

**Deloitte.**



---

Audit & Enterprise Risk Services

---

# Continuing the Journey

## The 2005 Business Continuity Survey

Audit • Tax • Consulting • Financial Advisory.

# Table of Contents

1	Foreword
2	Executive Summary
3	Survey Objectives
4	The Survey Process: Design, Implementation and Evaluation
6	Key Findings
12	Conclusion
13	Appendix A: Analysis of Individual Questions
18	Appendix B: Statistical Summary

# Foreword

A man in a dark suit stands with his back to the camera, looking out of a large window with horizontal blinds. The window is partially open, and the light from outside is visible. The room has a blue carpet with a small pattern. The overall tone is professional and contemplative.

The CPM Group (CPM) and Deloitte & Touche LLP (Deloitte & Touche) are pleased to present the results of the **2005 Business Continuity Survey**. This sixth annual survey demonstrates that the business continuity function, and its professional practice, both continue to play an important role in operational risk management. Survey results show that executive management remains primarily concerned with regulatory compliance, and with fulfilling fiduciary responsibilities by addressing operational resilience in response to a broad array of disruptive events.

The survey results also suggest that significant progress has been made in extending business continuity planning initiatives at the enterprise level. However, as you will see from the findings to follow, more work lies ahead in achieving full enterprise implementation and optimal risk mitigation.

# Executive Summary

The Deloitte & Touche/CPM 2005 Business Continuity Survey finds that investment in Business Continuity Management (BCM) has been elevated and extended to the enterprise level. Just six years ago, only 30% of respondents had corporate business continuity plans, including those addressing crisis management. Now, more than 83% have formal business continuity plans, and 56% have crisis management plans that have been tested. These survey results confirm that proactive Crisis Management Planning has now become a core requirement of most BCM programs, as evidenced by the strong commitment to expanded testing. We have seen strong Financial Services Industry (FSI) participation in this trend, with the following industries indicating plans are developed and tested at least annually: Banking/Investment Banking (61%), Telecommunications (60%), Other Financial (59%), Utilities (56%), Insurance (50%), and Brokerage (40%).

While operational resilience and fiduciary accountability remain key business drivers, survey results also identify regulatory compliance as a growing influence on management's decision to expand investment in BCM. Nearly a quarter of survey respondents indicate that regulatory compliance will continue to shape investment priorities during the next five years, while 18% indicated such compliance has been a key driver in the past. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), NASD 3510, Sarbanes-Oxley, and Basel II have all contributed directly to, or have heavily influenced, BCM investment across a wide range of industry groups.

BCM governance has become a somewhat more important consideration of executive management, with survey results indicating that 21.6% of responding organizations have established formal BCM Steering Committees, up less than three points from a year ago. However, executive focus on enhanced governance is evidenced by the fact that 34.4% of responding organizations have BCM reporting into an executive management function, and 13.6% reporting to Corporate Risk Management. As an example, in the financial services industry, 31.2% of the respondents indicate their BCM function is reporting directly to an executive management function, and 22% reporting to Corporate Risk Management.

Finally, an objective for our 2005 survey was to understand to what extent private sector organizations see value in U.S. Government initiatives to assist in responding to the threat of terrorist attacks. Our survey found that more than 50% of participating organizations believe that Department of Homeland Security's (DHS) Threat Advisory System rarely has value in supporting their own contingency response planning. Our findings are consistent with recent U.S. Government Accountability Office testimony before Congress that offered several recommendations for improving related communications between the DHS and the private sector.

These key findings, along with other important BCM benchmarks, have been detailed on the following pages of this report.

# Survey Objectives

The 2005 Business Continuity Survey aims to help your organization assess the state of Business Continuity Management, relative to other comparable firms and industries. Overall, the survey attempts to answer the basic but important question: **How does the level of business continuity preparedness for my organization compare to that of other companies?** CPM and Deloitte & Touche have analyzed survey data that compares key BCM attributes for several key market segments. The study has attempted to address key BCM risk management questions that include the following:

- Where has BCM been organizationally deployed?
- How much should be budgeted for BCM activity?
- What level of staffing should be dedicated to BCM?
- How will the regulatory environment influence BCM priorities?
- What trends are occurring in BCM governance?
- How are homeland security concerns influencing BCM programs?
- How are management tolerances for operational downtime changing?
- What changes are occurring in BCM testing strategy?
- How is BCM being affected by new risk management standards?

In addressing these questions, we believe that business continuity and risk management professionals will have a better benchmark of how to optimize risk mitigation investments in their organization.



# Survey Process

## Design, Implementation, and Evaluation



The Deloitte & Touche/CPM 2005 Business Continuity Survey was designed to measure the current state of BCM program initiatives across a wide range of public and private sector institutions. By doing so, we are able to report on key BCM benchmarks for comparison within and across organizations of various sizes and industries. By understanding your organization's strengths and weaknesses in BCM, and comparing your organization to key industry benchmarks, your management team will be better prepared to make effective decisions on how to mitigate risk and properly invest in its BCM program initiatives now and in the future.

Senior members of the Deloitte & Touche Security Services Group, along with senior staff at CPM, designed a questionnaire that was built on the findings of last year's survey and investigated various strategic and operational areas of business risk, response, and recovery.

### **Survey Participation**

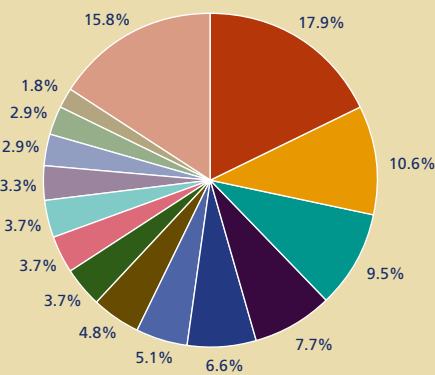
The survey scope was primarily centered on North America, and solicited the participation of a number of public and private sector organizations across a wide range of vertical market segments.

### **Survey Participant Demographics**

Deloitte & Touche and CPM sought a broad range of organizational participation in the 2005 Business Continuity Survey as a basis for enhanced reporting of results by industry group. Our 2005 Survey included 273 respondents, the broadest participation we have seen during the past six years, with specific breakdown by industries and job functions described as follows:

**Survey Respondents by Industry**

The population of survey respondents included a broad base of industry representation, with approximately 40% coming from Financial Services and 60% from other industry groups.

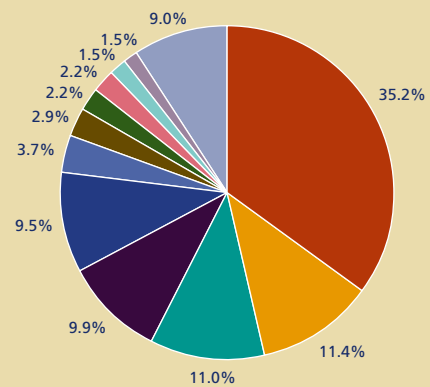


**Breakdown by Industry**

- Banking/Invest. Banking
- Other Financial
- Insurance
- Manufacturing/Industrial
- Government-All Levels
- Professional Services
- Retail/Wholesale
- Telecommunications
- Healthcare Provider
- Computer Infrastructure
- Utilities
- Education
- Data Processing
- Brokerage
- Other

**Survey Respondents by Job Function**

The population of survey respondents included 46% from business continuity and disaster recovery management, with broad based representation from other management functions.



