the aftermath of a devastating wildfire in California with losses totaling roughly \$18 million per day. It was created to establish a common system for federal, state and local government and the private sector addressing an emergency response organizational structure, compatible communications, clarity to chain of command, common terminology among agencies and so on. Jim Goltz, outreach manager for the California Integrated Seismic Network of the Governor's Office of Emergency Services, explained "It's a system that organizes emergency response functionally rather than on the basis of individual organizational responsibilities." From a government's perspective, when a private sector entity assumes a similar organizational structure to that of the ICS, it adds predictability.

While public and many large private organizations recognize how the ICS works as a hierarchy of authority, many small private organizations are still unfamiliar with the concept. Essentially, the business affected by the disaster is subordinate to the local first responders, who are subordinate to the Department of Homeland Security (DHS). Typically, the local first responders 'own' the incident and remain in charge until it is assigned to either DHS or the business.



In March 2004, a comprehensive national approach to incident management known as the National Incident Management System (NIMS), a "federalized ICS plan," was created to incorporate existing best practices including the ICS. NIMS provides a framework which government and private entities at all levels can interface and work together to manage domestic incidents.

Currently, the implementation of NIMS is required at the federal level by agencies that respond to domestic incidents. Those agencies are mandated to become compliant with NIMS by fiscal year 2006. State and local governments are required to incorporate NIMS by fiscal year 2007.

While there is not a mandated benchmark assessment tool, in January 2003, FEMA, the nation's primary disaster-relief agency which oversees federal response and recovery efforts, in cooperation with Emergency Management Accreditation Program (EMAP), an independent non-profit organization consisting of the U.S. Department of Transportation, the U.S. Environmental Protection Agency and the International Association of Emergency Managers, among others, launched the National Emergency Management Baseline Capability Assurance Program (NEMB-CAP). This comprehensive assessment program is part of a national effort to establish a baseline measurement of the nation's emergency management capabilities and to assist the emergency management community at all levels. It is a voluntary accreditation process for state and local emergency management programs, to be recognized for compliance with national standards, to demonstrate accountability and to focus attention on issues that requires improvement


and resources. It is in its third year of funding from FEMA and expects to complete its assessment of all fifty states by the end of fiscal year 2005.

Another assessment tool used by states is the National Incident Management System Capability Assessment Support Tool (NIMCAST). It is a web-based self-assessment tool designed to aid state and local organizations and jurisdictions in determining their capabilities and compliance against the requirements established in the NIMS.

As an incentive, beginning in fiscal year 2006, federal funding for state and local preparedness grants will be tied to compliance with the NIMS. The U.S. Small Business Administration also offers a variety of loan programs to assist businesses impacted by a disaster.

5. Interview Summaries

This section provides a brief summary of interviews of public and private organizations that have a head start over those who have not made investments in BC. The findings suggest that though there is a heightened awareness of increased business risks, reflection of this knowledge in business planning has yet to become an industry-wide mainstream practice. Many organizations adhere to *ad hoc* and company BC specific benchmarks to maintain their business operations. Unless a standard is driven by government regulations, organizations will look internally to decide what makes sense to their particular business.

 **The Business and Industry Council for Emergency Planning and Preparedness (BICEPP)** was established in 1983 as a private sector association, but later became a non-profit corporation. While BICEPP was founded by a government agency, it has always been led by a private sector entity supported by advice and guidance from the public sector. Its mission is to provide a networking forum on emergency preparedness and contingency planning within the private sector. BICEPP has been recognized by federal, state, county, city and other private organizations for its exemplary efforts in emergency planning and preparedness.

BICEPP's basic operating revenue is roughly \$20,000-\$25,000 per year that is generated from membership fees, seminars and other activities. In addition, the organization receives in-kind services and donations from member organizations. For instance, one of the Benefactor or Corporate member organizations may provide copies and invitations for events and so forth. For seminar speakers, the Governor's Office of Emergency Services (OES) arranges the use of the auditorium at the California Institute of Technology. Similarly, the venue for each monthly board meeting is held at a member organization's facility and is rotated on a quarterly basis.

Among its relationships with other organizations, BICEPP works cooperatively with the Community Emergency Response Team (CERT) Program, an organization whose concept was initially developed by the Los Angeles City Fire Department in 1985. FEMA, the Emergency Management Institute and the National Fire Academy adopted and expanded the CERT concept by providing education and training on disaster preparedness applicable to all hazards. Grants from the government may be available to local communities to initiate CERT programs. Robert Lee, executive director of BICEPP noted, "Many of BICEPP's member companies have introduced CERT into their overall preparedness programs."

