

# GUIDE TO BUSINESS CONTINUITY MANAGEMENT



## Frequently Asked Questions *Second Edition*

**protiviti**<sup>®</sup>  
Independent Risk Consulting

Business Risk

Technology Risk

Internal Audit

# Table of Contents

	Page No.
<b>Introduction</b>	<b>1</b>
<b>Lessons Learned From Hurricanes Katrina and Rita</b>	<b>1</b>
<b>Practical Answers About Pandemic Influenza or “Avian Flu”</b>	<b>5</b>
<b>The Business Continuity Basics</b>	<b>8</b>
1. What is business continuity management (BCM)?	8
2. BCM seems to include many different terms, some of which appear to be very similar. How are they similar or different?	9
3. Are homeland security and BCM the same?	9
4. Is there a best approach to business continuity planning (BCP)?	9
5. What is ITIL, specifically IT Service Continuity Management?	10
6. What is the relationship between business continuity and enterprisewide risk management?	11
<b>An Overview of the Regulatory Landscape</b>	<b>12</b>
7. Can you explain the regulatory landscape regarding BCM?	12
8. What is NFPA 1600?	14
9. There is a BCP requirement published by the SEC regarding New York Stock Exchange (NYSE) members. Are all NYSE-listed companies required to follow these BCP guidelines?	14
10. Does HIPAA include a requirement to implement BCM processes?	15
11. Does the JCAHO require BCM for hospitals?	15
12. Why is the FFIEC regulation called “the BCP Gold Standard”?	15
13. What is COBIT? Is it focused solely on information technology disaster recovery planning?	16
14. Are these the only BCM mandates one needs to consider?	16
<b>Executive Management Support and Sponsorship</b>	<b>17</b>
15. Who is the right person in the organization to own the BCM process?	17
16. How can a BCM team gain management buy-in?	18
17. How can you “sell” executive management on business continuity?	18
18. What is the value to an organization in designing and deploying BCM programs?	19
19. What are the critical elements of a business continuity policy?	20
<b>Risk Assessment and Business Impact Analysis (BIA)</b>	<b>21</b>
20. What are the most common approaches to executing a risk assessment?	21
21. What are the most common approaches to executing a BIA?	21
22. What is a recovery time objective (RTO)?	22

Table of Contents (continued)

Page No.

23. What is a recovery point objective (RPO)?.....22
24. Are questionnaires necessary when planning for business continuity? .....22
25. Are there ways around completing a formal BIA and risk assessment? .....23

Business Continuity Strategy Design 24

26. Where do recommendations for response and recovery strategies come from?.....24
27. How far apart should primary and alternate sites be? .....24
28. What are the key considerations for implementing internal (insourcing) versus third-party (outsourcing) recovery solutions? .....26
29. What is a "mobile recovery center"?.....26
30. What is an emergency operations center (EOC)? .....27
31. What are the key considerations when negotiating a third-party hot site contract? .....27
32. What are the differences among cold, warm and hot sites? .....28

Business Alignment 29

33. How do you structure an internal business continuity function/planning team? .....29

Plan Development and Strategy Implementation 30

34. Is software necessary to develop a plan? .....30
35. What is the difference between crisis management and crisis communications? .....30
36. What is a call tree?.....30
37. Is there a way to make the plan more efficient and effective? .....31

Training and Awareness 31

38. Are training and awareness the same?.....31
39. What are some successful business continuity training approaches? .....31
40. What are the available certification options? .....32
41. What are the available BCM education options? .....33

Testing and Maintenance 33

42. What are the prevailing practices regarding the storage of BCP documentation?.....33
43. How often should business continuity-related documentation be updated? .....33
44. How should the organization keep the plans current? .....34
45. How often should the business continuity strategy be tested? .....34
46. What are available test options? .....35
47. Should the organization expand testing beyond IT? .....36
48. Why does it take so long to adequately plan for an IT disaster recovery test? .....36

## Table of Contents (continued)

	Page No.
<b>Compliance Monitoring and Auditing</b>	<b>37</b>
49. Describe the connection (if any) between Sarbanes-Oxley and business continuity. ....	37
50. Is the PCAOB position on business continuity right or wrong? .....	37
51. How do organizations mature their business continuity programs? .....	38
52. How often should the business continuity program be audited? .....	38
53. What is the optimal role for internal audit in BCP? .....	38
54. Can an internal audit department – internal or outsourced – participate in BCP activities? .....	39
55. How does an organization review key vendor planning for business continuity compliance with industry best practices? .....	39
<b>Industry-Specific Questions for BCM Programs</b>	<b>40</b>
<i>Manufacturing</i> .....	40
56. Have you properly evaluated the risk of supply interruption from critical component suppliers? .....	40
57. What major systems or applications support the operations, particularly ERP and MRP? Has management designed manual backup procedures to carry out manufacturing schedules and order releases? .....	40
58. How would system outages prevent operations from accessing product configuration and inspection data? Are incoming inspection data available offline for use in receiving? .....	40
59. How do companies that rely solely on single-site manufacturing or computer-aided manufacturing operations plan for the impact of a long-term outage? .....	41
60. Can purchasing access MRP data offline to continue ordering products with key suppliers? .....	41
61. Where does my product recall procedure fit into a BCM program? .....	41
<i>Healthcare</i> .....	41
62. What should be the focus of my business continuity plan? .....	41
63. Should there be a separate plan for avian flu? .....	42
64. What type of testing should be performed and how often? .....	42
65. Who should oversee and maintain the plan? .....	43
66. Have you properly evaluated the risk of interruption in automated information availability? .....	43
67. How do healthcare organizations consider technology downtime (especially unscheduled or extended downtime) in their business continuity programs? .....	43
68. How would system outages prevent operations from continuing to deliver medical care following emergencies? .....	44
69. Does the organization rely on automated information systems to the extent that operations would cease during a long-term outage? .....	44
70. Can providers access EHR data offline to continue treating patients? .....	44

Table of Contents (continued)

	Page No.
<b>Telecommunications</b> .....	45
71. Have you properly evaluated the risk of interruption from key vendors, such as invoicing support? .....	45
72. How would system outages impact the mediation function? Are call detail records backed up offline? .....	45
73. Has management designed manual backup procedures for major systems or applications supporting the order, billing and mediation functions? If so, have they tested the plan? .....	45
74. How would management handle customer service if a call center were unavailable? Does the company have more than one call center? .....	45
75. Can billing operations access critical data offline to continue the billing function during a billing system outage? .....	45
<b>Retail</b> .....	46
76. What concerns do retailers have about point of sale (POS) transactions in the event of an extended network outage with the central office? Do the same concerns exist with debit transactions, credit transactions, returns and other chain-specific transactions? .....	46
77. What are the risks of self-distribution versus outside suppliers? What about the risk of larger, centralized distribution centers versus multiple smaller locations? If warehouses are limited to larger and less numerous sites, have retailers assessed and mitigated the environmental risks (e.g., fire, flood, etc.)? .....	46
78. Is the business insurance coverage based on geographic footprint and risk potential? Is there any business interruption insurance and is it adequate? .....	46
79. What issues are there in regards to the customer service functions? Can customers' questions and concerns be addressed shortly after a disruption? .....	46
80. How are buyers able to manually purchase products and supplies without the EDI up and running? .....	46
<b>About Protiviti Inc.</b>	<b>47</b>

---

## Introduction

Some of the most significant operational challenges in the history of Business Continuity Management (BCM) occurred in late 2004 and 2005. There were Hurricanes Katrina, Rita and Wilma along the Gulf Coast; the devastating tsunami in Asia and the terrorist bombings in London. These events, as well as other natural and man-made disasters, caused disruption and turmoil for hundreds of thousands of people, and plunged both global and local businesses into chaos and uncertainty for prolonged periods of time.

As a special feature, we begin this BCM FAQ Guide with an examination of two significant issues in the field of Business Continuity Management: the continuing difficulties caused by devastating hurricane seasons, and the potential business disruption that pandemic influenza, frequently referred to by the media as “avian flu,” could cause.

---

## Lessons Learned From Hurricanes Katrina and Rita

Hurricane Katrina was one of the most powerful hurricanes to ravage the Gulf Coast in half a century, and Hurricane Rita was the third most intense storm in the nation’s history. Business and government leaders have spent considerable time and effort chronicling the mistakes they made during these storms, but what are some key lessons that can be applied to the development of business continuity programs?

### Government Support

Clearly, the most significant lesson businesses learned is that they cannot expect the government to provide even basic services in the immediate aftermath of a large-scale disaster or crisis. With few exceptions, government entities at all levels failed miserably in rescuing and assisting residents of the Gulf Coast. Businesses did not fare any better. While few business plans explicitly state that the government will assist the organization after an event, it is an implicit assumption that underlies most business continuity planning (BCP) efforts. As businesses conduct plan reviews and exercises, they should work hard to ferret out unspoken assumptions about the availability and timeliness of government assistance, and determine whether these assumptions are realistic. Where businesses identify potential problem areas, such as local government’s inability to dispatch emergency medical response teams or law enforcement officials to business facilities, organizations need to develop contingency plans to continue operations in another location – even if it is in a highly degraded state.

### Relocation of Employees

It is just as likely that the government may be unable to provide basic services to your employees’ neighborhoods. In these cases, prudence dictates that your employees should not remain in the area. You should either plan to relocate them close to the intended recovery site or assume they will be unable to come to work in the days following a geographically widespread disaster, such as a hurricane, flood or earthquake. If employees – especially, but not exclusively, lower-wage employees – leave the area for an extended period of time, there is a strong possibility they will not return. Therefore, businesses must develop long-term strategies for replacing permanently relocated workers as part of their business resumption and IT recovery plans.

### Early Evacuation

During Hurricanes Katrina and Rita, it was not uncommon for people to spend 24 hours or more trying to leave the soon-to-be affected areas. When the government finally ordered the evacuation, traffic came to a standstill because so many people were attempting to leave at once. People fleeing Hurricanes Katrina and Rita discovered that hotel rooms and other temporary residences in the closest major cities were scarce because those who had evacuated earlier were already there. This meant many people had to travel much farther than expected to find safe shelter. For businesses, this meant that their employees were scattered over

a wider geographic area and could not easily return to work in the days and weeks following the storms. When a hurricane is imminent, businesses may want to encourage their employees to err on the side of caution and relocate early. This increases the likelihood that workers will be able to obtain hotel rooms or other accommodations that are near the business recovery site.