**Breakdown by Job Description**

- Bus. Continuity Mgmt.
- Disaster Recovery Mgmt.
- IT Management
- Risk Management
- Executive/Senior Mgmt.
- Security Mgmt.
- Business Operations Mgmt.
- Auditor
- Administrative Support
- Crisis Mgmt.
- Data Center Mgmt.
- Other

**Creating the Questionnaire**

Senior staff members from Deloitte & Touche and CPM developed the 2005 questionnaire by considering topics that were judged both relevant and timely. Several questions were incorporated that would reflect key aspects of business continuity program management, crisis management, and emergency response.

**The Data Collection Process**

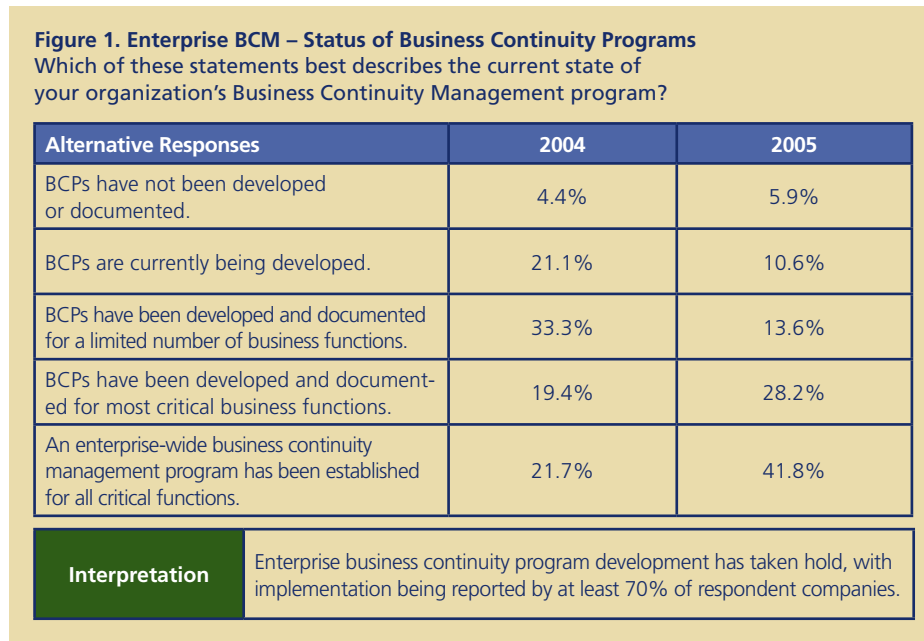
Once finalized, the 2005 questionnaire was posted to the CPM Group website. Participation was sought through targeted e-mail invitations and direct solicitation to Deloitte & Touche/CPM clients.

**Results Analysis**

Members of both Deloitte & Touche and CPM staffs participated in the analysis of data received from survey respondents. Our teams used research tools to cross-tabulate survey results and to prepare analyses measuring industry benchmarks.

# Key Findings

Deloitte & Touche and CPM are pleased to present key findings from the 2005 Business Continuity Survey. We believe these findings will offer executive management and BCM professionals in both the public and private sectors key benchmarks that will enable BCM assessment with peer organizations. We want to thank all participants for taking time to respond to this 2005 survey.



## Investment in Enterprise Level BCM

We are pleased to report that BCM programs appear to have been elevated and extended to the enterprise level, with implementation being reported for “most” or “all” functions by at least 70% of respondents, up from 41% in 2004 (see Figure 1). Financial Services Industry (FSI) firms continue to lead the way in enterprise level BCM investment. Survey results show strong BCM program investment levels in Banking (96%), Insurance (92%), and other FSI firms (90%). Survey results also indicate significant investment in enterprise BCM in Telecommunications (70%), Government (65%), Retail (62%), Brokerage (60%) and Computer Hardware/Software Manufacturers (60%).

Survey results also indicate that crisis management plans are seeing increased investment, along with an expanded commitment to annual testing among 41% of survey respondents, up from 29% in 2004 (see Figure 2). We have seen strong FSI industry participation in this trend: Banking/Investment Banking (61%), Telecommunications (60%), Other Financial (59%), Utilities (56%), Insurance (50%), and Brokerage (40%) indicating plans are developed and tested at least annually.

Enterprise-level BCM also appears to be supported by an increased level of funding. Across all survey respondents, the number of organizations reporting annual BCM budget allocation in excess of \$1 million has increased to 29%, up from 18% in 2004.

**Figure 2. Enterprise BCM – Crisis Management Planning**  
Which of these statements best describes the current state of your organization's Crisis Management plan?

Alternative Responses	2004	2005
Responsible Executives are identified, but there is no formal crisis management plan or assigned roles and responsibilities.	23.3%	20.5%
Crisis Management and Emergency Response Team members are identified, and a Crisis Command Center has been established.	22.8%	23.1%
Crisis Management and Emergency Response Team plans are informal and partially tested.	25.0%	15.0%
Crisis Management and Emergency Response Team plans are developed and tested annually.	25.0%	34.4%
Crisis Management and Emergency Management Team plans are tested at least quarterly.	3.9%	7.0%

#### Interpretation

Organizations are expanding their investment in formal Crisis Management Programs, and are incorporating these plans into their testing programs.

**Figure 3. Regulatory Drivers – Status of Regulatory Compliance**  
Which of these statements best describes the current state of your organization's regulatory and industry compliance?

Alternative Responses	2004	2005
Awareness of regulatory requirements is limited to internal audit and compliance functions.	20.6%	13.2%
Business units are aware of regulatory, compliance, legal and industry issues affecting them.	25.6%	26.4%
A BIA is performed periodically to identify legal/regulator issues and quantify potential fines or penalties.	12.8%	11.7%
Executives understand existing regulatory issues, and the organization is fully compliant with minimal audit exception.	35.6%	38.1%
The organization maintains membership on regulatory boards and works to constructively influence regulatory direction.	5.6%	10.6%

#### Interpretation

Executive management is becoming increasingly focused on the regulatory side of business continuity, placing greater emphasis on the need to measure and monitor compliance.