As the original sponsor of the Los Angeles City Fire Department's CERT Patch program, BICEPP conducted a CERT Train-the-Trainer course in 2003 with plans to conduct another course in 2005 or 2006. In 2001 and 2004, it sponsored the BICEPP Emergency Response Team Challenge, an activity in which private and public sector teams compete in an event based on the proficiency of CERT disciplines.

In addition, BICEPP frequently co-sponsors programs, workshops and seminars with public sector organizations such as the OES, the Los Angeles County Office of Emergency Management and the Los Angeles City Emergency Preparedness Department. It also collaborates with non-government organizations, such as the California Emergency Services Association and the American Red Cross Emergency Network Los Angeles.

While there are a number of non-profit organization and non-governmental organizations, many of these organizations have different agendas, according to Lee, who is also a partner of a consulting business in emergency and security management. The Association of Contingency Planners mainly focuses on IT. Another organization, Emergency Network Los Angeles, is a coalition of non-profit community-based organizations that coordinates with government agencies and the private sector to provide assistance to individuals, families and organizations following emergencies and disasters.

Organizations like BICEPP strengthen the partnership between the public and private sector by harmonizing efforts and sharing best practices and successful strategies in BC planning. Clearly, collaborative efforts representing a wide range of organizations from various industries can achieve quicker and more efficient results than by independent and uncoordinated efforts.



Southern California Edison (SCE), a subsidiary of Edison International, is one of the nation's largest investor-owned electric utilities, serving more than 13 million people in a 50,000 square-mile area of central, coastal and southern California excluding the city of Los Angeles and other cities. As a critical player of the U.S. infrastructure, SCE has a responsive role to recover services to its customers as quickly as possible. The premise of BC is not enough to ensure continuity if a major part of the infrastructure, its employees and customers are also adversely affected by an event.

According to Kelly Shivertaker, manager, emergency planning and preparedness of SCE and president of BICEPP, "California is unique in integrated planning among utilities. The utilities in California have been not only planning, but integrating those plans for a considerable period of time because in the 1950s, the California Utilities Emergency Association (CUEA) was formed." Jim Goltz, a board member of BICEPP added, "There are certain federal regulations that apply to all states, but there are a lot of internal regulations by the state or non-regulations depending upon philosophy within states." CUEA provides a coordinated effort among government agencies, public and private utilities, and community-based organizations. In emergencies, it provides information and support during response, restoration and recovery efforts to gas, electric, water, wastewater, telecommunications and pipeline utilities in California. CUEA, funded primarily by member utilities, operates the Utilities Branch of the Governor's Office of Emergency Services.

While not as highly regulated as the financial services industry, electric utilities must comply with General Order No.166 under the Public Utilities Commission of the state of California. It provides standards for operation, reliability, and safety during emergencies and disasters. SCE is required to file a compliance report as it relates to general order No.166. Other regulations include those from the California Independent System Operator.

Prepared to respond effectively to an incident, SCE's ICS-trained field employees, those who are out servicing equipment and restoring services, are able to identify and coordinate with first responders. In addition, the ICS and the Standardized Emergency Management System (SEMS)⁷ template are integrated into SCE's emergency operations center. Shivertaker is supported by one assistant, 3 professionals dedicated to emergency management and two individuals responsible for fire management who work with the fire agencies for training purposes. Collectively, Shivertaker's staff works as liaisons to individuals within each department of the organization.

⁷ Following the Oakland/Berkeley Hills Fire of 1991, the California legislature enacted the Standardized Emergency Management System (SEMS) to manage response to multi-agency and multi-jurisdictional emergencies. Based on the ICS, SEMS is used as a unified emergency response across the state and is often used as a national model.

In respect to insurance coverage excluding catastrophic events, SCE is a self-insured organization. Shivertaker explained, “If the disaster were of a catastrophic nature and met a certain financial threshold, then our insurance would apply but not before that.” As part of a requirement from the insurance company, SCE must demonstrate plans that are in place to respond to an emergency event.

Shivertaker, is also a member of the private sector committee of Kentucky-based Emergency Management Accreditation Program (EMAP), a program that is using NFPA1600, the standard recommended by the 9/11 commission for private sector emergency preparedness standard, as a foundation. Robert Lee, executive director of BICEPP added, “It is very similar to the ISO ratings. It is the same idea, but uses these criteria with some manipulation to do it.” The EMAP Commission is currently working with the DHS to use EMAP standard and procedures to conduct baseline assessments of all states and territories by December 2005.

While the past couple of years have seen a dramatic increase in board awareness on the importance of BC policies, Shivertaker added that companies should extend this duty “to all employees who hold responsibility – through annual performance reviews related to bonuses, promotional opportunities and salary.” Although not featured in the extensive discussions of corporate governance (CG) and corporate social responsibility (CSR), the trickle-down effect of BC throughout an organization and the extended enterprise can be interpreted as another facet within the realm of CG and CSR.