### **Employees' Availability**

After Katrina and Rita, many companies expected employees to return to affected areas to support the business recovery, but did not provide any incentive for them to do so. In some cases, talented employees simply moved elsewhere and sought work rather than go through a prolonged separation from their families while attempting to piece their companies back together. In general, most organizations state that their employees are their greatest asset, yet companies often do not plan to provide assistance for employees affected by a disaster. Since employees' first concern naturally will be for their families and their homes, developing and communicating an assistance plan in advance of a disaster is both compassionate and pragmatic. Companies that provide material assistance for affected employees will find that their workers are able to return to their jobs substantially earlier than if they had not received assistance.

### **Return to Primary Location**

Travel back to an affected area may not be as simple as a business continuity plan might assume it will be. After Katrina struck in late August, commercial flights to New Orleans were effectively suspended until September 13, 2005 (and were still operating at only 50 percent as late as March 29, 2006). Amtrak rail was shut down until October 9, 2005, as well. The local bus depot was closed and used as a temporary jail. Since charter aircraft will be among the resources in short supply and high demand, it makes sense for businesses to come to an agreement with one or more providers in advance of an event to improve the likelihood of availability of aircraft and pilots.

### **Supporting Infrastructure Services**

Basic services such as utilities, trash collection and publicly accessible healthcare can be interrupted for an extended period of time. If your planning scenarios assume unavailability of members of your staff, consider that these service providers – be they public or private sector – also will be operationally impacted by an event and almost certainly will face similar unavailability of their own staffs. Frequently, following regional disasters, some organizations recover their own operations only to find that the supporting infrastructure – sanitation, utilities, mass transit, telecommunication, hotels, restaurants, etc. – are not as well prepared. Determine in advance how your organization will compensate for their absence.

### **Pre-positioning of Critical Resources**

Companies in areas prone to regional disasters, such as hurricanes or earthquakes, should consider pre-positioning critical resources at an alternate location outside the area. The resources should be easily accessible prior to the incident as well as immediately following the disaster. Perishable items should be rotated routinely, while other items can be stored for much longer periods.

### **Permanent Relocation of Business**

In the weeks following a large-scale disaster, basic services can be delayed for an extended period of time and an organization's workforce can be scattered. It therefore makes sense for businesses to plan to be away from their original locations – at least for the short term, but perhaps permanently. Most organizations want to be good corporate citizens and return to rebuild a devastated area, but it makes sense to analyze the risks and costs associated with trying to reconstitute at the original site versus rebuilding somewhere outside the impacted area. Identifying a "Plan B" location not only allows you to pre-position resources, train staff at that location and facilitate an orderly relocation of affected employees, but also allows you to acquire potentially limited resources at that location before the inevitable post-disaster rush for scarce goods and services occurs.

## **Distance to Alternate Location**

There have been several surveys in recent years regarding the appropriate distance of a recovery site from the primary site. Generally these surveys have suggested 15-25 miles is a good distance because of (1) the probability that the event would not affect facilities so far away from each other and (2) the likelihood that most employees will commute roughly as far following a disaster as they do every day. However, Katrina raised the possibility that this standard distance would not be far enough to mitigate the impact. Considering that difficult hurricane seasons are predicted for the next decade or two, organizations would be wise to identify in advance alternate locations well beyond 25 miles from their primary sites, even if these alternate locations are not fully outfitted as recovery sites.

## **Dual Processing Centers**

Companies with only single facilities located in the affected areas of the Gulf Coast found them severely damaged or completely destroyed following the hurricane, and thus lost all processing capabilities. If possible, businesses should explore the strategy of implementing dual processing locations. This is especially important if the organization would have to support customers affected by the same disaster (e.g., insurance companies, pharmacies, healthcare providers, local/county government, etc.). The existence of multiple processing locations allows for load balancing of processing and continued operations of critical processes prior to, during and following natural disasters.

## **Decentralize Critical Processes**

Companies located in the Gulf region whose critical processes (e.g., information systems, call centers, distribution centers, manufacturing, etc.) were all concentrated in the region found that they had lost and had to recover everything. Companies that decentralized their processes found that while one area was affected, other critical processes remained operational and could support customers and sites affected by the disaster. Advances in technology and telecommunications allow for processes to operate efficiently in a decentralized manner. In addition, redundancy can be easily incorporated into the system to allow for multiple routes for data and information to be transmitted between locations.

## **Testing and Exercising**

Many organizations with plans to relocate people and resources have never tested them in preparation for a disaster of regional scope. Some plans fail to consider the competition for everyday resources, such as rental cars/trucks, hotel rooms, shipping providers, etc., which occurs after a massive event. Others identify in general terms the types of people, vital records and equipment they would like to relocate, but do not have a system to quickly identify, gather and transport these resources. In addition, many plans do not account for damage caused by flooding, looting or other ancillary effects of the storms. Businesses must anticipate and plan for secondary damage (e.g., flooding, fires, theft, etc.). This includes obtaining the appropriate insurance to assist with recovery.

## **Plan Maintenance**

When disaster strikes, it is not uncommon for businesses to ignore their plans. This is because plans might be overloaded with detail or be unfamiliar to the personnel intended to use them during the crisis. Companies should diligently read through and critically evaluate the information contained in their plans and ensure that the information is complete, accurate, comprehensive and actionable. Subject-matter experts (SMEs) should be involved in the plan review and maintenance activities to ask and answer relevant questions specific to each critical process. This will help ensure that the plan reflects the current state of the business and can serve as a useful guide during a disaster and its aftermath.

## **Emergency Funds**

Katrina proved that the old adage “cash is king” is still correct. In the absence of an infrastructure to process credit cards or other forms of electronic payment, cash is still the most effective way to acquire resources – especially those in short supply and high demand. Consider how you will make cash available in a secure fashion to meet the needs of your business continuity effort.

## **Site Selection**

Site selection matters. The Insurance Information Institute reported that 1997 was the first time in U.S. history that 50 percent of the population lived in areas prone to hurricanes or earthquakes. Clearly there are advantages to being in these markets, but companies should consider the geographic risk of a site before locating key resources there. Many companies that currently have concentrated resources (e.g., call centers, data centers, etc.) in areas prone to earthquakes and hurricanes are moving them out in an effort to minimize the risk to the company.

## **Communications**

During Hurricanes Katrina and Rita, organizations that did a good job of getting their message out to employees, customers, suppliers and other stakeholders saw better results than those that stumbled. Communication efforts must be streamlined before an event occurs in order for communication to be effective during and after an event. Businesses must consider alternate communication methods in recovery planning. This is especially important when people are forced to disperse as much as they did pre- and post-Katrina. Communicating with other cities is especially important. Businesses should establish a means for their employees to contact displaced supervisors and peers. Employees should also know how to contact the company once they have settled in their new locations. To prepare for disruption of local infrastructure, businesses should identify major newspapers and other media outlets in the largest cities outside the potential disaster area. Developing communication teams for internal and external audiences, rehearsing roles and responsibilities, and even measuring the time it takes to issue a press release, employee communication, shareholder notice, etc., are valuable exercises that provide a baseline for senior management to use as they make decisions following an event. Practicing the communications system also emphasizes the importance for businesses of getting reliable information quickly and not relying on hearsay or information from unreliable sources.

## **Operating for a Longer Period of Time**

It is common for companies to plan for only a 30-day outage of the primary facility. However, following Katrina and Rita, companies found that they could not return to their locations even after 30 days. Many companies were forced to evaluate permanent relocation of their processes. By pre-identifying potential locations, either within or outside the region, organizations can help expedite recovery. In addition, plans should include the assumption that travel to and from the affected areas may be impossible for an extended period of time. When identifying a long-term or permanent relocation space is not practical, write into the continuity plan a step regarding the need to triage the affected facility and make the long-term decision soon, before others can acquire it.

## **Command and Control**

It is common for companies to assign responsibility for declaring a disaster to only a few key executives. Many companies located in the Gulf Coast region followed this practice prior to Katrina. However, after dealing with the severity of a storm such as Katrina, management at many companies quickly realized that when disasters hit, employees need to have a higher level of empowerment to make decisions based upon the situation and the recovery plan framework. This allows individuals to obtain resources sooner and thus accelerate recovery of the organization. In addition, within the recovery plan framework, a command and

control organization should be documented and understood by all employees. The command and control organization should outline the chains of command, identify specific commanders and their associated backups, and indicate whether commanders can or cannot transfer command. In addition, specific roles and responsibilities for each commander should be clearly documented. The plan also should state that higher-level executives cannot usurp authority from the designated commanders. Chains of command must never break down during such events, and having documentation to refer to is essential. Education and testing are important tools in the preparation process as we approach the next hurricane season. Decision-makers should thoroughly understand their role in the recovery and be properly trained on how to access and implement the corporate recovery plans.

### **Solid Supply-Chain and Logistical Planning**

Considering that hurricane season has a defined time frame and the storms provide sufficient advance warning, there are plenty of opportunities to plan for the logistical necessities required in the potentially impacted areas. While companies may or may not be affected by the event, critical suppliers and customers in the affected region may be. Companies should identify multiple suppliers for critical resources required for their processes. These vendors should be geographically dispersed, thus reducing the risk that primary and alternate suppliers will be affected by the same disaster. In addition, if critical customers are located in affected regions, alternate delivery methods should be developed and discussed. This might include directly shipping to the final consumer or to alternate warehouse locations. Companies should work with both their suppliers and customers to preplan how to minimize logistical risks associated with a large-scale regional disaster.

### **Family Communications and Evacuation Planning**

It is important for employees to know that their families will be safe during and after a disaster, and that they can efficiently evacuate from the danger zone. Company management should encourage families living in disaster-prone areas to create and document a family recovery plan. The plans should address issues such as how family members will contact each other and specify meeting places outside the area in the event that the family members are separated. The plans should establish alternate routes for evacuation in case primary roads are closed or made impassable due to traffic. The plans should be shared with family or friends located outside the danger area so that those people know what to expect. As with business recovery plans, family plans should clearly define and document roles and responsibilities.

---

## **Practical Answers About Pandemic Influenza or “Avian Flu”**

### **What is “avian flu”?**

Current media awareness centers around an avian influenza known as H5N1. It is a disease found in and spread among migratory wild birds and birds living in close proximity, such as on poultry farms. As of June 2006, almost all human infections are confirmed to have occurred in individuals who handled infected birds or their waste. Public health officials are concerned that the H5N1 strain has many of the characteristics of an avian flu that could mutate into one that is transmitted human to human, although no one can be certain that this particular strain will ever make that transition. Beyond this strain, the larger concern centers on another strain of influenza becoming pandemic. Much has been made of the Spanish flu pandemic of 1918 since it had such devastating consequences, but it is less commonly known that there were three influenza pandemics in the 20th century, the most recent occurring in 1968-1969.