## Growing Influence of Regulatory Drivers on BCM Investment

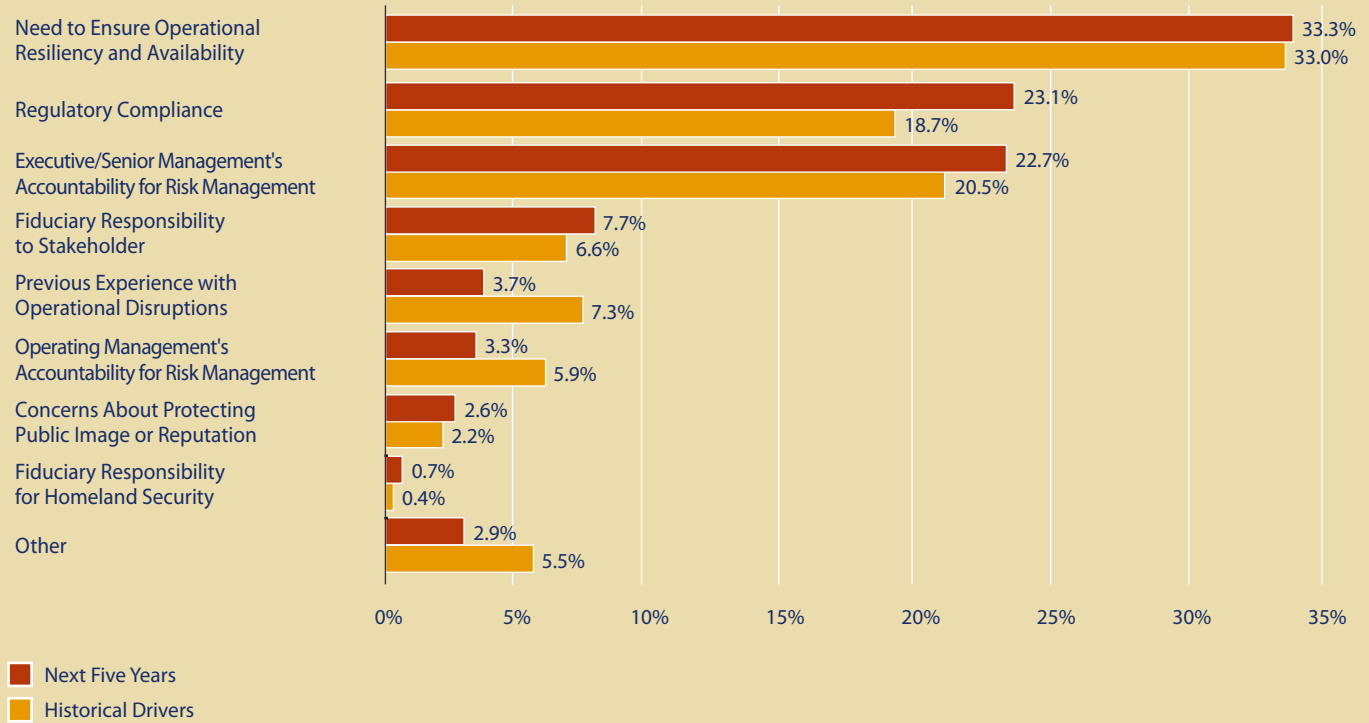
Changes in the public regulatory environment during the past five years appear to be having a collective influence, either directly or indirectly, on the number of organizations reporting BCM investment. As such, we have observed that regulatory considerations have become a key driver for investment in BCM programs, placing greater emphasis on the need to measure and monitor compliance. Survey results below show a shift in focus that extends beyond simply understanding regulatory issues and requirements, with respondents reporting only a 7% increase in such understanding and full compliance since 2004 (see Figure 3). Instead, the number of responding organizations engaged in membership on regulatory boards and/or working to influence regulatory direction increased significantly in 2005 to 10.6%, up from 5.6% in 2004.

Further, survey results also indicate that executives are becoming increasingly involved in BCM governance and oversight because of regulatory compliance concerns, presumably as regulators place greater emphasis on accountability for overall risk management (see Figure 4).

## Regulatory Requirements

We have also seen many opportunities where regulatory requirements elevate executive management's awareness and willingness to invest in business continuity. Most recently, this includes compliance with NASD (National Association of Securities Dealers) Rule 3510 within the Brokerage Industry that focuses on the recoverability of securities processing. Likewise, the requirements of the US Health Insurance Portability and Accountability Act (HIPAA) within the Healthcare Industry mandate contingency planning for patient data.

Figure 4. Business Drivers for Establishing a Business Continuity Program



From an industry perspective, survey results indicate that concerns about regulatory compliance appear to be having the greatest emphasis on BCM in Telecommunications (70%), Banking (60%), Utilities (56%), Manufacturing (52%), Insurance (48%), and Non-Brokerage Financial (62%)

This 2005 Business Continuity Survey also finds that regulatory requirements are having a significant influence on the identification, classification, and off-site relocation of critical vital records and data. Aggregate survey results indicate that the number of organizations that have identified vital records from both a regulatory and business process perspective grew from 13.9% in 2004 to 23.4% in 2005, a first step in critical data/record protection. The impact of HIPAA regulations was apparent in record identification, with the Healthcare (60%) and Pharmaceutical (50%) industries leading this trend.

### Management's Tolerance for Downtime

Driven by business mandates, regulatory requirements, enabling technologies, and the changing economics of IT infrastructure, management's tolerance for operational downtime have been in steady decline for some years. This year's survey results continue to validate this trend, indicating management's tolerance for operational downtime continues to decline, with recovery time objectives for core operations being set at hours, not days.

In aggregate, 12.1% of survey respondents indicated their organizations had zero tolerance for operational downtime for their most critical activities, up from 5.6% in 2004 (see Figure 5). There was not significant variance across industries: Perhaps surprisingly, our results indicate that a requirement for zero downtime is not unique to the Financial Services industry (FSI)<sup>1</sup>. Analysis indicates that some participants from industries including Utilities, Healthcare, Manufacturing, and Computer Infrastructure report zero tolerance for downtime for their most critical activities. 12.8% of survey respondents from finan-

<sup>1</sup> The Financial Service Industries (FSI) identified include Banking, Investment Banking, Brokerage, Insurance, and other firms identified by respondents as FSI.

**Figure 5. Management Tolerance – Core Business Recovery Times**  
 If your core business function operations are interrupted, what is your organization's tolerance for downtime (i.e., recovery time objectives) for your most critical activities?

Alternative Responses	2004	2005
Zero tolerance for downtime	5.6%	12.1%
Less than two hours	18.3%	16.1%
Two to eight hours	43.9%	19.0%
Eight to 24 hours		27.1%
24 to 72 Hours	13.3%	17.9%
72 Hours to 5 days	18.9%	5.9%
Greater than 5 days		1.9%

**Interpretation** Tolerance for downtime continues to decline in most organizations, with Recovery Time Objectives for core business functions being established in hours not days.

cial services companies indicated zero tolerance for operational downtime for their core operations, compared to 11.6% across all other industries. Still, 55% of FSI respondents report tolerances of “eight-hours” or less for core operation compared to 42.1% across all other industry respondents, indicating that FSI is less tolerant of down-time.

### Homeland Security Advisory System

DHS periodically issues Threat Condition ratings along with Advisories in order to provide “actionable information” about credible threats targeting our nation’s critical infrastructure. Given the level of private sector investment in critical infrastructure, we asked survey respondents “To what extent has your company developed contingency plans that respond to changes in DHS Threat Condition ratings and related Advisories?” The 2005 survey found that almost 70% of respondents indicate that DHS Advisories and/or changes to Threat Condition ratings are not considered in determining their response to threat events (see Figure 6). Only 16.5% of respondents indicated that such DHS communications are monitored for either reactive (4.5%) or proactive (11.7%) response. Of these respondents, the Utility industry indicated the greatest likelihood of responding to such threats, with almost 67% of respondents indicating some form of reactive or proactive response pattern.

Similarly, our survey found that approximately 50% of respondents indicated that DHS Threat Condition ratings rarely provided value in determining how they will respond to potential threats. (see Figure 7). Only 16.5% of respondents indicated that such communications often or always had value.