Amgen, a Fortune 500 company, is a leading human therapeutics company in the biotechnology industry. For 25 years, the company has served millions of patients and continues to be an entrepreneurial, science-driven enterprise. After the events of the 1994 Northridge earthquake, the company decided to build a more comprehensive level of planning for BC and emergency management and response.

For Amgen, BC governance is centralized at its corporate office in Thousand Oaks, California. Its BC Council, a group of senior management level representatives from each of the major business units meets on a quarterly basis. A core responsibility is setting goals and expectations for BC planning activities on a yearly basis. A BCP planning group consisting of a staff of three coordinates with each of the business units. Including the information systems group, there are 5 individuals who are DRII certified BC professionals: 3 local disaster recovery experts and 2 corporate-level experts. The Council has been instrumental in responding to issues that have been addressed including funding for additional information system back-up testing and planning for critical systems. A recent issue that has been addressed to the Council concerns a requirement for its service providers and suppliers to integrate BC planning into their operations.

While Amgen's BC approach was primarily developed in-house, it has utilized outside consultants to provide guidance in the development and execution of its BC process. Each site works with local authorities including police and fire. Amgen employs the ICS template for its larger sites and a modified version for its smaller sites. There are individuals responsible for these operations including the incident commander and recovery commander.

To identify risks, a hazard analysis is conducted at each site. Based on the activities that take place at each site, plans are developed to address different types of impact to a building from an infrastructure failure related to the local area. For instance, there have been incidents when Amgen had to generate its own power at its operations in Puerto Rico.

Amgen recognizes the importance of spreading its IT risks across its 2 back-up centers. It also contracts hot site support from third-party providers, like Sun Guard, for its larger systems. However, the organization is currently moving toward having other sites backed up on two main data centers at its corporate office. For the operational side, Amgen has deployed dual-site redundancy at facilities and duplicated key talent of people. Recovery time objectives (RTO) are based on the site and the business operation. For instance, Amgen has a critical operation on Rhode Island where the downtime is less than 4 hours. RTO for research sites is as much as 5 days. For corporate-wide downtime issues, the most critical business systems are needed back in operation within 4 hours.

While auditing its BC process does not analyze cost, it does determine if each of the business units meets internal standards and requirements for planning activities. Chris

Wright, manager of corporate emergency services, explained, “Auditing is done where we have a corporate standard document that requires a level of BCP for each of the business units.” In addition, Amgen utilizes risk management and insurance brokerage services of Aon Corporation and FM Global as its property insurer. These insurance companies assess the level of Amgen’s BC planning, exercise activities and training, among others.

Regulations that affect Amgen include the Health Insurance Portability and Accountability Act of 1996 (HIPPA) concerning security of personal health information and the Occupational Safety and Health Administration (OSHA) regulations regarding employee emergency planning.

Although making the business case for BC presents many challenges, BC is considered good business practice among many organizations including Amgen. For 2004 testing, travel and other expenses related to BC, Amgen spent from \$1 million to \$5 million excluding salaries. Wright, who is also vice president, private sector of BICEPP, summed up: “From an operational standpoint, investing in BC keeps the company in compliance. From a long-term perspective the company is more viable.” Organizations like Amgen will clearly have the advantage in today’s competitive global market of R&D by adding the element of BC to their corporate governance.

Company A is a subsidiary of a major international food company, which offers a broad product base, including chocolate and confections, beverages, ice cream, milk products, pet and baby food, prepared foods, and bottled water brands that are distributed by a separate subsidiary. Many of its brands are unique to particular countries, with products tailored to meet local tastes.

Described as having a role model BC program in the industry, Company A started its practice 11-12 years ago following the First Interstate Bank fire in Los Angeles in 1988. Likewise, this widely known high-rise fire turned the attention of many other organizations to initiate BC practices.

While Company A is domiciled in the U.S., its parent company takes an active role in promoting BC planning (BCP) as a high priority worldwide effort. The interview participant explained, "Our BC policy is on a global scale ... efforts are being standardized throughout the company so that all functions are using the same applications, systems, etc." Company A's role is to collaborate with the business units, factories, distribution centers, and customer service centers in the U.S. to ensure their recovery plans are "complete, current and effective in recovering the business." Supported by management, the BC process is led by a certified business continuity professional, who was certified through the program at DRII.

Company A utilizes BCP software and recovery services of Hewlett-Packard, Rentsys, and Strohl Systems, among others. In addition, off-site facilities are deployed for back-up purposes. With operations running 24/7, the downtime tolerance varies for each critical business function.