The World Health Organization (WHO) is tasked with tracking the number of human cases of H5N1 infections throughout the globe. It is significant that the number of cases doubled from 2004 to 2005 and from 2005 to 2006 (projected).

Country	2003		2004		2005		2006 (as of June 27)		Total	
	cases	deaths	cases	deaths	cases	deaths	cases	deaths	cases	deaths
Azerbaijan	0	0	0	0	0	0	8	5	8	5
Cambodia	0	0	0	0	4	4	2	2	6	6
China	1	1	0	0	8	5	12	8	21	14
Djibouti	0	0	0	0	0	0	1	0	1	0
Egypt	0	0	0	0	0	0	14	6	14	6
Indonesia	0	0	0	0	19	12	46	37	65	49
Iraq	0	0	0	0	0	0	3	2	3	2
Thailand	0	0	17	12	5	2	2	2	24	16
Turkey	0	0	0	0	0	0	12	4	12	4
Vietnam	3	3	29	20	61	19	0	0	93	42
Total	4	4	46	32	97	42	100	66	247	144

Total number of cases includes number of deaths. WHO reports only laboratory-confirmed cases.

There have been many doomsday predictions regarding H5N1, but no one at present can know the potential impact. One reason is that until the strain mutates and is actually transmitted human to human, it is not possible to develop a vaccine for it. The process of discovering that the flu has mutated, acquiring and testing samples, developing and testing a vaccine, and distributing the vaccine to the at-risk population could take anywhere from four to nine months, and it is not possible to predict how far or how fast the flu would spread in that time. There are several concerns with this strain, including a higher than 56 percent mortality rate among those infected and its ability to affect young, healthy people – unlike the mortality commonly seen in “seasonal” flu. It is not expected that anything approaching the above mentioned mortality rate would be present in a global H5N1 pandemic, since the most deadly influenza pandemic on record (1918) saw only a 2.6 percent mortality rate, but it is simply not knowable at this time.

One independent public policy think tank produced a model in which the worst-case scenario resulted in 142 million fatalities globally and a global economic impact of \$4.4 trillion. More conservative estimates expect between 2 and 7.4 million fatalities globally and between \$300-400 billion in economic impacts.

**Why do we believe an avian influenza pandemic could affect organizations?**

The closest thing we have seen to how an influenza pandemic would affect commerce is the SARS outbreak of 2003. In that case, parts of the world had significant impacts from relatively few cases, which resulted in about 800 fatalities worldwide. No fatalities were reported in the United States and 43 were reported in Canada.

In the case of SARS in Toronto, businesses did shut down. Those with employees or customers using public transit were most affected. Some employees wanted to avoid not only travel to Asia, but also incoming visitors and even raw materials and equipment arriving from Asia. Many Asian cultures saw no stigma in the wearing of masks in the workplace, but because SARS originated in Asia, in some cases there was backlash and discrimination aimed at Asians. In almost all cases, organizations were highly reactive to SARS, leading to mistakes in managing the impact, such as buying ineffective protective masks and providing untimely or incorrect information to employees. Businesses also were unable to forecast the impact of employee and customer concerns about the safety of mass transit and areas of public assembly (stadiums, shopping centers, large offices, etc.).

## What should an organization do to prepare?

Since it is uncertain that a pandemic flu will ever occur, it is difficult to argue that an organization should make wholesale changes to the way it operates. For example, if a core business strategy has been to consolidate similar operations, it would be unrealistic to recommend dispersing call center operations or other customer-facing business units simply to mitigate the impact of a pandemic flu.

The other extreme is to discount the possibility of a pandemic flu since there is no certainty that it will occur. The simple fact is that there is no certainty that any business continuity risks will actually materialize. However, this does not mean that businesses should not take reasonable proactive measures. For example:

- Evaluate the overall risk of pandemic influenza to your organization. If leadership is incapacitated or lost, will the organization continue to thrive? Is the workforce more or less likely to be affected by the impact of an avian influenza? Dependence on mass transit, international travel, frequent presence in areas of public assembly and contact with strangers will all increase the exposure and impact.
- Consider the possibility that employees will not come to work during a pandemic and the impact if this occurs. Employees who use public transit to commute and/or are coming to a workplace with a high concentration of people likely will be most concerned about exposure to others who are ill. It would be naïve to believe that parents will choose work over caring for their sick children; therefore, what accommodations can and should be made? Consider how these people could be utilized while working from home, if at all. For example, are the necessary technological and workflow tools and vital records present in their homes so that they could continue working for several weeks during an outbreak?
- Work with your Human Resources management team to determine how the absenteeism policy might be altered in the event of a pandemic. Employees may not come to work for many reasons – illness, fear, childcare issues or the need to care for a loved one. All things considered, it would not be unreasonable to assume that 20 to 30 percent of the workforce could be absent for one week or more. It also is important to determine what incentive, if any, will be provided to those who do come to work. If there is no penalty for being absent and no additional reward for coming to work, employees might choose to stay home, and avoid the risk of coming to work and being exposed to the influenza.
- Decide how your business continuity response would change if multiple facilities were concurrently affected. Many business continuity programs are built around the risk of a catastrophic event affecting one operation at a time. Documented or not, the assumption is that the resources of the rest of the enterprise will be available to assist one impacted location. This is a realistic assumption for normal business continuity exposures, but unrealistic for a pandemic flu.
- Evaluate the impact on demand for your product or service in the event of a pandemic flu. Many consumer businesses will see demand fall dramatically, but others could see an actual increase. Consider not only the customer interaction as it occurs now, but the channels customers will likely use during a pandemic (Internet, call centers, etc.).
- Contact your key business partners and vendors to determine their level of attention to this matter. If defined service level agreements are in place, determine whether the preparations the business partner has taken will realistically allow them to meet the agreement. If not, and you cannot convince them to enhance their preparation, outline contingency plans for their failure during a pandemic flu. If they are a critical vendor, develop a more comprehensive contingency plan.
- Consider how you would curtail or suspend international travel during a pandemic, especially to affected regions. Since employees may choose not to get on mass transit at all, consider the impact of a suspension of all business travel for an extended period (several weeks to several months or more).
- If your business has a retail arm, determine the cost and benefit of voluntary closure. If you determine that customers and employees are unlikely to come to the location, it may be better to voluntarily close to safeguard the assets there.

- Evaluate the impact of international logistical operations. In the event of a pandemic, it is likely governments will close or severely restrict borders.
- Most importantly, communicate with your employees now about the steps you have taken to prepare for a pandemic flu. It is unrealistic to believe that employees, having never heard of your preparations before a pandemic, will be able to listen attentively when one occurs.

Build a disease pandemic component into your BCM program, both at the executive crisis management planning level and the tactical business resumption level. As you develop this component, you may want to consider the following issues:

- Crisis management programs are designed to help executives manage the uncertainty surrounding catastrophic events. Since there are so many variables outside the control of any one company in a pandemic – government quarantines, interruption of interstate commerce, commandeering of the public health infrastructure, etc. – it is especially important that an organization’s crisis management program has a system to quickly gather and interpret information to prevent confusion and chaos.
- BCM involves doing things to mitigate the impact of a crisis – not developing risk-specific plans. The difficult aspect of a pandemic influenza is the unique set of circumstances that it could involve. Organizations that find the balance between leveraging existing planning and addressing a pandemic as a stand-alone event will find it easier to develop an appropriate plan.
- Consider how we recommend that companies address hurricane planning in the Southeast: Create a specific set of action steps leading up to the hurricane, but use a foundational BCM program from the moment of impact on to address business recovery. While this is not a perfect parallel, it might be the closest peer scenario we have to use as a frame of reference.
- The use of the Business Pandemic Influenza Planning Checklist ([www.pandemicflu.gov/plan/checklists.html](http://www.pandemicflu.gov/plan/checklists.html)) can be an effective way for organizations to determine any gaps in existing business continuity planning that should be augmented by a specific pandemic plan. While the Checklist does not provide many answers on how to implement its recommendations, it is an excellent outline that businesses can use to drive program enhancements and verify organizational preparedness.

---

## The Business Continuity Basics

### 1. What is business continuity management (BCM)?

BCM is the development of strategies, plans and actions that provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise.

BCM consists of three core elements:

1. Crisis Management is a process designed to enable an effective response to an event. Crisis management processes focus on stabilizing the situation and preparing the business for recovery operations.
2. Business Resumption Planning, or Business Recovery Planning, involves the recovery of critical business functions and processes that relate to or support the delivery of core products or services to a customer.
3. IT Disaster Recovery addresses the recovery of critical IT assets, including systems, applications, databases, storage and network assets.

## 2. BCM seems to include many different terms, some of which appear to be very similar. How are they similar or different?

One of the more confusing aspects of business continuity is the terminology. A number of terms are similar to BCM, but with slightly different meanings.

Examples include:

- Disaster Recovery, which is a term reserved for the recovery and resumption of critical technology assets in case of a disaster. Disaster recovery can include tasks such as resuming individual systems (e.g., Wide Area Network or an ERP application), or recovering all critical aspects of the IT environment.
- Resumption Planning is reserved for the recovery of critical business functions that are separate from IT. Examples of resumption planning include resuming call center functions, manufacturing processes or payroll.
- Contingency Planning refers to tactical solutions addressing a core resource or process. As opposed to BCM, contingency planning is typically an isolated action and does not resemble a program or a series of related actions. An example of contingency planning is determining how to handle the loss of a specific vendor, or creating processes to work around the loss of a key piece of equipment on an assembly line.
- Recovery Planning is most closely related to BCM. These two terms can be used interchangeably.
- Emergency Response includes the immediate actions taken to preserve lives and safeguard property and assets. Emergency response is often a subset of a broader crisis management program. An example of an emergency response action is an evacuation plan.

## 3. Are homeland security and BCM the same?

The Department of Homeland Security (DHS) has always been candid about the need for both businesses and public entities to develop plans to address interruptions. Federal agencies have been directed to develop continuity of operations programs since 1994, and business continuity requirements date back to the 1960s. DHS has supported all these efforts, emphasizing the need to build public/private partnerships for BCM along the way.

Recently, the DHS introduced Ready Business, an initiative to encourage improved preparedness in the private sector. According to the DHS, “an investment in planning today will not only help protect your business investment and your livelihood, but will also support your employees, customers and stakeholders, the community, the local economy and even the country.” Information at [www.ready.gov/business](http://www.ready.gov/business) includes downloadable posters and training aids, as well as templates that small businesses can use to help develop BCM programs.