As stated by the U.S. Government Accountability Office (GAO) testimony<sup>2</sup> before Congress in 2004, “The value of the Homeland Security Advisory System will be the extent to which it is useful as guidance for and actually used in the implementation of prevention, vulnerability reduction, and response and recovery measures by relevant parties, including the general public.” As such, half of the survey respondents are reporting that DHS communications are providing limited value to contingency planning and response initiatives. There may be several reasons for this. For example, actionable information from DHS requires a level of specificity that cannot be consumed by private sector organizations that lack proper security clearance to receive it. Additionally, DHS information on threat conditions is frequently not specific enough to provide direct guidance to organizations that may be at risk. While the GAO has reported several recommendations for improving the Homeland Security Advisory System, time will tell whether expected improvements in this system will result in the value expected by the government for future DHS communications.

<sup>2</sup> U.S. General Accounting (currently Government Accountability) Office Publication #GAO-04-538T, Mr. Randall A. Yim, Managing Director – Homeland Security and Justice Issues, Testimony Before the Subcommittee on National Security, Emerging Threats, and International Relations Committee on Government Reform, House of Representatives, March 16, 2004, “Homeland Security – Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System.”

**Figure 6. Private Sector Use of Homeland Security Advisories**  
The Department of Homeland Security (DHS) periodically issues Threat Condition Ratings along with Advisories that contain “actionable information” about credible threats to our nation’s critical infrastructure.

<b>Question</b> – Given that approximately 85% of critical infrastructure is privately owned, to what extent has your company developed contingency plans that respond to changes in DHS Threat Condition Ratings and related Advisories?	
Alternative Responses	Percent
Contingency response plans do not consider DHS Advisories or change to Threat Condition Ratings.	50.5%
Contingency response plans do not consider DHS Threat Condition Ratings/Advisories, but they are monitored.	19.0%
DHS Threat Condition Rating/Advisories are monitored, with plans designed for general reactive response.	13.9%
DHS Threat Condition Rating/Advisories are monitored, for potential reactive response to specific threats.	4.8%
DHS communications are monitored with proactive response to Threat Condition Ratings and reactive response to Advisories.	11.7%

### BCM Budget Allocation

Analysis of survey responses included cross-tabulation of key demographic data, including the comparative relationships between reported revenue and BCM budget (see Appendix B – Figure 1). Deloitte & Touche and CPM analyzed revenue-to-budget responses for both financial services companies and those in other industries. The 2005 survey results show that FSI firms with at least \$50 Million in annual revenues allocated at least twice the budget for BCM compared with non-FSI companies. For organizations with \$50 Million or less, 2005 BCM budget allocation appears to be roughly equivalent between FSI and non-FSI firms.

Survey results also indicate that 20.5% of all responding organizations reported having no formal budget allocation for Business Continuity Management at all.

### BCM Staffing Levels

The 2005 survey analysis indicates a strong correlation between BCM budget allocation and full-time equivalent (FTE) staffing dedicated to business continuity planning. Based on a mode scoring (see Appendix

**Figure 7. Homeland Security – Value of DHS Advisories**  
In March 2004, the U.S. Government Accountability Office (GAO) released a report citing the needs for improvements in the DHS Homeland Security Advisory System. The GAO noted the federal, state, and local officials have requested that DHS provide more specific information when releasing Threat Advisories so that contingency response can be designed and concentrated more effectively.

<b>Question</b> – Given that GAO’s concern, how valuable do you consider the information contained in DHS Threat Advisories in helping to determine how your organization will respond to potential threats?	
Alternative Responses	Percent
DHS Threat Advisories have no value.	24.9%
DHS Threat Advisories rarely have value.	25.3%
DHS Threat Advisories sometimes have value.	33.3%
DHS Threat Advisories often have value.	9.9%
DHS Threat Advisories always have value.	6.6%

B – Figure 2), the survey data showed that full-time staffing of business continuity functions will normally be seen in organizations whose BCM budgets exceed \$500,000. Above this level, survey results indicate that organizations will dedicate one FTE in support of BCM program operations for every \$750,000 to \$1.5 Million in BCM budget allocation (see Appendix B – Figure 2). Given market pricing for qualified staff, this means that firms are making significant BCM investment in areas other than personnel, perhaps in redundant facilities, communications infrastructure, vital records and data protection solutions, redundant equipment, training, and other critical requirements.

However, as stated above, FSI organizations do allocate more budget than do non-FSI companies; thus the absolute numbers of BCM practitioners in FSI firms is considerably higher than in other industries.

### BCM Governance

The survey results indicate that governance of BCM has become a more important consideration among executive management versus what was reported in the 2004 survey but only slightly so. There is a small increase in the number of respondents reporting that executives are more aware and involved in BCM program oversight and agenda setting during 2005 (see Figure 8).

**Figure 8. Convergence of Business Continuity Management**  
Which of these statements best describes the current state of your organization's BCM management leadership and convergence?

Alternative Responses	2004	2005
Board of Directors and executive management attention to BCM is limited to audit cycles.	14.4%	8.4%
Executive management is aware that BCM plans may exist, but their commitment to enhanced BCM is limited and inconsistent.	33.3%	34.8%
A BCM Steering Committee has been formalized and is engaged, with business unit and IT leadership being fully aligned.	18.9%	21.6%
A formal and comprehensive Business Continuity Management governance structure is in place.	16.7%	16.5%
Executive management is actively involved in setting BCM program priorities and agenda.	16.7%	18.7%

#### Interpretation

Prudent risk management and regulatory drivers (e.g., Sarbanes-Oxley) are influencing the establishment of formal governance initiatives that oversee business continuity.

One key measure of executive management's commitment to effective BCM governance is where in their organization they place BCM responsibilities. Survey results indicate that 34.4% of organizations have BCM reporting into an executive management function, while IT management retains the BCM function in approximately 23.8% of all organizations (see Appendix B – Figure 3).

Of special note is this year's finding that a growing number of FSI organizations appear to be placing business continuity planning within the Corporate Risk Management function. In 2005, 22% of FSI organizations report that BCM is placed within Corporate Risk Management, up from 16.1% in 2004. This trend appears to be most evident in banking and investment banking where these firms are now addressing Basel II compliance, and are seeking to coordinate operational risk management efforts, including business continuity. Centralizing operational risk management under a common reporting structure may give these organizations a better chance of improving their risk mitigation investments and facilitating regulatory compliance.

## Concentration Risk

Although it has long been a business continuity consideration, concentration risk became a focus issue for boards of directors, executive management, and corporate risk managers following the events of September 11. Recognizing that centralized operations create potential exposure in the event of a targeted attack, many organizations have considered decentralizing their operations in order to reduce risk and enhance resiliency. Such

consideration would require a risk mitigation approach that considers the level of acceptable concentration in the deployment of key people (e.g., executives, operations, and staff), critical business processes, and supporting technology infrastructure (e.g., IT, facilities, and utilities).

Deloitte & Touche and CPM sought to understand the level of concern organizations have placed on concentration risk, and to assess how such concern has influenced implementation of both decentralized business and data center operations.