Unlike the compulsory requirements in the financial services industry, there have been no mandatory regulatory requirements that have affected the organization's BC practice. It is self-regulatory.

While Company A practices BIA, the interviewee pointed out that, "Testing of recovery plans is the most important factor and two recovery tests, including one full-scale test per year is desirable for the organization."

To keep up with BC trends, BCP and IT representatives of Company A attend BC and disaster recovery seminars, conferences, emergency training sessions, as well as other governmental training sessions. In the past, Company A representatives received Incident Command training at the California Specialized Training Institute, a training branch of the state of California Governor's Office of Emergency Services.

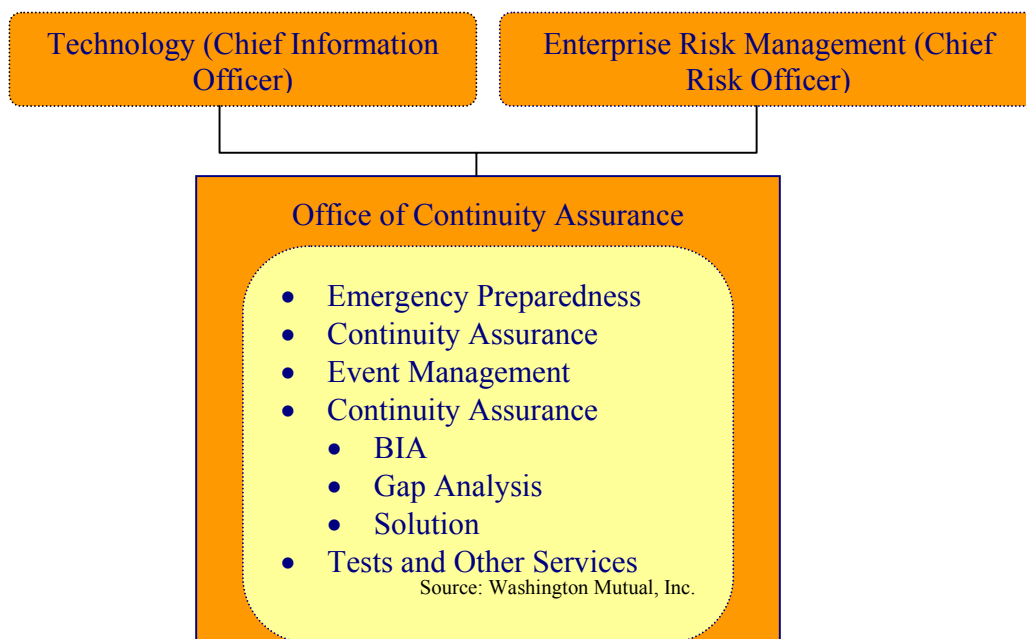
While BC is gaining widespread attention, there is clearly a consensus that attention is focused on BC usually after the occurrence of a major disaster. Once the disaster is resolved, the focus reverts back to day-to-day business priorities and away from BC. The interviewee pointed out, "We must be vigilant about making sure that recovery plans are in place and up-to-date." The interviewee added that BC planners could reinforce a

culture of risk-awareness and accountability through “on-going preparedness communications, recovery testing, and awareness programs in their companies.”

Washington Mutual

Washington Mutual, Inc. (Wamu) is established as one of the nation's leading financial services companies and continues to serve consumers and small to mid-sized businesses through the various subsidiaries in the Washington Mutual family of companies. The organization manages its activities, operations, products and services around its two customer categories: consumers and commercial clients.

Wamu's BC practice is a corporate-wide system centralized at its headquarters office in Seattle, Washington. The Office of Continuity Assurance is headed by Annie Searle, senior vice president, enterprise risk services. In 1999, Searle handled the technology recovery operations of the business. At that time, BC, insurance services and physical security were all part of the risk management department. In 2002, a BC plan was proposed to the executive committee. In 2003, the BC program was transferred to Searle, who presently has a staff that includes 3-4 DRII certified professionals.



At the corporate level, Wamu's Office of Continuity Assurance is staffed with a steering committee that sets BC standards and policy. They coordinate with the BC liaison of each of the divisions of the company. Each liaison is responsible for the recovery planning and implementation of policies and procedures for that particular division.

Wamu's annual report includes updated BC policies and events, mission critical processes, critical business processes, BIA results and the 'Readiness Rating' matrix, which is evaluated based on tests with a targeted recovery time, among others. Searle noted that in 2004, 2,000 mission critical processes were identified. In 2005, that number

increased to 2,700 processes. The board of directors reviews the BC report as they determine the order of recovery for the organization.