DHS has endorsed NFPA 1600 (from the National Fire Protection Association) as the standard for preparedness efforts for individual organizations. NFPA 1600 is addressed further in Question 8.

## 4. Is there a best approach to business continuity planning (BCP)?

Although a vague question, it is commonly asked and is actually quite valid. A company’s business continuity approach and project scope may vary widely, and are driven exclusively by business requirements (and constraints). However, a number of common project characteristics remain (although the process to meet these project objectives vary):

- Business Continuity Program Design and Deployment – including definition of policies, standards and tools to support business continuity efforts. In addition, an effective BCM program should include assigning accountability and responsibility for each key area (e.g., crisis management, business resumption and IT disaster recovery).

- Business Impact Analysis – establishing recovery objectives (business and technology), as well as the associated justification for each.
- Risk Assessment – identifying and prioritizing threats and failure scenarios to which the organization may be vulnerable.
- Strategy Design and Implementation – identifying and implementing continuity strategies that best meet the organization's needs, based on a cost-benefit analysis.
- Plan Documentation – documenting response, recovery and restoration procedures to enable effective business continuity operations.
- Testing – validating and continuously improving business continuity strategies and plans.
- Training and Awareness – increasing knowledge regarding business continuity operations, both in terms of response/recovery team members, as well as employees in general.
- Compliance Monitoring and Audit – establishing compliance with internal and third-party business continuity standards.

## 5. What is ITIL, specifically IT Service Continuity Management?

The IT Infrastructure Library, or ITIL®, is used to aid the implementation of a framework to manage IT services, one of which is IT Service Management (ITSM). This framework defines how Service Management is applied within specific organizations. As a framework, it is completely customizable for use within any type of business that has a heavy reliance on IT infrastructure. Although the British government created ITIL, it has rapidly been adopted across the world as the standard for best practices in the provision of IT service.

The ITIL ([www.itil-itsm-world.com/what.htm](http://www.itil-itsm-world.com/what.htm)) consists of seven sets: Service Support; Service Delivery; Planning to Implement Service Management; ICT Infrastructure Management; Applications Management; Security Management; and The Business Perspective.

The main focus of ITSM is generally divided into two main areas – Service Support and Service Delivery. Together, these two main areas comprise the disciplines that embrace provision and management of effective IT services.

Continuity management principles are addressed in the Service Delivery category. In addition to continuity management, the following four principles also are addressed:

1. Service Level Management
2. Capacity Management
3. Availability Management
4. IT Financial Management

From an ITIL perspective, continuity management is the process by which plans are put in place and managed to ensure that IT Services can recover and continue should a serious incident occur. Not just focused on reactive measures, ITIL addresses proactive measures as well, with the objective of reducing the risk of a disaster.

ITIL's Continuity Management is regarded as the recovery of the IT infrastructure used to deliver IT Services, but many businesses rely on this framework to assist with the design and implementation of the more all-encompassing process of BCP, ensuring the end-to-end business environment can continue should a serious incident occur.

Continuity management involves the following basic steps:

- Prioritizing core business processes and IT applications that must be recovered by conducting a Business Impact Analysis (BIA)
- Performing a Risk Assessment (Risk Analysis) for each core business function and IT service, to identify the assets, threats, vulnerabilities and controls in place for each service
- Evaluating the options for recovery
- Producing the continuity plan
- Testing, reviewing and revising the plan on a regular basis

#### **6. What is the relationship between business continuity and enterprisewide risk management?**

In its recently released Enterprise Risk Management (ERM) Integrated Framework, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM as:

*A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

The definition reflects certain fundamental concepts. ERM is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy-setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity, and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared toward achievement of objectives in one or more separate but overlapping categories

BCM is one component of an effective enterprise program designed to manage risk and is therefore emerging as one of many pillars within ERM.

# An Overview of the Regulatory Landscape

## 7. Can you explain the regulatory landscape regarding BCM?

Since 2001, nearly every BCM regulatory requirement or standard has been enhanced or expanded to address increases in the threat environment, as well as a focus on corporate governance. The following chart outlines the more common regulations and standards, along with specific requirements associated with each.

Business Continuity Program Component/Task	NFA 1600 National Fire Protection Association	NYSE 446, NASD 3510 Requirements for Securities Broker/Dealers	COBIT Control Objectives for Information and Related Technologies	JCAHO Joint Commission on Accreditation of Healthcare Organizations	FFIEC Federal Financial Institutions Examination Council	HIPAA Health Insurance Portability & Accountability Act
<b>Process Management</b>						
Institute a BCM process that includes crisis management, business resumption planning and IT recovery	●	●			●	
Establish a BCM steering committee that includes a coordinator and others who have both operations and technology expertise	●				●	
Define BCM objectives	●	●		●	●	
Document a BCM mission statement	●					
Schedule and document BCM testing and maintenance events				●	●	●
<b>Conduct a Risk Assessment</b>						
Identify key legislation, insurance, regulations and industry codes of practice	●		●		●	●
Define a formal risk assessment process with the objective of identifying the source, likelihood and vulnerability of specific threats that may affect operations	●	●		●	●	●
Assess current mitigating controls	●	●		●	●	●
<b>Conduct a Business Impact Analysis</b>						
Identify key business processes and critical dependencies; the impacts of potential business interruptions should be identified and continually updated	●	●		●	●	●
Identify process-specific Recovery Time Objectives (RTO)	●	●	●		●	●
Identify minimum capacity requirements to restore business operations to an acceptable level	●	●	●		●	●
Prioritize recovery efforts based on established RTOs	●	●	●			
Review Service Level Agreements between the organization and its external partners	●	●	●	●	●	●
Identify and catalog critical resources, records, facilities, equipment, vital records, critical data and infrastructure	●	●	●	●	●	●

<b>Business Continuity Program Component/Task</b>	<b>NFPA 1600</b> National Fire Protection Association	<b>NYSE 446, NASD 3510</b> Requirements for Securities Broker/Dealers	<b>COBIT</b> Control Objectives for Information and Related Technologies	<b>JCAHO</b> Joint Commission on Accreditation of Healthcare Organizations	<b>FFIEC</b> Federal Financial Institutions Examination Council	<b>HIPAA</b> Health Insurance Portability & Accountability Act
<b>Define Recovery Strategies</b>						
Establish a procedure for contracting with vendors in order to acquire critical resources in the event of a disaster	●	●	●	●	●	●
Identify and document contact information and procedures for local authorities	●	●	●	●	●	
Identify alternate recovery site(s) for all critical business processes	●	●	●	●	●	●
Conduct a cost-benefit analysis to determine the location and costs associated with recovery site alternatives and the distance from the primary site	●		●		●	
<b>Define BCM Procedures</b>						
Create standard methods for documenting response, recovery and restoration procedures, communication plans, etc.	●	●	●	●	●	
Develop and document procedures for relocating and recovering critical business processes based on management-approved recovery time objectives	●	●	●		●	●
Document emergency response and business/IT process recovery procedures that are team-based, checklist-oriented and chronological	●	●	●	●		
Define the names of emergency response and recovery team members, together with their contact information	●	●	●	●	●	
Create response, recovery and restoration activities that take into account personnel safety, and physical and IT security	●	●	●		●	●
Document crisis communications procedures	●	●	●			
Identify a crisis communications coordinator	●	●				
Develop and document training plans; training should occur on a regular, defined basis	●		●		●	●
Assign, document and communicate roles and responsibilities for BCP testing; tests should involve all critical business units, departments and functions	●		●	●	●	●
Utilize numerous types of testing approaches (tabletop drills, disaster simulations and full plan tests)	●		●		●	
Implement a post-test analysis report and review process	●		●	●	●	
Define and document specific timelines for updating the business continuity plan	●	●	●		●	
Store the BCP both online and off-site	●		●		●	
Audit the BCM process on a periodic basis to ensure compliance with company standards	●	●	●		●	●

## 8. What is NFPA 1600?

NFPA is the National Fire Protection Association, a standards-making body headquartered in Massachusetts. Their most popular work is NFPA 101, the Life Safety Code that governs most life safety issues in commercial buildings across the country. It is common for local and state governments to adopt NFPA standards verbatim into their building and life safety codes.

NFPA 1600 is the standard on disaster management and business continuity. Work on the standard began in the 1990s, with the first version published in 2000 and an updated version published in 2004. Unlike many standards and regulatory requirements, NFPA is industry neutral, and even applies to the public sector's ability to prepare for, respond to and recover from disasters (commonly known as Continuity of Operations Planning, or COOP). This standard is only three pages long and includes elements of prevention, preparedness, response and recovery.

NFPA is not nearly as far-reaching as other standards in the industry, but it serves as a reasonable first step for organizations without an up-to-date BCM program. Many industries, such as financial services and healthcare, have requirements that go far beyond NFPA 1600.

The standard became especially significant after the Federal 9/11 Commission recommended it as the National Preparedness Standard, encouraging everyone from insurance companies to credit rating agencies to include it in their evaluations of their customers. Since that time, Congressional leaders have proposed Homeland Security legislation (HR 4830) to direct the Secretary of Homeland Security to develop and implement a program to enhance private sector preparedness for emergencies and disaster preparedness. The Department of Homeland Security (DHS) initiative also is known as "Ready Business" and includes its own endorsement of NFPA 1600.

## 9. There is a BCP requirement published by the SEC regarding New York Stock Exchange (NYSE) members. Are all NYSE-listed companies required to follow these BCP guidelines?

The NYSE Rule 446 requires member companies to maintain and test business continuity plans/strategies. Member firms are the organizations that are trading securities, not those being traded. The National Association of Securities Dealers (NASD) published almost identical requirements for their membership. The SEC approved both the NYSE and NASD rules.

The NYSE/NASD requirement mandates a flexible plan that includes:

- Data backup and recovery (hard copy and electronic)
- Identification of all mission-critical systems
- Financial and operational assessments
- Alternate communications between the member and its customers
- Alternate communications between the member and its employees
- Alternate physical location of employees
- Critical business constituent, bank and counter-party impact
- Regulatory reporting
- Communications with regulators
- How the member will assure customers' prompt access to their funds and securities in the event that the member determines it is unable to continue its business

According to the NASD and NYSE, each member's plan must address the above-listed categories to the extent applicable and necessary. At the same time, the categories are not exhaustive; members should address other key areas for their business continuity strategies to be considered complete and thorough. Additionally, members are required to assign a member of senior management to review and approve the plan each year.