When analyzing results by industry, Financial Services Industry (FSI) firms emphasize decentralized business operations to a higher degree than non-FSI organizations, as well as for their data centers (see Appendix B – Figure 4). For example, 74.3% of FSI firms reported anywhere from a limited to significant commitment to decentralized business operations, and 77.1% for data center operations. This can be compared to non-FSI who report 39.7% and 46.7% for business and data center operations respectively.

FSI business concentration risk findings may reflect the "branch channel" business model for retail and commercial banking, brokerage, and insurance industry firms. The influence of decentralized data center operations is also consistent with the influence of the U.S. Securities and Exchange Commission May 2003 Interagency Paper on *Sound Practices to Strengthen the Resilience of the U.S. Financial System* on the largest FSI firms (<http://www.sec.gov/news/studies/34-47638.htm>).

# Conclusion

The 2005 Business Continuity Survey findings reveal trends demonstrating executive concern for effective governance and regulatory compliance, which may influence priorities for a broad array of risk mitigation initiatives in the coming years. The growing influence of regulatory considerations specific to BCM were also noted, including industry based requirements imposed by NASD 3510 and HIPAA as key regulatory drivers. We also believe the influence of public risk management frameworks (e.g., Basel II, COSO) will increase management's focus on BCM governance and enhanced risk management controls, including those for BCM. One explanation for increased executive emphasis on BCM governance may be the indirect effects on public companies of the Sarbanes-Oxley Act of 2002 (SOA).

While early interpretations of Section 404 of the SOA considered business continuity and operating risk management directly, later clarifications excluded these areas. The Act requires companies to adopt an "internal controls framework." Given this SOA requirement, a possible answer is that many public companies have adopted the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework for this purpose. Many have done so because of their familiarity with the COSO framework, and because the SEC has viewed this framework in a favorable light.

The COSO framework includes a major element suggesting that management implement a process for identifying and managing risks – both internal and external. As such, COSO is not limited to internal controls for managing financial risk. Section 404 requires and the COSO framework supports control activities for managing operating risk to the extent that they address controls surrounding financial reporting. This creates a tangential requirement to address business recovery for financial reporting processes to ensure full compliance with SOA Section 404.

Outside of major metropolitan areas and certain industries, the survey suggests that the specific threat from terrorism will only be one of a broad array of threat events that will drive the business continuity planning priorities of survey respondents. We expect this broad-based perspective will continue to dominate private-sector risk management initiatives and business continuity planning priorities for the foreseeable future.

# Appendix A

## Analysis of Individual Questions

### Question 1

We first asked about the general status of Business Continuity Management. Over 80% of the respondents said that they had business continuity plans for critical business functions all the way to operational, tested plans, and an enterprise-wide BCM function involved in maintaining the availability of critical functions and resources. This compares to 75% in 2004. Within this overall response, one-seventh of all respondents had some plans in place; one out of ten had plans being developed and only 6% had no plans at all. This indicates that business continuity continues to gather support and that plan implementation continues to expand across entire enterprises – not just a few business units or departments.

### Question 2

We next asked about the presence of business process/work area recovery plans. These types of plans focus more specifically on critical business processes, such as supply chain management, with the recovery plans designed specifically for vertical business units, as opposed to horizontal business processes, which can cut across multiple business units. Almost 60% of the respondents either have plans in place to address specific business processes or have incorporated process improvement activities into their BCM programs to enhance their ability to recover. Over 20% have completed business impact assessments to identify critical business processes in advance of producing business continuity plans. Finally, only 12% (as compared to 20% in 2004) said they have merely identified the need for enterprise-level recovery, in addition to more traditional technology recovery.

### Question 3

One of the often overlooked areas of business continuity is the interdependency firms have with other organizations. All companies probably depend on one or more outside organizations for something that helps their businesses or government agencies function properly. It is critical that, during plan development efforts, all of the outside organizations a company needs to achieve its business goals be identified. More importantly, it is important to determine that those organizations have contingency plans in place that address how they remain in operation in the aftermath of a crisis situation. The level of interaction can range from knowledge of existing emergency plans to reciprocal recovery arrangements and sharing of recovery facilities. The survey showed that 35% had developed a list of key third party firms (down from 40%), and that 21% (down from 28%) had identified dependencies and third-party recovery capabilities, in addition to their lists. Sixteen percent said they had incorporated third-party recovery issues into business continuity plans, contractual agreements, and reciprocal testing and support agreements. More apparently needs to be done in this important area.

### Question 4

The most effective way to determine if business continuity, security and crisis management plans work is to exercise them. It was reported that 65% (up from 50% in 2004) were conducting regular tabletop exercises (15%), tests of critical plan components (42%), and full-scale integrated tests (8%). We noted that about one in five had identified testing goals and added them to plans, and that only one in six (as compared to one in four in 2004) were performing no tests at all. While preparations for an exercise can be rigorous and time-consuming, especially for a large-scale integrated test, tabletop exercises can be effective, especially for business units, and are not particularly difficult to organize. The key challenge is to convince management and staff – at all levels – that completing a plan is not enough. Exercising can make the difference, especially when a real disaster occurs.

### Question 5

The traditional antecedent of business continuity is disaster recovery (or technology recovery), and it involves “bringing back the box”. Disaster recovery focuses on recovering and restoring data and the systems that processed it. These typically included mainframes and storage systems, midrange systems, and, today, include servers, switches, routers, and many other related devices. Naturally, we expected a certain number of companies would still focus on recovering the “glass house” and related systems, and we found that 14% (down from 22% in 2004) of the respondents said their plans focused solely on recovering primary IT platforms. Expanding on that category, we noted that 45% (up from 38%) have plans in place for recovering mainframes, mid-range systems, LAN/WAN and client-server systems, and even some business unit testing. Less than one-fourth have fully integrated technology and business unit recovery plans. Only 18% (up from 17%) said they either have no interaction with business units (9%) or have at least completed a technology risk assessment and implemented some risk mitigation activities (9%). Almost seven out of ten organizations surveyed have some form of technology recovery plan in place.

### Question 6

Despite the critical importance of telecommunications to business and government, it may be overlooked as part of the business continuity process. Both voice and data communications need to be incorporated into business continuity programs. Without communications resilience, most organizations cannot function properly. The survey confirmed that telecommunications is still considered an important issue. Only 12% (as compared to 21% in 2004) have no plans to deal with a telecom disruption or outage. Further, almost nine out of ten address telecommunications at some level. About 30% have a nominal level of support for telecom recovery, and 40% address most telecom technologies in their plans. The key challenges continue to be identifying single points of failure, increasing network resilience through the infrastructure, deploying backup systems and network services, incorporating these elements into business continuity plans, and exercising telecom infrastructure resilience regularly.

### Question 7

Protection of vital records – regardless of format or technology – is an essential part of business continuity. Key activities are to identify the records to protect, determine their criticality to the organization, and define how to store records in a secure, protected environment that also makes it easy to retrieve critical records when they are needed. Less than 10% (down from 20% in 2004) had a vital records program in place that they consider inadequate. While 23% (up from 14%) had identified their vital records – although they did not have a program to protect them – the remaining 67% (unchanged from 2004) said they had various programs in place to protect their vital records. Among the respondents, 37% (up from 30%) were using some form of off-site storage; 18% (down from 26%) had a records retention program; and 13% (up from 10%) were actively using leading-edge technologies like electronic vaulting, journaling and data replication.