Readiness Rating Matrix	
Best Practices	High Resiliency
Satisfactory	Within Acceptable Risk Limits
Elementary	Basic
Insufficient	Low
Source: Washington Mutual, Inc.	

Eighty percent of Wamu’s BCP is dedicated to 1) protect data 2) continue operations. Provisions of the disaster recovery plan for IT assets allow each data center to recover its operations at an alternate data center. Recovery facilities are strategically located in Washington

and California and a new enterprise center is situated in Texas. The crisis management team is primarily based in Seattle, Washington. Like other organizations with advanced practices, Wamu regularly tests alternate sites and BC processes. As part of the program, Wamu’s risk ratings establish an order of priority that is then presented to the Executive Committee of the bank to validate for priority in the instance that all critical business processes disrupted simultaneously. Searle commented that Bank of America and Wells Fargo Bank has the same practice.

Its comprehensive and robust BC approach requires its vendors to implement a BC program that reflects Wamu’s practice. In addition, vendors must provide documents that demonstrate test results of existing BC plans. Among the bank’s interdependent business relationships with external organizations, those with advanced BC practices include AT&T, IBM, MCI and Fidelity.

A risk matrix model is used to determine the level of risk demonstrated by each vendor. For instance, a vendor that supports customer data is identified as a high risk vendor. Offshore vendors that focus on customer support or development require a site visit and audit by Wamu. In particular, when IT and business processes are outsourced to offshore locations, banks are faced with risk management challenges. From a regulatory perspective, offshoring issues bring enhanced due diligence from bodies including the Office of Thrift Supervision. Regulations enforce financial institutions like Wamu to tighten internal BC governance controls, standards, policies and protocols to minimize the impact of risks.

Recent legislations, such as SOX have also been having an impact on financial institutions. Other industry compliance requirements such as the FFIEC¹⁰ and the Gramm-Leach-Bliley Act¹¹, among others have also affected Wamu.

A particular strength of Wamu is its extensive involvement in public and private partnerships. For instance, Wamu embraces the ICS system and is connected to several other early and response tools. In addition, it collaborates with the Washington University’s earthquake program, the Financial Services Information Sharing and Analysis Center (FSISAC), the Secret Service in San Francisco, DHS, New York state

¹⁰ See Appendix A.

¹¹Gramm-Leach-Bliley Act of 1999 includes provisions to protect consumers’ personal financial information held by financial institutions.

and NY police. With a wide range of partnerships, Wamu does not limit itself to a single ICS. In addition, Wamu's program integrates wireless products such as Blackberry and ImpactWeather, Inc., a provider of forecasting, monitoring, and notification services.

Risk mapping for business interruptions has allowed Wamu to identify the following to be high probability and high-impact events: Hurricanes and tornados due to location of businesses, phishing and ID theft. Wamu performs annual table top testing, or scenario simulations using printed plan materials to prepare for such events.

In the organization, each mission critical process identifies its own RTO. The general practice is: 1 hour → 2 hours → 4 hours → 8 hours. For instance, RTO for the main frame and wire room is under 4 hours or half a business day. Most mission critical and business critical processes must be back in operation within 8 hours, or a normal business day.

Wamu's general BC budget that includes payroll, training, contracts with wireless providers and so forth excluding contracts with hot site vendors such as Sungard and other services is approximately between \$1million and \$5 million. While the value on BC will not be apparent until an event occurs, investing in BC "keeps Wamu clean and clear on a risk scale," expressed Searle.

Described as a "leading-edge bordering on world class," Wamu's BC program keeps up with emerging trends through guidance from external auditors, professional conferences and other meetings with peers.



Westcorp is a financial services holding company for Western Financial Bank, a federally chartered and insured savings bank that offers a wide range of services through its banking operations, which includes retail and commercial banking operations in Southern California. Westcorp also owns nearly 85% of publicly traded auto finance firm WFS Financial Inc, one of the nation's largest independent automobile finance companies.

In September 2005, North Carolina-based Wachovia, a major U.S. bank, announced that it has agreed to acquire Westcorp for \$3.42 billion. With the purchase, Wachovia will mark its entry in California's retail branch-banking market and into the non-prime auto loan market. The merger is expected to be completed in the first quarter of 2006.

Westcorp's BC practice, which includes IT recovery and business recovery, is viewed as a very critical operation to the company. Across the company, there are approximately 25 different BC teams. The teams are primarily within IT functions and major business functions. The board of directors takes an active leadership role and on an annual basis reviews the BC program, which is documented and reviewed by regulators. The board and senior management addresses and promotes BC practices.