#### **10. Does HIPAA include a requirement to implement BCM processes?**

Several aspects of BCM are included in the security section of the HIPAA requirements. Specifically, HIPAA (Section 164.308) calls for:

- Data backup plan (required)
- Disaster recovery plans (DRPs) (required)
- Emergency mode operation plan (required)
- Testing and revision processes (addressable)
- Applications and data criticality analysis (addressable)

As noted above, the business continuity-related provisions of HIPAA are marked as required or addressable. In terms of HIPAA, addressable means that if, after the healthcare organization's due diligence is complete and they can prove the provision is unnecessary, they do not have to comply.

Additionally, section 164.310 requires contingency plans for facility access and security. Section 164.312 requires procedures to gain access to protected health information during an emergency.

The contingency plan requirements were a major focus area during the public comment period. The Department of Health and Human Services did not agree that the requirement was overly burdensome or costly and emphasized that this requirement must be met on time (for most organizations, April 2005).

These HIPAA requirements generally expand on most healthcare organizations' BCM requirements as mandated under the Joint Commission on Accreditation of Healthcare Organizations (JCAHO). A common misconception is that the HIPAA requirements are exclusively focused on information technology. Although most of HIPAA is IT focused, Protected Health Information (PHI) is found in many forms, and the Emergency Mode Operation plan is not an IT issue at all. Rather, this requirement addresses how the provider will continue to protect PHI if normal IT controls are gone, which could be considered the most difficult provision in the regulation.

#### **11. Does the JCAHO require BCM for hospitals?**

EC.1.4 clearly states the healthcare organization (provider) must develop an emergency management plan that addresses mitigation, preparedness, response and recovery. The requirement includes a hazard vulnerability analysis (risk assessment), development and training of teams with a variety of roles, plan escalation protocols, business resumption procedures, and annual maintenance and testing.

BCM is especially important for healthcare organizations because they could be in a situation where their normal operations are compromised concurrently with an increase in the community's demand for their services.

#### **12. Why is the FFIEC regulation called "the BCP Gold Standard"?**

The Federal Financial Institutions Examination Council (FFIEC) standard is the most aggressive standard in the U.S. marketplace. The FFIEC has greater governance, risk assessment, business impact analysis, planning, testing and maintenance requirements than any other standard. It contains an entire section on senior management's business continuity responsibility, which is a helpful reference for any company in any industry.

The standard also is an excellent example of the increasing expectations surrounding BCM. The standard was significantly expanded in 2003 from the 1996 version. Although still listed in the category of IT Examination, the standard itself states, “BCP is more than recovery of the technology, but rather a recovery of all critical business operations.”

The FFIEC’s own summary is an excellent resource for developing the scope of a business continuity program:

- BCP should be conducted on an enterprisewide basis.
- Thorough business impact analyses and risk assessments are the foundation of an effective BCM program.
- BCP is more than the recovery of the technology; it is the recovery of the business.
- The effectiveness of a business continuity plan can only be validated through thorough testing.
- The business continuity strategy/plan and test results should be subjected to an independent audit.
- A business continuity plan should be periodically updated to reflect and respond to changes in the institution.

Interestingly, the FFIEC is not a series of “dos and don’ts,” but rather a call for companies to make robust assessments of their needs and make reasonable judgments on the composition and content of their BCM programs. For example, following their discussion of institutions serving critical financial markets, the FFIEC states: “*Smaller, less complex institutions generally do not need the same level of planning, but are expected to fulfill their responsibility by developing an appropriate BCP and periodically conducting adequate tests.*”

### **13. What is COBIT? Is it focused solely on information technology disaster recovery planning?**

Control Objectives for Information and Related Technologies (COBIT) has been developed as a generally applicable and accepted standard for sound IT security and control practices. The standard provides a reference framework for management, users, and IS audit, control and security practitioners. COBIT, issued by the IT Governance Institute and now in its third edition, provides tools to assess and measure the enterprise’s IT capability for the 34 COBIT IT processes. COBIT’s importance has increased as a result of Sarbanes-Oxley Section 404, given its framework is useful for internal controls documentation and assessment.

Although the COBIT definition implies a sole focus on IT, the standard is written in such a way as to apply to crisis management, business resumption planning and information technology disaster recovery. Because of the relationship between Sarbanes-Oxley Section 404 and COBIT, more practitioners are exposed to this standard than ever before (although BCM is specifically excluded from Section 404 compliance).

### **14. Are these the only BCM mandates one needs to consider?**

There are many more BCM requirements that apply to most companies. OSHA regulations place some crisis management requirements on the majority of U.S. employers. Customer mandates, such as ISO/TS 16949 in the automotive industry, require contingency planning.

The Federal Reserve Board, Office of the Comptroller of Currency and the SEC worked together to design and publish the Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, which outlines additional expectations for BCM in the context of a regional event.

The GAO issued a 111-page report on how the private sector needs to prepare for potential terrorist attacks.

Clearly, the expectations on both public and private sector organizations for improved preparedness are higher than ever before. Some of the additional government and industry requirements for business continuity and crisis management include:

- Prudential Standard
- Gramm-Leach-Bliley Act
- State EHS regulations
- FDA recall and safety requirements
- Foreign Corrupt Practices Act
- Critical Infrastructure Protection
- ESEA Title IV
- FEMA
- National Contingency Plan
- FERC
- OSHA
- State insurance departments
- ISO 17799
- Local high-rise emergency plan requirements
- USA PATRIOT Act
- Food industry guidelines
- Turnbull Commission
- Federal preparedness circulars
- Australian/New Zealand 4360:1999

*Note: The table associated with this question was originally printed in the Information Systems Control Journal (Volume 3). Business continuity program tasks/components were compiled based on DRI International and BCI professional practices, and Protiviti personnel experiences.*

---

## Executive Management Support and Sponsorship

### 15. Who is the right person in the organization to own the BCM process?

Organizations typically provide leadership to the business continuity program through three roles:

1. Sponsorship – providing or ensuring organizational and financial support
2. Ownership – direct responsibility for ensuring support, as well as overall program execution
3. Custodianship – responsibility for the coordination of BCM tasks that are executed throughout the organization

The sponsorship and business continuity program ownership roles continue to trend toward organizational elements with visibility of the entire business, as well as experience with risk management. Based on these trends, Protiviti has developed a list of sponsors and owners in an order of decreasing effectiveness:

- Finance – The CFO or a direct report, to include risk management or loss prevention
- Executive Council – A member of the senior management team, to include the general counsel, director of human resources or manager of corporate communications
- Operations – The COO or a direct report, to include security and Environmental, Health and Safety (EHS)
- Information Technology – The CIO or a direct report in data center operations (some organizations have a program/project management office, where BCM may reside)
- Internal Audit – The director of internal audit enforces the company’s business continuity policies through decentralized execution or dedicated internal audit resources

#### **16. How can a BCM team gain management buy-in?**

Most organizations that have successfully obtained management buy-in have done so using one of the following five methods:

1. Internal Policy – An internal business continuity policy, reflecting the risk appetite of the organization, is useful in driving responsibility and accountability for BCM, as well as the scope of the planning effort.
2. Monitor the Regulatory Landscape – Regulatory requirements remain the primary driver for business continuity. A number of regulatory requirements mandate senior management participation in the planning process.
3. Lessons Learned From Other Companies – Business continuity actions taken by other companies (of a like size or in the same industry) often drive action or increase maturity in others. This is particularly the case if an organization successfully recovered from a perceived catastrophic failure (although the opposite is also true).
4. Publicize Successes and the Corresponding Value – Business continuity programs can act as a competitive differentiator (internally and externally) and a source of positive public relations. Customers can feel confident in the organization’s ability to respond effectively to a wide variety of crises, and employees can be assured they work for a company that cares about their well-being.
5. Insurance Return on Investment – In certain circumstances, a tested, up-to-date business continuity program can have an effect on business interruption insurance premiums.

#### **17. How can you “sell” executive management on business continuity?**

In the absence of regulatory requirements, audit findings or specific customer demands, the best method to sell management on the need for a business continuity program is using the results from a risk assessment and Business Impact Analysis (BIA).

The risk assessment is the process of identifying the (continuity-related) risks to an organization through a review of the business environment, an evaluation of the probabilities of certain events and a review of risk mitigation controls (design and operation).

The BIA is the careful study of an organization’s individual business processes and support functions, as well as the system of business processes in its entirety, to better understand objectives regarding continuity of operations. The key tasks that make up a BIA include:

- Estimating the financial impact of downtime by calculating the quantifiable loss potential
- Measuring the less tangible impacts of downtime

- Identifying process interdependencies
- Estimating the impact of a business interruption on stakeholder perception, and process timing
- Defining recovery time objectives for business processes and applications, as well as application-specific recovery point objectives
- Establishing a level of capability at the recovery time objective

The conclusions drawn by the risk assessment and BIA, together with the corresponding recommendations, are bolstered through industry benchmarking data (regarding program scope, recovery objectives, spending and strategies). The organization's insurance carrier also may be able to provide information regarding business interruption premium savings offered by a tested business continuity program, as well as insight regarding Director and Officer (D&O) Liability insurance.

The last component of the executive management "sales" message is the cost-benefit analysis. The cost is the funding and resources necessary to add resiliency and recoverability to the existing business and technology environment, whereas the benefit is "impact avoidance."

The process described above is often executed as a special project, although an emerging trend is to execute the risk assessment/BIA as an internal audit sponsored project. The Institute of Internal Auditors, or The IIA, has issued Practice Advisory 2110-2 stating that internal auditors can play a direct role in the organization's planning, to include the risk assessment, without compromising independence.

#### 18. What is the value to an organization in designing and deploying BCM programs?

In 2002, *Contingency Planning & Management*, an industry periodical, conducted a study to determine why organizations invest in BCP. Stakeholder protection, past experiences, regulatory concerns and corporate image made up the majority of reasons given.

Organizations design and deploy business continuity solutions to manage:

- Regulatory risk
- Financial risk
- Reputation risk

**Regulatory risk** is a major driver of BCM. A growing number of corporations are held accountable by regulatory bodies to maintain tested business continuity plans. Organizations that do not employ business continuity plans could be fined, and in some cases, prohibited from operating or delivering products or services.