### Question 8

We next asked respondents how they protected their physical facilities (buildings and real estate) and infrastructures, e.g., HVAC, power, and security. Less than 10% of respondents (down from 12% in 2004) indicated they were aware of the need for alternate work areas, but had no plans in development. Twenty-one percent said their facilities plans were in development but utilities plans were not in place. The remaining 69% said they have existing building security and safety plans but no linkage to business requirements (23%); facilities plans were integrated with business unit plans to support recovery and were tested annually (36%); and the organization is exploring and implementing public/private cooperation (10%, an increase from 4%). What is probably most significant is the more than doubling of the recognition of the need for greater public/private cooperation, an area that is increasingly important in the face of continued terrorist threats.

### Question 9

The human side of business continuity – life safety – addresses multiple issues. These include personal safety, emergency notification following an incident, and emergency evacuation and relocation. An area of concern in this category was the fact that 17% of the respondents depend on their local fire departments to define their human safety responses. It may be preferable that organizations take a proactive approach, rather than relying exclusively on first responders. Ideally, the development and implementation of these programs should be a joint effort between private and public sector organizations. Only 21% (down from 36%) said they have fire safety plans and call trees in place, and that individual business units handle people issues. Sixteen percent (down from 23%) said they have evacuation and relocation plans developed in coordination with their facilities departments. Approximately 46% (more than twice 2004 figures) said their evacuation, communications and facilities plans are tested annually; they leverage the internet; and incorporate employee assistance and transportation programs.

### Question 10

Awareness and training programs for business continuity, security and crisis management are critical to the overall success and acceptance of these initiatives. Without knowledge of what they are supposed to do in an emergency, employees could be placed in harm's way. Each survey respondent had some level of awareness and training in place. Less than half (45%) had training programs limited to business continuity plan execution. Additional activities included joint training by business continuity department and business units (24%); business continuity training for all company employees (10%) with attendance optional; and expanded company-wide training with training modules for specific responsibilities, a department library, an intranet site, and mandatory attendance at training sessions (12%). Almost 9% have established a business continuity library and/or intranet site, and have added business continuity training to overall corporate training requirements.

### Question 11

Crisis management – the actions needed for responding to an unplanned event that threatens the organization – represents a critical part of any business continuity activity, regardless of the organization's size. About 20% of respondents said they had identified the appropriate senior management but had not assigned them formal roles or responsibilities in a crisis. Twenty-three percent said they had identified a crisis management team, an emergency response team and a command center. The next group, at 15%, said they had defined crisis management and emergency response teams, but conducted only partial program tests. Another 34% (up from 25%) said they had the teams in place and conducted annual plan tests. The remaining 7% (up from 4%) said they tested their plans and teams at least quarterly. A higher percentage of companies are completing their plans and conducting regular crisis response exercises.

**Question 12**

Considering the growing need for compliance with Sarbanes-Oxley regulations, 13% (down from 21%) responded simply that they were aware of their requirements for regulatory compliance; by contrast, 26% said their business units were aware of regulatory, compliance, legal, and industry issues affecting them. Carrying the issue of compliance to the next level, 12% said they have completed business impact assessments of the risks associated with non-compliance with regulations. Almost 40% (up from 36% in 2004) said they were fully compliant with applicable regulatory and legal issues, that executive management was involved, and there were minimal audit exceptions. The most actively involved firms – approximately 11%, up from 6% – said they were members of various regulatory boards, and actively develop and influence regulations. In summary, almost half of the respondents said they can demonstrate compliance at various levels – a 25% improvement over 2004.

**Question 13**

Successful business continuity programs result from senior management commitment coupled with a solid governance process. Top-down management support is essential. Only 8%, down from 14% in 2004, reported that their management only focuses on the issue when audits are looming. A third of the respondents said their senior management is aware of crisis plans (35%). Steering Committees are useful in securing management support; 22% said they have such committees in place. These committees were aligned with the needs of technology departments and business units. We also note that 17% said they have a comprehensive BCM governance structure in place, and another 19% said they have “active executive involvement” in program development. While the last two categories are highly desirable – and the most difficult to achieve – progress continues to be made in this key area.

**Question 14**

It is not uncommon for a specific event, such as a fire, flood, severe weather, or a major technology failure to encourage development of a business continuity program. Other than responding to these kinds of events, we asked the respondents to specify the primary reason for business continuity in their firms today. Choices included senior management accountability (21%), operating management accountability (6%), need to address operational resilience and availability (33%), regulatory compliance (19%), stakeholder protection (7%), previous business disruption (7%), public relations/corporate image (2%), responsibility to prepare for homeland security (<1%), and other (6%). An important point to make is that while senior management acceptance of business continuity and regulatory compliance are two key drivers, so is the need to strive for uninterrupted business operations.

**Question 15**

Following from Question 14, we asked where the focus would be on these same drivers over the next five years. Choices included senior management accountability (23%), operating management accountability (4%), need to address operational resilience and availability (33%), regulatory compliance (23%), stakeholder protection (8%), responsibility to prepare for homeland security (<1%), previous business disruption (4%), public relations/corporate image (3%), and other (3%). As can be seen, the areas of concern will be largely the same.

**Question 16**

We asked where business continuity typically resides within an organization. Respondents said it reports to corporate management (34%), legal (<1%), financial management (7%), human resources (<1%), risk management (14%), facilities management (5%), information technology (24%), data center (1%), information security (5%), physical security (2%), and other (7%). The results reflect the disparate location of business continuity activities in corporate organization charts.

**Question 17**

When developing business continuity plans, a key metric is to identify risk tolerance, especially for critical business functions. This is often stated in terms of a recovery time objective (RTO). Fully three-fourths of respondents said they needed their most critical activities back in business within 24 hours. About 18% said they could handle critical system outages lasting up to three days. Six percent said they could last three to five days, and 2% said they could wait five days or longer. Notably, about one in eight (12%) require zero downtime.

**Question 18**

Getting external firms to participate in the business continuity process is very important – but perhaps overlooked. The 2005 results show increasing emphasis. About 62% (compared to 69% in 2004) said there is no reciprocal participation in plan testing among suppliers and service providers. Among the remaining respondents, 21% (compared to 17% in 2004) said vendors participate in the respondents’ plan tests but it is not reciprocal, 4% (no change) said they participated in their vendors’ tests but not conversely, and finally, 13% (compared to 9%) claimed full plan test participation and reciprocity.

### Question 19

Questions 19 and 20 address the relationship between business continuity, change management and capacity planning. First, about 20% of respondents (compared to 36% in 2004) said they had no formal change management process. About 26% said there is no involvement between business continuity and change management. One-fourth (compared to 50% in 2004) said there is informal involvement between the organizations. The remaining 29% (compared to 14%) said they had varying levels of engagement between the two disciplines, ranging from including business continuity plans in the change management process to full involvement of business continuity in enterprise-level strategic change processes. Clearly the level of engagement has increased.

### Question 20

The level of interaction between business continuity and capacity planning was similar to change management. Again, about 23% (compared to 48% in 2004) said they have no formal capacity planning process. About 24% said there is no formal involvement among the disciplines. Slightly more than one-fourth (26%, compared to 40%) said there is informal consultation between business continuity and capacity planning. Of note, 26% (compared to 12% in 2004) said the two disciplines are actively engaged, ranging from tactical integration of business continuity with capacity planning to strategic integration for enterprise-wide applications.