In 2005, the company implemented a program that focuses on its vendors that are most critical to its operations. The program involves meeting with the vendors and reviewing their BC and disaster recovery plans and test results. As a result, 14 disaster recovery exercises were performed. The interviewee stressed, "The starting point for this process is really to get involved when a contract is signed with a vendor so that we are able to get the proper language reflecting BC and disaster recovery for the services it provides to us." To maintain a sustainable BC program, the business contract owner works closely with its legal department to discuss BC terms and conditions when contracting with vendors.

Westcorp has a combination of recovery mechanisms in the event of a business interruption. Multiple hot site vendors are used for different platforms. Some contracts with hot site providers offer ready computer systems and a certain percentage of application systems are recovered with these services. The company also has an internal backup recovery capability for certain systems at other sites. In addition, Westcorp has identified emergency operation centers within its organization and multiple backup facilities to relocate its operations. There are 3 major buildings in California and over 40 locations across the U.S. and 19 banking branches and 3 data center locations. In addition, each office is backed by another remote office that is equipped to perform the same business operations. For example, during one event, its office in Florida was evacuated in response to a hurricane and another office in a different state assumed its operations.

By applying a Business Impact Analysis-type process, Westcorp has identified the cost of downtime for mission critical and business critical applications on an annual basis. The interviewee noted, "We break all of our critical systems by: mission critical, business

critical and all other.” RTO for mission critical functions is within 48 hours. RTO for business critical functions is within 72 hours.

Westcorp’s plans are developed in-house based in MS Office Applications (MS Word, Excel) and others. Westcorp requires the business owners of the plans to certify the plans quarterly. The plans are subject to be table-top tested quarterly.

Westcorp uses an Incident Management (IM) process that works in concert with the Incident Command System (ICS) used by Federal and State emergency response agencies (i.e., FEMA, fire, police, etc.). The IM process addresses those activities required after the initial emergency response completes and incident management is turned over to the Westcorp Executive Management Team (EMT). It describes how Westcorp will communicate both internally with our associates and how external communications should be addressed with the news media, customers, dealers, shareholders, vendors and key investors.

Like most financial companies, Westcorp invests heavily in complying with the requirements of the OTS, SEC, and FFIEC, among others regarding BC and disaster recovery. The interviewee added, “A lot of the banking regulators refer to the council’s document as a guideline. The OTS and the Federal Reserve Board do have their own audit programs, but the majority in the banking industry will use the council’s document as a guideline. Government agencies perform the actual evaluation and audit.”

6. Conclusion

In August 2001, FEMA held a training session for state emergency-preparedness officials that discussed the three most likely catastrophes to hit the United States, according to the Los Angeles Times. First on the list was a terrorist attack in New York. Second was a powerful hurricane striking New Orleans. Third was a major earthquake on the San Andreas fault¹² in Southern California. Given the passing of the first two events, earthquake experts are reassessing how to manage a major quake. The Southern California Earthquake Center reported that there is an 80% to 90% chance of a tremor of seven or higher on the Richter scale hitting Los Angeles within the next 20 years. Six in ten Californians live in areas of high earthquake risk.¹³

Despite seismic improvements, officials believe the worst case scenario could mirror the level of destruction and disruption experienced on the Gulf Coast. Although California is better than where it was 5-10 years ago, it is certainly not prepared. More than 900 hospitals still require retrofitting and those that cannot meet the 2008 deadline have received five-year extensions. About 78% of hospitals have at least one facility at risk according to the California Hospital Association. Across the state, more than 7,000 schools are also vulnerable. About a third of masonry buildings, considered the most likely to collapse remain unreinforced.¹⁴ Furthermore, an impact to California's major aqueducts and gas lines that are located near the fault could have an adverse effect on critical infrastructure. These scenarios are a wake up call for society to foster interest and responsibility toward BCM capabilities in dealing with an increasingly complex environment.

In today's competitive and uncertain global economy, a forward-thinking trend is to align national BCM development efforts to those worldwide. Multinational companies should benchmark their local practices against internationally agreed standards. Another consideration is to develop an integrated BCM policy that is applicable throughout the organization, whether at a head office in New York or a branch office in Tokyo.

Another growing reality is addressing BCM challenges during mergers and acquisitions, which usually entails some organizational turmoil, leadership changes and cost-cutting measures. This points the need for a shift toward greater intra-organizational and inter-organizational cooperation among partnerships across all channels. With many interdependent relationships, BCM policies will have to be flexible regardless of industry, business operations, geographic location and size. For example, in the financial services industry, what is acceptable for one institution may be more than what the next institution needs to recover their businesses due to their different mix of services.

More importantly, as BCM governance is steered by the decision-making in the boardroom, any shift in the attitude of policy setters can affect the broader economy

¹² Hector Becerra and Jia-Rui Chong. ". Los Angeles Times. "California Earthquake Could Be the Next Katrina". September 8, 2005.