The next risk category that drives business continuity programs is **financial risk**. Companies choose to mitigate financial risk by focusing on factors that minimize financial loss and maintain market share, including:

- Responding to customer demands
- Understanding officer liability
- Minimizing single points of failure and critical external dependencies

In terms of customer demand, a company may hold its suppliers accountable to maintain business continuity plans and protect its supply chain. In the case of a supply-chain risk management, a company might use contract provisions to hold a supplier accountable for the delivery of products or services. This can happen in lieu of "force majeure" clauses, which declare the company exempt from the terms and conditions of the contract in the case of an event beyond the reasonable control of the company.

If the company's directors and officers can be held liable for a company's response to a business interruption, they are more likely to develop and enforce business continuity planning. Companies want to minimize the existence of single points of failure and critical external dependencies. For example, a company can face huge costs if it utilizes only one supplier and that supplier is suddenly unable to provide core products or services. A company may implement BCM solutions to make sure operations can be resumed quickly in this case.

**Reputation risk** is the third main risk category that influences business continuity decision making. The drivers that relate to reputation risk include:

- Protecting the company's brand in the face of growing competition
- Maintaining the public's approval for the way the company handles a crisis

### 19. What are the critical elements of a business continuity policy?

A growing number of organizations rely on a formal, documented business continuity policy to drive the business continuity program. Although the content and the format of business continuity policies differ based on existing standards and the culture of the organization, we recommend nine key elements in order to drive this process toward an optimal level of maturity and preparedness:

- **Accountability** – Names the executive or executives accountable for the BCM program planning and execution, to include responsibility for resourcing and strategy decision making.
- **Roles and Responsibilities** – In addition to the executive sponsor, the policy establishes roles and responsibilities for all employees regarding planning, as well as activities before, during and after the disaster.
- **Analysis** – Establishes the need for and standards associated with risk assessments and business impact analyses (the cornerstones of the planning effort).
- **Legal, Regulatory and Contractual Assessment** – Requires the participation of the organization's general counsel in the analysis of federal, state and local regulations, as well as customer contractual requirements impacting business continuity strategies.
- **Business Continuity Execution** – Identifies specific actions necessary to develop optimal business continuity strategies that meet business requirements, as well as how the organization intends to manage crises and business interruptions.
- **Business Continuity Strategy and Plan Maintenance** – Specifies the standards regarding the review and maintenance of business continuity analysis, strategies and documentation.
- **Testing (Exercising)** – Defines test types, frequency of testing activities and standards associated with planning for testing (setting objectives, success criteria, etc.).
- **Training and Awareness** – Sets specific standards regarding the training of personnel named in the response and recovery plans, as well as general awareness for employees affected by the business continuity strategies.
- **Internal Audit Participation** – Requires the participation of internal audit in the planning process and/or the review of compliance with the requirements set forth in the BCM policy.

Taken together, the above-mentioned elements of a business continuity policy will assist an organization's planning team in gathering the necessary support and resources to effectively manage the BCM program.

---

## Risk Assessment and Business Impact Analysis (BIA)

### 20. What are the most common approaches to executing a risk assessment?

Most risk management disciplines utilize a risk assessment to identify and prioritize threats, risks and failure scenarios. BCM is no different. Within BCM, a wide variety of risk management processes are used; most identify and prioritize risk using a combination of likelihood (probability) and severity (impact). In addition to likelihood and severity, another characteristic that may be factored into the prioritization effort is *detectability* (will the organization have advance warning of the threat with enough time to react, or is there a control in place to prevent or mitigate this risk?). An important distinction from other risk management disciplines is that BCM-related risk assessments take into account risk mitigation controls.

Regardless of the process used to prioritize, a data-gathering process must be defined to obtain information regarding likelihood, severity and possibly detectability. Data can come from a wide variety of sources. Historical research and interviews are two of the more effective data-gathering techniques for the risk assessment.

Historical research is particularly strong for environmental and man-made threats. However, the likelihood and severity of risks often can be a “gut feel” based on experience and historical precedent. A number of online sources may be used to collect historical information regarding environmental risks. One-on-one interviews with employees and facilitated group sessions are effective in identifying actual interruptions that have impacted the organization in the past, thus enhancing the reliability of likelihood and severity estimates.

The ultimate responsibility for data validation and the acceptance of conclusions resides with senior management, typically taking the form of a BCM steering committee.

### 21. What are the most common approaches to executing a BIA?

Approaches to BIAs differ by organization. The BIA process will vary based on industry dynamics, business complexity, use of technology, frequency of change and management style. The four main elements of the BIA are scoping, data collection, conclusions and reporting.

- **Scoping** – This includes information technology and/or business functions. It may be internally focused, or it may include critical business partners, vendors and customers. The scope of the BIA drives all subsequent analytic efforts.
- **Data Collection** – Data collection is most effective when done in group-facilitated sessions and one-on-one interviews. Questionnaires and a review of management reporting also can be efficient in certain corporate cultures.
- **Conclusions** – In some organizations, quantitative finds drive the process, whereas in others, qualitative impacts are just as important. Types of impacts that should be considered include:

Work Stoppage and Idle Workforce	Environmental, Health and Safety Impairment	Customer Service
Regulatory Violations or Noncompliance	Loss of Market Share	Strained Vendor Relations
Financial Loss/Delay	Lost/Delayed Sales (Margin) or Opportunity Costs	Employee Morale/Retention
Loss of Stakeholder or Investor Confidence	Cash Flow Interruption	Negative Market Reaction
Reputation Impairment	Financial Control and Reporting Exposure	SLA/Contractual Noncompliance

- **Reporting** – Text versus graphs, reports versus presentations. Corporate culture and audience should determine the exact format to ensure findings are understood and actionable.

Regardless of the approach, the BIA is a management-owned initiative. The results must be accepted by the executive management team before the rest of the project can effectively take place.

## 22. What is a recovery time objective (RTO)?

An RTO is the period of time in which systems, applications and/or business functions must be recovered after an outage. For example, Customer Service must be recovered after one business day; therefore, Customer Service has an RTO of one day. If this time period is exceeded, the organization could sustain significant financial, regulatory, service or reputation damage.

An important consideration when identifying an RTO is that this time represents an initial, minimally acceptable capability/capacity following the business or technology interruption. A return to 100 percent capability/capacity at the RTO is very rare and costly to ensure. In reality, it is a much smaller percentage given the potential up-front and maintenance costs necessary to recover 100 percent of the normal day-to-day operational capability.

## 23. What is a recovery point objective (RPO)?

An RPO describes the data loss tolerance for a business function or application. For example, the payroll department may have an RPO of 24 hours for the PeopleSoft payroll module, meaning that in a worst-case situation, they can afford to lose and/or be forced to recreate 24 hours of data.

Let's explore a data loss scenario in practical terms. Company X uses a tape backup solution for PeopleSoft. Once a week, a full backup is performed, and each night (at approximately 2:00 a.m.), daily incremental backups are performed. At 8:00 a.m. each day, the tapes are moved off-site, where they reside for one month (at a minimum).

Let's examine three examples in order to demonstrate how to calculate data loss potential based on the process used by Company X (assuming the last backup was run on November 3 at 2:00 a.m. local time, and the tapes were taken off-site the following morning at 8:00 a.m.).

- 10:00 a.m. on November 3 – data loss potential of eight hours (10:00 a.m. minus 2:00 a.m.)
- 3:00 p.m. on November 3 – data loss potential of 13 hours (3:00 p.m. minus 2:00 a.m.)
- 6:00 a.m. on November 4 – data loss potential of 28 hours (even if a tape backup was performed at 2:00 a.m. on November 4, the tapes are still on-site; therefore, the backup media is unavailable if the data center was destroyed or unavailable. As a result, the November 3 media would have to be used.)

Assuming an RPO of 24 hours, management may or may not be willing to accept the risk of this current backup process.

## 24. Are questionnaires necessary when planning for business continuity?

No, questionnaires are not a mandatory data collection instrument during the BCP process. Although questionnaires can be useful when collecting discrete, quantifiable information, they should not be relied upon as the sole data collection method. Experience shows that when questionnaires are utilized, the information returned only provides 30 percent of the data necessary to reach conclusions regarding recovery objectives, as well as the information necessary to write the plans themselves.

If the organization elects to use a questionnaire for data-gathering purposes, we recommend the following:

- **Clarify expectations up-front** – State clearly that this is one method of data collection, and a follow-up meeting will be scheduled to discuss and expand upon responses; provide an estimate of how long the questionnaire will take to answer.

- Allow sufficient time to administer the questionnaire – The use of questionnaires can extend the length of a business continuity project given the need to allow sufficient time for the respondents to answer and return the completed document (for example, be sure a one- to two-week turnaround meets the project steering committee’s expectations).
- Beta test the questionnaire – Once the initial version of the questionnaire is written, provide it to a select number of respondents to ensure the instrument is easily understood and the responses match the intent of the questions (also check to see if the time estimate is realistic, as well). For more complex questionnaires, offer a question-and-answer session, as well as a “dry run” opportunity.
- Keep it short and simple – People dislike answering questionnaires, particularly long ones. Limit the questionnaire to 20 questions when possible, aiming for a 30- to 60-minute response time.
- Limit the questions to discrete information – Save opinion or qualitative questions for interviews and group-facilitated sessions. Ask “yes and no” questions, or questions with answers supported by discrete data.
- Follow up with one-on-one or group facilitated interviews/meetings – Again, questionnaires can only return a partial answer. Questionnaire results should be discussed to ensure the respondent truly understood the question, and additional opinion/qualitative questions should be discussed. One of the most important questions that should be discussed in a follow-up meeting is, “What should the recovery time objective be for your business function?”

## 25. Are there ways around completing a formal BIA and risk assessment?

Yes – but the end state remains the same. A number of organizations, particularly those planning for near-term events with business continuity implications, are creatively implementing processes designed to reach risk assessment and BIA conclusions without analytic processes that span many months.

In terms of working through the key elements of a risk assessment, an organization may not have the time to complete an in-depth, exhaustive analysis of all environmental, man-made, business process, supply-chain and information technology continuity risks. Additionally, the business continuity project charter may not focus on risk mitigation, but rather on true business continuity strategy design and development. With this in mind, a business continuity steering committee and/or project team may define a realistic worst-case scenario to structure the planning process. This scenario should impact the entire organization. A worst-case scenario assists in the scoping and planning effort, and provides a framework to assist planners in developing response and recovery strategies. Most organizations find that using a worst-case scenario helps them plan for less significant scenarios (all that’s needed are defined escalation procedures toward a worst-case scenario).

An example of an abbreviated BIA follows a format similar to the risk assessment. A facilitator works with a cross-functional team to define impacts (at an organizational level, as opposed to a business function or technology level), which in turn assists with the establishment of business process and technology priority levels, recovery objectives and an order of recovery. Again, this process is designed to reach preliminary conclusions in hours, as opposed to many weeks, using the input of business process owners throughout the organization.