### Question 21

About 21% of the respondents (compared with 28% in 2004) told us that they had no budget for business continuity. Half (50%, compared with 53% in 2004) said they spent upwards of \$1 million; 22% spent from \$1 million to \$10 million (compared with 16%); 6% said they spent from \$10 million to \$50 million (compared with 2%); and almost 2% (compared with <1%) spent over \$50 million.

### Question 22

Following up with Question 21, we asked respondents the approximate percentage they spent on various items in their budgets, using the ranges supplied in the previous question. Responses were calculated by dividing the total percentages supplied for each category by the number of responses. Choices were external recovery sites (21%), internal recovery sites (9%), department salaries and benefits (13%), vital records and data backup (8%), voice and data communications (6%), equipment and infrastructure (12%), software (4%), documentation (4%), consulting (3%), contingency outsourcing (2%), and other (19%). Since the categories were modified from those used in the 2004 survey, a comparison to those results cannot be made.

### Question 23

This question asked for each respondent's industry. Choices and responses included banking/investment banking (18%), brokerage (2%), other financial (11%), manufacturing/industrial (8%), transportation (1%), utilities (3%), telecommunications (4%), healthcare (4%), pharmaceutical (2%), government (US federal, state, local) (7%), military services (<1%), insurance (10%), retail/wholesale (5%), petroleum/chemical (1%), education (3%), building/property management (<1%), information/data processing services (3%), lodging/food service (<1%), event/amusement facilities (none), media/entertainment (2%), professional services (5%), computer infrastructure (hardware/software) (4%), and other (9%). As with Question 22, we modified the categories from the 2004 survey.

### Question 24

This question asked respondents to describe their primary job function. Choices and responses included executive/senior management (10%), crisis management (2%), security management (4%), business operations management (3%), Business Continuity Management (35%), disaster recovery management (11%), information technology management (11%), data center management (2%), internal audit (2%), administrative support (2%), and other (9%). As with the previous two questions, we modified the categories from 2004.

### Question 25

We asked respondents to tell us how many employees were in their companies. The number of respondents from companies with 1000 or fewer employees declined from the 2004 survey. Conversely, the number of companies with employees ranging from 1000 to over 50,000 employees increased from 2004. Only about 30% (down from 44% in 2004) worked for companies with 1,000 employees or less. Larger firms dominated the survey, with 41% (up from 32% in 2004) having 1,000 to 10,000 employees and 29% (up from 23%) having 10,000 and more staff.

### Question 26

When we asked about annual revenues, 37% (up from 34%) had revenues over \$1 billion; 30% (up from 29%) had from \$100 million to \$1 billion; 22% (up from 20%) had between \$10 million and \$100 million; and 11% (down from 17%) had less than \$10 million.

**Question 27**

Given the concerns about business concentration, e.g., centralized versus decentralized business operations, we asked the respondents to tell us how management is addressing the issue. Better than 50% were addressing the issue via some level of decentralization. Specifically, one-fourth said the issue was not being addressed at all. About 22% said management was aware of concentration risk, but chose not to decentralize business operations. About 30% said management has implemented limited business decentralization to mitigate concentration risk. Finally, about 24% said management was addressing concentration risks through significant business operations decentralization and other means.

**Question 28**

We also asked about concentration risk as it applies to data center operations. Almost 60% were addressing the issue via some level of data center decentralization. Fewer than one-fourth (23%) were not addressing the issue at all. Management initiated limited data center decentralization for 26% of the respondents. One-third of the respondents (33%) said management was addressing concentration risk via extensive data center decentralization and other means.

**Question 29**

This question asked respondents how many full-time equivalent (FTE) staff members were dedicated to business continuity. Fully 27% said they had none or less than one FTE, which means the business continuity person, had other duties besides business continuity. Thirty percent had 1-2 business continuity employees; 23% had 2-5; 6% had 5-10, and almost 14% had more than 10 business continuity professionals on staff.

**Question 30**

The next question asked respondents to tell us what kinds of products and services they were using. Progressing through the list, in order of preferences, off-site data storage (89%), server mirroring (60%), e-mail server backup/recovery capability (59%), data replication software (57%), hot site (54%), business continuity plan development software (44%), disaster kits for emergency teams (42%), second data center configured for disaster recovery (39%), preconfigured office space, ready for occupancy in a disaster (38%), emergency notification system/software for rapid message dissemination (36%), cold site (34%), data vaulting (34%), business impact analysis software (22%) and other (3%).

**Question 31**

Among its many activities, the Department of Homeland Security (DHS) issues periodic Threat Condition ratings and Advisories related to the safety and viability of the nation's infrastructure. We asked the respondents to tell us how often they use these advisories. Half the respondents (50%) do not use the DHS advisories in the course of emergency planning. Advisories only are monitored by 19% of the respondents. The remaining 31% monitor both Threat Condition ratings and Advisories and use the data – in varying degrees – as part of their emergency plans.

**Question 32**

With regard to Threat Advisories, we asked the respondents to tell us how useful the information contained in Advisories was to their organizations, specifically to help them better respond to threats. Respondents were evenly divided between those who thought the Advisories offered little value, and those who felt they were valuable. One-fourth (25%) said the Advisories had no value. Another 25% said the Advisories rarely had any real value. The remaining 50% said the Advisories sometimes (33%), often (10%) or always (7%) contained useful information.

# Appendix B

## Statistical Summary

Figure 1. Cross-Tabulation of Revenues to BCM Budget (Green Box Identifies Mode Score)

All Industries		BCM Budget Allocation							Total	Average
		No Budget	< \$500K	\$500K to \$1M	\$1M to \$5M	\$5M to \$10M	\$10M to \$50M	> \$50M		
Annual Revenue	< \$10M	33.3%	43.3%	20.0%	0.0%	3.3%	0.0%	0.0%	100.0%	\$1,741,667
	\$10M-\$50M	40.6%	31.3%	18.8%	9.4%	0.0%	0.0%	0.0%	100.0%	\$1,507,813
	\$50M-\$100M	25.9%	48.1%	18.5%	7.4%	0.0%	0.0%	0.0%	100.0%	\$1,444,444
	\$100M-\$500M	35.4%	37.5%	8.3%	16.7%	0.0%	2.1%	0.0%	100.0%	\$2,869,792
	\$500M-\$1B	8.6%	42.9%	20.0%	25.7%	2.9%	0.0%	0.0%	100.0%	\$3,485,714
	\$1B-\$5B	7.8%	29.4%	25.5%	25.5%	5.9%	5.9%	0.0%	100.0%	\$7,200,980
	> \$5B	4.0%	8.0%	16.0%	22.0%	18.0%	22.0%	10.0%	100.0%	\$17,620,000
	Percentage	20.5%	32.2%	17.9%	16.8%	5.1%	5.5%	1.8%	100.0%	\$6,034,799

### Revenue to BCM Budget Allocation

Deloitte & Touche and CPM survey results show that among organizations with at least \$50 Million in annual revenues, BCM budget allocation for Financial Services Industry (FSI) companies is at least two times that of non-FSI. For organizations with \$50 Million or less, budget allocation appears to be roughly equivalent between FSI and non-FSI firms.