¹³ "Getting Ready for the Big One". The Economist. September 17, 2005.

¹⁴ Hector Becerra and Jia-Rui Chong ". Los Angeles Times. "California Earthquake Could Be the Next Katrina". September 8, 2005.

beyond the direct impact to the organization from an unforeseen event. This suggests a crucial part of any decision-making process must consider how well risks are managed. The broad view of organizational responsibility and accountability forms the basis for the concept of corporate social responsibility, the triple bottom line reporting that incorporates economic, social and environmental performance considerations in evaluating overall company performance including tangible and intangible benefits such as keeping a company competitive and protecting its brand image and reputation. Thus, one consideration is to make policies and procedures of a sustainable BCM program transparent to the public as it has a direct influence and impact on the triple bottom line. As BCM is an integral part of the business model that maximizes long-term stakeholder value, it should also be linked to corporate governance. Organizations should be committed to maintaining adequate to high standards of continuous improvement in BCM to meet the present and future needs of its stakeholders. From this perspective, BCM should be incorporated as another discipline to corporate governance and corporate social responsibility.

Appendices

Appendix A: Federal Financial Institutions Examination Council (FFIEC) Regulatory Agencies

	<p>The Federal Reserve Board (FRB) has supervisory and regulatory authority over a wide range of financial institutions and activities. It works with other federal and state supervisory authorities to ensure the safety and soundness of financial institutions, stability in the markets, and fair and equitable treatment of consumers in their financial transactions.</p>
	<p>Federal Deposit Insurance Corporation (FDIC) establishes standards and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System</p>
	<p>The National Credit Union Administration (NCUA) is the federal agency that charters and supervises federal credit unions and insures savings in federal and most state-chartered credit unions across the country through the National Credit Union Share Insurance Fund (NCUSIF), a federal fund backed by the full faith and credit of the United States government.</p>
	<p>The Office of the Comptroller of the Currency (OCC) charters, regulates, and supervises all national banks. It also supervises the federal branches and agencies of foreign banks. Headquartered in Washington, D.C., the OCC has four district offices plus an office in London to supervise the international activities of national banks.</p>
	<p>The Office of Thrift Supervision (OTS) is the primary regulator of all federally chartered and many state-chartered thrift institutions, which include savings banks and savings and loan associations. OTS was established as a bureau of the U.S. Department of the Treasury on August 9, 1989, and has four regional offices located in Jersey City, Atlanta, Dallas, and San Francisco. OTS is funded by assessments and fees levied on the institutions it regulates.</p>
<p>Source: FFIEC</p>	

The FFIEC BC Planning booklet provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services. The information in this appendix is provided by FFIEC.

The FFIEC advises that comprehensive planning should be conducted using the following approach:

Business Impact Analysis

- Identification of the potential impact of uncontrolled, non-specific events on the institution's business processes and its customers
- Consideration of all departments and business functions, not just data processing
- Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses.

Risk Assessment

- A prioritizing of potential business disruptions based upon severity and likelihood of occurrence
- A gap analysis comparing the institution's existing BC planning to what is necessary to achieve recovery time and point objectives
- An analysis of threats based upon the impact on the institution, its customers, and the financial markets

Risk Management

- Written and disseminated so that various groups of personnel can implement it in a timely manner
- Specific regarding what conditions should prompt implementation of the plan
- Specific regarding what immediate steps should be taken during a disruption
- Flexible to respond to unanticipated threat scenarios and changing internal conditions
- Focused on how to get the business up and running in the event that a specific facility or function is disrupted
- Effective in minimizing service disruptions and financial loss

Risk Monitoring

- Ensures a BC plan is viable through testing, independent review, and periodic updating. Four types of tests are outlined:
 - ✓ Walk-through
 - Discussion about the BC planning in a conference room or small group setting
 - Individual and team training
 - ✓ Table-top Drill
 - Practice and validation of specific functional response capability
 - Role playing with simulated response at alternate locations/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment
 - Mobilization of all or some of the crisis management/response team
 - ✓ Functional Testing
 - Demonstration of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning
 - Actual or simulated response to alternate locations or facilities using actual communications capabilities
 - ✓ Full-Scale Testing
 - Validation of crisis response function
 - Demonstration of knowledge and skills, as well as management response and decision-making capability
 - On-the-scene execution of coordination and decision-making roles
 - Actual, as opposed to simulated, notification, mobilization of resources and communication of decisions
 - Activities conducted at actual response locations or facilities

Additional Guidelines

- A formal audit of the BC planning should be conducted at least annually and presented to management and the Board of Directors for approval.
- An independent party should review the BC planning and tests.
- Senior management and boards of directors should review five specific areas of responsibility with regards to BC planning.
- Examiners and auditors should determine if financial institutions have appropriate strategies that include continuity for interdependent entities and stakeholders, including utilities, telecommunications, third-party technology providers, key suppliers, business partners, customers and so forth.