It should be noted that Protiviti does not advise companies to permanently substitute an abbreviated analytic process for a more in-depth risk assessment and business impact analysis. However, the examples noted above provide a way to “jump start” the planning process, particularly when the organization faces a distinct deadline or management has not formally endorsed the BCM process. However, going forward, the abbreviated processes should be “refreshed” with more thorough analyses that take into account information and perspectives from multiple levels within the organization.

---

## Business Continuity Strategy Design

### 26. Where do recommendations for response and recovery strategies come from?

When recommending possible response and recovery strategy options to a business continuity steering committee, information comes from two sources. Before a strategy option can be proposed, the planning team must understand recovery objectives, order of recovery, interdependencies and assumptions. This information is developed during the BIA process. After recovery objectives and associated considerations are outlined, the actual strategy can be developed. Whether the focus is on crisis management, business resumption or information technology, strategy options are developed based on industry practices and in some cases, vendor recommendations. Industry trade shows, peer group discussion and experience will all factor into the development of a list of strategy options, as well as high-level implementation and maintenance cost estimates. When combined, the BIA and strategy design process will provide all elements of the cost-benefit analysis, which will aid in the decision-making process.

### 27. How far apart should primary and alternate sites be?

In terms of business continuity, the most common discussion centers around the distance of a primary site from an alternate location. Some practitioners believe that the primary and alternate sites should be within 20-30 miles in order to minimize employee travel, decrease communication costs, and ensure minimal recovery time for both business processes and information technology assets. Others have taken the opposite viewpoint, arguing that regional disasters have caused widespread business interruptions that have affected an organization's primary and alternate sites simultaneously. Documented examples include the ice storms in Kansas City in 2001 and Quebec in 2000, as well as the terrorist attacks in New York City. Based solely on the experience in New York, the SEC, Federal Reserve and the OCC teamed to issue new regulations focused on 9/11 lessons learned – one of which was geographic separation. Here is an excerpt from this white paper:

*The systemic effects highlighted several important vulnerabilities that may not have been widely appreciated prior to September 11. First, it was clear that business continuity planning had not fully taken into account the potential for wide-area disasters and for major loss or inaccessibility of critical staff. Contingency planning at many institutions generally focused on problems with a single building or system. Some firms arranged for their backup facilities to be in nearby buildings on the assumption that, for example, a fire might incapacitate or destroy a single facility. Very few planned for an emergency disrupting an entire business district, city or region. As a result, some firms lost access to both their primary and backup facilities in the aftermath of the September 11 events, severely disrupting their operations. Institutions also generally had not considered the possibility that transportation of personnel could be significantly disrupted and preclude the relocation of staff to alternate sites.*

Based on this experience, the white paper initially mandated a geographic separation (greater than 170 miles) for critical components of the U.S. financial system:

*In light of the September 11 experience, most now believe that the financial services industry must consider how to achieve greater geographic diversity of operations ... in order to withstand events of greater geographic scope than previously considered. Many now see the need to plan for extended periods of inaccessibility of more than one operating site within the same area. City-wide disruptions may be the minimum benchmark for planning purposes going forward, and the ability to withstand disruption of an entire metropolitan area or region also is being considered by some organizations.*

However, the final version struck the distance mandate, citing:

*The agencies do not believe it is necessary or appropriate to prescribe specific mileage requirements for geographically dispersed backup sites. It is important for firms to retain flexibility in considering various approaches to establishing backup arrangements that could be effective given a firm's particular risk profile. However, long-standing principles of business continuity planning suggest that backup arrangements should be as far away from the primary site as necessary to avoid being subject to the same set of risks as the primary location. Backup sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water*

*supply and electric power) used by the primary site. Moreover, the operation of such sites should not be impaired by a wide-scale evacuation at or the inaccessibility of staff that service the primary site. The effectiveness of backup arrangements in recovering from a wide-scale disruption should be confirmed through testing.*

For larger organizations that are wrestling with the idea of where to place alternate workspace or data centers, the following table breaks down the advantages of a nearby location compared to some of the continuity-related risks that this strategy may introduce.

Advantages*	Risks
<ul style="list-style-type: none"> <li>• Employees will incur minimal additional travel time following business interruptions; additional company travel costs will be minimal as well.</li> <li>• Employees will be better positioned to handle both family and work considerations following a disaster given minimal additional time away from home.</li> <li>• Regular, full-time employees can still work at a nearby location following the interruption.</li> <li>• Mass transportation may be affected in such a way as to prohibit employees from traveling to distant alternate sites (depends on geography and home location of employees); hence, nearby recovery locations may be preferable.</li> <li>• Communication costs associated with data replication due to short distance will be minimal.</li> <li>• Some technology and communication assets will be unable to perform in a high availability manner beyond short distances.</li> <li>• Local business suppliers may have an easier time routing their shipments to a closer location rather than one farther away.</li> </ul>	<ul style="list-style-type: none"> <li>• Temporary employees may be required at a distant location (unless operations are already dispersed).</li> <li>• Naturally occurring threats (e.g., fires, floods, high winds and ice) could affect all facilities in a given region.</li> <li>• Man-made threat scenarios could affect both primary and alternate facilities (e.g., terrorism, toxic chemical spills, etc.).</li> <li>• Quarantine or 'no-go' areas may affect both the primary and alternate facilities.</li> <li>• Mass transportation may be affected in such a way as to prohibit employees from traveling to local alternate sites (depends on geography and home location of employees).</li> <li>• Utility failure (i.e., electricity, natural gas, water and telecommunications) could affect both the primary and alternate facilities.</li> <li>• Mass illness or other health-related risks could affect a significant number of employees in a given region (bio-terrorism or naturally occurring illness).</li> <li>• Supply-chain interruptions (to include vendors supplying recovery resources) caused by regional transportation issues could affect both locations.</li> </ul>

*\* Many of these advantages may be present for geographically dispersed recovery solutions if employees are dispersed to both locations.*

What are some of the questions that should be asked before making a decision regarding the location of the alternate site? Here are some of the key discussion points:

1. Does your organization already have a potentially suitable location in a different region, with a trained staff pool, that can temporarily sustain the business following an interruption?
2. Where is your client base located (locally, regionally, nationally, internationally), and what is the criticality of the company's services during a local or regional event?
3. Does the potential (local) alternate location employ adequate risk mitigation strategies to protect against the likely effects of a regional outage (redundant telecommunications paths, backup power generators, fuel storage, alternate transportation paths, etc.), and how long can the company continue to operate in this manner?

In today's business environment, some business leaders are electing to implement co-located recovery sites, whereas others are doing the exact opposite. The most important consideration is to understand the risks involved through the execution of a comprehensive risk assessment, and electing to accept risks to which your organization may be vulnerable. If management is unwilling to accept risks that have a regional flavor, a geographically dispersed recovery strategy may be the best solution (despite the potential cost increase).

## 28. What are the key considerations for implementing internal (insourcing) versus third-party (outsourcing) recovery solutions?

When an organization determines the need to identify business continuity locations for response and recovery purposes, it should invest time and effort to clearly understand risks and requirements, and assess whether an internal or external solution is the best fit. This includes understanding business recovery requirements, service levels, and any other key metrics to ensure that the end-state continuity capabilities will effectively support the business.

The decision to insource or outsource recovery solutions is not purely an economic consideration. The ability to react and adapt to changes in the business, and the ability to ensure quality service, are the primary drivers. To determine whether it makes sense to insource or outsource, consider the following:

- Defining and measuring the solution – Successful continuity solutions are dependent on not only how well an organization defines its business recovery requirements, but also how well it can measure success.
- Financial savings – Outsourcing, in many cases, provides a cost-effective alternative to providing the services in-house.
- Sharing the risk – When you outsource your business continuity solutions, you essentially share the risk with your alternate site provider; however, control is often sacrificed.
- Delivery – Delivery is not guaranteed if an organization outsources to a third-party provider, unless management arranges for a dedicated site, which can eliminate the cost-effective element of outsourcing.
- Scalability – The end-state solution needs to be positioned to meet your organization's growth requirements, not just its current state.
- Stability – A key consideration, especially for IT, is to focus exclusively on outsourcing functions and assets deemed stable and reliable (mature, definable and measurable). Other less stable business functions or IT components, which are constantly changing, are probably not good candidates for outsourcing, since their variability drives change, and change drives increased cost and instability.
- Subject matter expertise – In some cases, a business does not have the skills to adequately staff both a primary and an alternate location, whereas a third-party may be better positioned to assist with initial recovery operations in the absence of personnel (if impacted by the event, or if they are traveling to the alternate site).

To summarize, the most important insourcing/outsourcing consideration is to ensure the solution (internal or external) is the right choice to effectively support the business. Organizations, like individuals, may be willing to pay more for the right level of support.

## 29. What is a “mobile recovery center”?

Based on lessons learned from 9/11 and the recent hurricane activity in the Southeastern portion of the United States, employee availability and travel restrictions are driving unique response and recovery strategies. One such strategy is the use of mobile recovery centers. Mobile recovery solutions provide on-site or local recovery capabilities through the use of temporary workspace trailers, preconfigured with power, environmental systems, information technology assets (to include personal computers) and voice/data communications (delivered through satellite coverage).

Most providers of mobile recovery solutions promise delivery within 24 to 72 hours. Mobile recovery solutions are flexible, and can be used as data centers, call centers and general office space. In terms of general office space, configurations ranging from 10 to 1,000 seats are available. Some organizations use mobile recovery solutions as retail space if needed to support an affected customer base (particularly when customer service is needed following a natural disaster).

Key considerations when evaluating this solution include:

- Vendor service level agreements and the size of the fleet relative to subscription base
- The availability of a location to “park” the trailer

### **30. What is an emergency operations center (EOC)?**

An EOC is the physical location where an organization comes together during an emergency to coordinate response and recovery actions and resources, and make management decisions. These centers may alternatively be called crisis command centers, situation rooms, war rooms or crisis management centers. A properly designed EOC should serve as an effective and efficient facility for coordinating emergency response efforts. An EOC may serve a number of uses including operations tracking, decision-making and training. The EOC can optimize communication and coordination through effective information management and presentation. Key success factors involve organization, design, team, affordability and practice.