Approximately 20.5% of all responding organizations have no formal budget allocation for BCM, with only 8.3% of FSI organizations reporting no budget allocation and 28.7% for all non-FSI firms. Industries exceeding this 20.5% level include Professional Services (50%), Computer Hardware/Software Manufacturers (40%), Information Processing (38%), Telecommunications (30%), Manufacturing/Industrial (28.6%), Pharmaceutical (25%), Utilities (22%), and Government (22%).

### BCM Budget Allocation to Staffing Allocation

Benchmark survey results indicate a strong correlation between BCM budget allocation and full-time equivalent (FTE) staffing dedicated to business continuity planning. We have observed that full-time staffing of business continuity functions will normally be seen in organizations whose budget threshold exceeds \$500,000 or more. However, survey data appear to show that organizations will dedicate one FTE in support of BCM program operations for every \$750,000 to \$1.5 Million in BCM budget allocation.

As noted above, some survey participants reported BCM staffing allocation despite the fact that they have no reported BCM budget. Our best interpretation of this finding is that BCM staff responsibilities have been formally assigned while BCM budget has not been formally allocated.

Figure 2. Cross-Tabulation of BCM Budget to BCM Staffing (Percentage of Respondents Reporting)

All Industries		BCM FTE Staffing Levels									Average FTEs
		None	< 1	1	1-2	2-3	3-4	4-5	5-10	> 10	
BCM Budget	No BCM Budget	35.7%	42.9%	3.6%	10.7%	1.8%	3.6%	0.0%	0.0%	1.8%	0.8
	Under \$500,000	11.4%	28.4%	21.6%	13.6%	13.6%	3.4%	4.5%	2.3%	1.1%	1.5
	\$500K to \$1 Million	2.0%	4.1%	34.7%	14.3%	16.3%	12.2%	8.2%	4.1%	4.1%	2.5
	\$1 Million to \$5 Million	2.2%	0.0%	8.7%	8.7%	10.9%	21.7%	10.9%	17.4%	19.6%	5.0
	\$5 Million to \$10 Million	0.0%	0.0%	0.0%	0.0%	0.0%	28.6%	0.0%	7.1%	64.3%	8.0
	\$10 Million to \$50 Million	0.0%	0.0%	0.0%	6.7%	6.7%	0.0%	0.0%	13.3%	73.3%	8.6
	Over \$50 Million	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	100.0%	10.0 >

Figure 3. BCM Organization Placement (2004 versus 2005)

Where Does the Business Continuity Planning Function Report in Your Organization?		Corporate Function Owning Business Continuity Planning					Total
		Executive/Senior Mgmt.	Risk Management	Information Security	IT Management	Other	
2005	All Observations	34.43%	13.55%	5.13%	23.81%	23.08%	100.00%
	FSI Only	31.19%	22.02%	3.67%	22.94%	20.18%	100.00%
	Non-FSI	36.59%	7.93%	6.10%	24.39%	24.99%	100.00%
2004	All Observations	33.33%	12.78%	5.00%	27.78%	21.11%	100.00%
	FSI Only	29.03%	16.13%	1.61%	25.81%	27.42%	100.00%
	Non-FSI	35.59%	11.02%	6.78%	28.81%	17.80%	100.00%

## Organizational Placement of the BCM Function

One measure of Executive Management's focus on Business Continuity Management is where in their organization they have placed continuity planning responsibilities. Benchmark survey results for the past two years indicate that about one-third of organizations have business continuity planning function reporting to Executive/Senior Management, with IT management still retaining this function in approximately 24% of organizations.

## Management of Concentration Risk

Deloitte & Touche and CPM sought to understand the level of concern organizations place on concentration risk, and to assess how such concern has influenced implementation of both decentralized business and data center operations for organizations of different size. We asked respondents to tell us whether concerns about concentration risk had driven their organizations to consider decentralizing either their business or data center operations. Survey responses indicate that across all organizations, regardless of revenue base, the percent of respondents indicating a significant commitment to decentralized data center operations is measurably higher than for decentralized business operations.

**Figure 4. Differences in Approach to Concentration Risk Management**

FSI Versus Non-FSI Firms		Concentration Risk Management Comparison of Business & IT Approaches to Risk Mitigation			
		Business		Data Center	
		FSI	Non-FSI	FSI	Non-FSI
Response Criteria	Not Addressed	25.7%	60.3%	22.9%	52.4%
	Awareness Only				
	Limited Decentralization				
	Significant Decentralization	74.3%	39.7%	77.1%	47.6%
	Decentralization and Other				
Total		100.0%	100.0%	100.0%	100.0%

When analyzing results by industry, we observe that Financial Services Industry (FSI) companies emphasize decentralized business operations to a higher degree than non-FSI organizations, for both business and data centers. For example, 74.3% of FSI firms reported anywhere from a limited to significant commitment to decentralized business operations, and 77.1% for data center operations. This can be compared to non-FSI who report 39.7% and 47.6% for business and data center operations respectively.

FSI business concentration risk findings may reflect the “branch channel” business model for retail and commercial banking, brokerage, and insurance industry firms. The influence of decentralized data center operations are also consistent for FSI firms that have been influenced by standards identified in the May 2003 Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.

# Contacts

Chris Lee  
Deloitte & Touche LLP  
Security & Privacy Services  
Service Line Leader  
225 West Santa Clara Street  
San Jose, CA 95113-2303  
408 704 4314  
chrislee@deloitte.com

Steve Ross  
Deloitte & Touche LLP  
Security & Privacy Services  
Business Continuity Leader  
2 World Financial Center  
New York, NY 10281-1414  
212 436 2226  
stross@deloitte.com

Eric Beck  
Deloitte & Touche LLP  
Security & Privacy Services  
Senior Manager  
2 Hilton Ct  
Parsippany, NJ 07054-0319  
973 683 6193  
erbeck@deloitte.com

For more information about our services, please  
visit our Web site: [www.deloitte.com/us/security](http://www.deloitte.com/us/security)

Deven Kichline  
Editor-in-Chief  
CPM – Global Assurance  
The CPM Group  
20 Commerce Street  
Flemington, NJ 08822  
Main: 908 788 0343 x117  
Fax: 908 788 3782  
dkichline@contingencyplanning.com

[www.ContingencyPlanning.com](http://www.ContingencyPlanning.com)

**General Disclaimer**

This publication contains general information only, and Deloitte & Touche LLP is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified advisor.

Deloitte & Touche LLP, its affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

**About CPM Group**

The CPM Group is an information resource for the business continuity/COOP, emergency management and security professions. From information assurance and homeland security to benchmarking research and corporate governance, the CPM Group offers e-newsletters, conferences, business development, list rental, web and e-publications, advertising and sponsorships, list rentals and custom products. The CPM website is a source for industry news stories and information.

Web site: [www.contingencyplanning.com](http://www.contingencyplanning.com).

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas – audit, tax, consulting and financial advisory services – and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the U.S., Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP and their subsidiaries), and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting and financial advisory services through nearly 30,000 people in more than 80 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's Web site at [www.deloitte.com/us](http://www.deloitte.com/us).