Appendix B: Disaster Recovery Institute International (DRII) – Subject Area Overview

The following information is provided by DRII:

1. Project Initiation and Management

Establish the need for a Business Continuity Management (BCM) Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organizing and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.

2. Risk Evaluation and Control

Determine the events and external surroundings that can adversely affect the organization and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

3. Business Impact Analysis

Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.

4. Developing Business Continuity Management Strategies

Determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the organization's critical functions.

5. Emergency Response and Operations

Develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Center to be used as a command center during the emergency.

6. Developing and Implementing Business Continuity and Crisis Management Plans

Design, develop, and implement Business Continuity and Crisis Management Plans that provide continuity within the recovery time and recovery point objectives.

7. Awareness and Training Programs

Prepare a program to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management Program or process and its supporting activities.

8. Maintaining and Exercising Plans

Pre-plan and coordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organization's strategic direction. Verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

9. Crisis Communications

Develop, coordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, Internet, etc.).

10. Coordination with External Agencies

Establish applicable procedures and policies for coordinating continuity and restoration activities with external agencies (local, state, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes or regulations.

Interviews

Ms. Tessa Badua-Larson. Federal Emergency Management Agency. Program Specialist. July 5, 2005. Oakland, California.

Mr. Eric A. Beck. Deloitte & Touche LLP. Enterprise Risk Services and Security Services Group. Senior Manager. June 16, 2005. Parsippany, New Jersey.

Mr. Casey De Shong. Federal Emergency Management Agency. Congressional & Intergovernmental Affairs Specialist. July 5, 2005. Oakland, California.

Mr. Robert Fenton. Federal Emergency Management Agency. Chief, Response and Recovery Division. July 5, 2005. Oakland, California.

Mr. James D. Goltz. California Governor's Office of Emergency Services. Outreach Manager for the Earthquake Program, California Integrated Seismic Network, Disaster Assistance Division. Business and Industry Council for Emergency Planning and Preparedness. Board member. June 17, 2005. Pasadena, California.

Mr. Farley Howell. Federal Emergency Management Agency. National Preparedness Division Director. July 5, 2005. Oakland, California.

Mr. Robert G. Lee. Business and Industry Council for Emergency Planning and Preparedness. Executive Director. North Hills, California.

Ms. Kathleen McGrorty. Deloitte & Touche LLP. Audit and Enterprise Risk Services - Business Continuity Management. Senior Manager. April 20, 2005. Los Angeles, California.

Ms. Caren Roberson. Westcorp. Vice President. Director of Marketing Communications. June 15, 2005. Irvine, California.

Mr. David M. Sarabacha. Deloitte & Touche LLP. Business Continuity & Security Services. Senior Manager. June 16, 2005. Dallas, Texas.

Ms. Annie Searle. Washington Mutual Bank. Senior Vice President, Enterprise Risk Services. June 14, 2005. Seattle, Washington.

Ms. Sarah Shields. U.S. Department of Homeland Security, Office of Public Affairs. July 5, 2005. Washington, DC.

Ms. Kelly Shivertaker. Southern California Edison. Manager, Emergency Planning & Preparedness. Business and Industry Council for Emergency Planning and Preparedness. President. June 17, 2005. Rosemead, California.

Mr. Chris Wright. Amgen Inc. Manager, Corporate Emergency Services. Business and Industry Council for Emergency Planning and Preparedness. Vice President, Private Sector. June 15, 2005. Thousand Oaks, California.

Ms. Sally Ziolkowski. Federal Emergency Management Agency. Mitigation Division
Director. July 5, 2005. Oakland, California.

Works Cited

Chong, Jia-Rui; and Becerra, Hector. Los Angeles Times. "California Earthquake Could Be the Next Katrina". September 8, 2005.

The Economist. "Getting Ready for the Big One". September 17, 2005.

Gaouette, Nicole. "A Diminished FEMA Scrambles to the Rescue". Los Angeles Times. September 1, 2005. <http://www.latimes.com/news/nationworld/politics/la-na-fema1sep01,1,7749651.story?coll=la-news-politics-national>

Gilbert, Alorie. "Data recovery firms slog through the post-Katrina Gulf Coast". Cnet News.com. September 5, 2005. <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/09/05/BUGG0EHTR01.DTL&type=printable>

Rogers, David; and Fields, Gary. The Wall Street Journal. "Already Under Scrutiny, FEMA Is Now In The Spotlight". August 31, 2005.