### **31. What are the key considerations when negotiating a third-party hot site contract?**

Although industry trends indicate organizations are bringing recovery solutions in-house, hot site contracts remain prevalent. In order to ensure hot site contracts are cost-effective and meet business requirements, META Group (now part of Gartner) and Protiviti have developed the following considerations:

- In advance of the vendor selection process, develop and weigh selection criteria.
- Although SunGard, IBM and Hewlett-Packard remain the largest providers of hot site services, a number of specialist providers exist; therefore, dozens of qualified providers may be positioned to respond. In order to execute a focused vendor selection process, use a Request for Information (RFI) to select three finalists, and a Request for Proposal (RFP) to select a partner.
- Based on a BIA, define detailed application and network recovery objectives and associated recovery configurations. Share recovery strategy configurations with potential technology partners (following the RFI process).
- Consider a shorter hot site contract length. Business and technology change frequently, and change orders are often expensive. Shorter contracts may take advantage of the trend of decreasing technology costs.
- Consider an integrated backup communication network and site backup strategy to take advantage of economies of scale (some providers can present both solutions together).
- Ensure the hot site contract provides testing and access rights consistent with internal policies. Consider contracting for assistance with initial recovery actions where critical skills may be lacking or missing altogether.
- Contract for on-site storage of necessary resources to assist with critical recovery actions.
- Integrate data backup solutions (with an RPO of less than 24 hours and an RTO of less than 48 hours) with the hot site solution to take advantage of economies of scale.
- Include terms allowing termination of the contract in the event a similar internal capability is developed.

### 32. What are the differences among cold, warm and hot sites?

The following table defines and highlights the differences/implications associated with cold, warm and hot sites (both internal and third-party outsourced solutions).

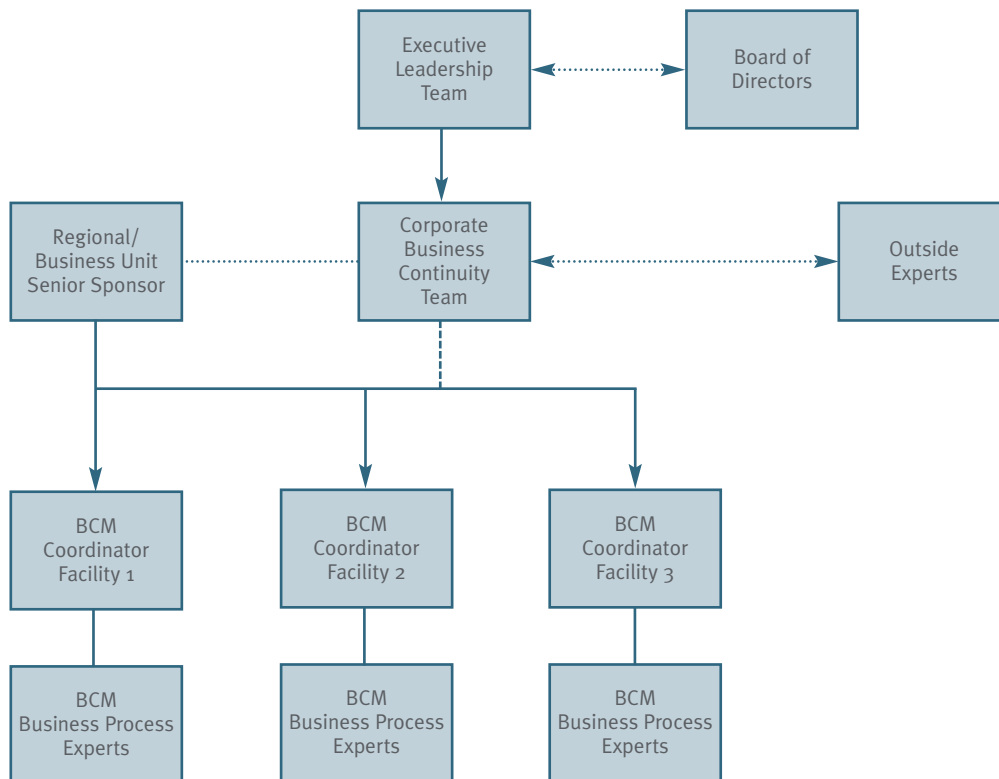
Recovery Option	Description	Pros	Cons	Data Delivery Method	Minimum Recovery Time Supported	Maximum Length Usage
<b>Internal Hot Site</b>	A facility with pre-placed server, computer, telecommunications and environmental infrastructure (all in a stand-by mode).	Guaranteed availability and unlimited testing. Always under control of the organization.	Additional data center and hardware capital expense is required. Additional complexity is introduced into the environment, which affects ongoing support and operations. Additional personnel may be needed at the alternate site.	Tape Backup	17 Hrs	Unlimited
				Disk Backup Replication	7 Hrs	Unlimited
				Data Replication	2 Hrs	Unlimited
<b>External Hot Site</b>	A third-party facility with pre-placed server, computer, telecommunications and environmental infrastructure (all in a stand-by mode).	Can be purchased as a service, no additional capital expense is required.  Multiple recovery locations provide increased protection.	No guaranteed availability.  Limited usage.	Tape Backup	24 – 72 Hrs	30 Days
				Disk Backup Replication	7 – 36 Hrs	30 Days
				Data Replication	2 – 36 Hrs	30 Days
<b>Internal Warm Site</b>	A raised floor facility with full environmental infrastructure. Limited server infrastructure and communication lines are also typically present.	Provides guaranteed space and avoids the purchase of recovery hardware.	Requires an investment in floor space, infrastructure and communications. Relies on the shipment of hardware from third parties.	All	5 – 20 Days	Unlimited
<b>Internal Cold Site with Quick Ship</b>	A raised floor facility with pre-installed environmental infrastructure, but no server infrastructure or active communication lines. Infrastructure would be provisioned using prearranged “quick” ship agreements with hardware vendors.	Provides guaranteed space and defers the purchase of recovery hardware.	Significant time required to recover; relies on third parties to provide equipment and configure communication lines. Requires effective asset management to ensure accurate recovery of applications.  The time required to install communications and infrastructure varies greatly.	All	5 – 20 Days	Unlimited
<b>External Cold Site with Quick Ship</b>	A raised floor facility with pre-installed environmental infrastructure, but no server infrastructure or active communication lines. Infrastructure would be provisioned using prearranged “quick” ship agreements with hardware vendors.	A contract can be purchased as a service; no additional capital expense is required. External cold site providers typically have nearby communication lines, which can be utilized, and have experience in performing complete recoveries.	Significant time required to recover; relies on third parties to provide equipment and configure communication infrastructure. Requires effective asset management to ensure accurate recovery of applications.	All	5 – 20 Days	Unlimited

---

## Business Alignment

### 33. How do you structure an internal business continuity function/planning team?

Most companies assign one individual with ultimate responsibility for coordinating business continuity plan development. Tactical responsibility for documenting and updating plans generally rests at the lowest level of management possible to ensure enough specificity in the plan content to fully recover the business function or process. A typical structure in a larger organization might look as follows:



In this model, both senior management and the board have an increased role and responsibility regarding BCM. Also of note, a core team overseeing the application of the corporate BCM policy across all business units and locations is in place. The responsibility for developing business continuity plans remains within the business unit and relies on the time and expertise of the business unit staff. To the degree outside experts are used, they are usually retained through the corporate identity and used to ensure consistency in plan design and execution, as well as expedite development, exercise and maintenance.

The most important issues to note when developing internal business continuity teams are that roles and responsibilities are clearly communicated and that those chosen for specific roles are trained and empowered to do what is asked. All too frequently, companies delegate responsibility for business continuity planning too low within an organization. As a consequence, plans do not express the actual needs of the organization, and when it is necessary to use the plan, significant gaps are uncovered.

---

## Plan Development and Strategy Implementation

### 34. Is software necessary to develop a plan?

No. The majority of organizations elect to develop business continuity plans using standard, Word-based templates typical of smaller- to medium-sized, single-site organizations. However, a growing number of companies, particularly larger, geographically dispersed organizations, are electing to implement software solutions to develop plans, manage content and disseminate updated plan documentation.

Although software solutions can add value, management should address three important considerations in order to make the investment pay off:

1. Recognize that software and template customization is needed before implementation and use. Purchasing software does not mean the organization is purchasing a plan.
2. Access controls should be implemented to protect sensitive information and adhere to privacy concerns.
3. “Fantasy plans” can create a false sense of security. Organizations that acquire business continuity software tools must beware of the “solution in a box” syndrome. A tool set can be a great aid, but the development of effective business resumption or IT disaster recovery plans requires people with the right skills and experience.

### 35. What is the difference between crisis management and crisis communications?

Crisis management is an organization’s overall effort to stabilize and prevent further damage after an unplanned event. Crisis management takes place at all organizational levels, beginning with executive management. Crisis management includes initial efforts from all departments, such as communications/public relations, regulatory affairs, environmental health and safety, human resources, legal, corporate security and the business units.

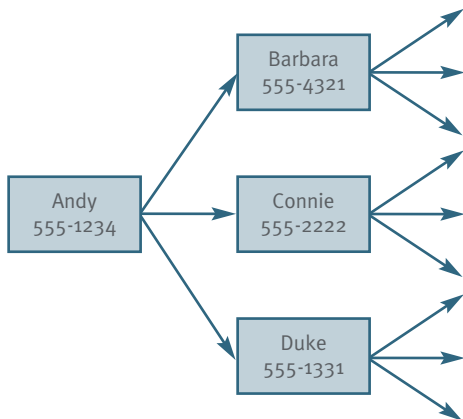
Crisis communications is only one component of crisis management. Crisis communications includes all communications before, during and after an event, including targeted communications to employees, customers, the community, regulatory agencies, shareholders, the board and those affected by the situation. Because crisis communications is involved in every type of event, from product recall to data center fire, it is critically important. The trend in crisis communications is to have multidisciplinary teams for internal and external communications working together on messaging. Public relations, sales and marketing, human resources and investor relations all work together to develop and deliver internally and externally directed messages.

Here’s an example noting how crisis management and its crisis communications subcomponent work together. After a bomb explodes in a main bank branch location, the corporate security director informs the crisis management team that threats against other sites were made, but are not deemed credible. However, the general council advises the CEO that it’s not worth taking the chance. The CEO decides to close down all facilities. The EVP of human resources decides the organization needs to pay employees regardless. The corporate controller notes the financial impact of the decision. The chief risk officer notes the regulatory implications. The crisis communications team communicates the facts to those at the scene, as well as other stakeholders (employees, customers, investors and regulatory bodies). Overall, crisis communications processes are dependent on decisions made by the crisis management team.

### 36. What is a call tree?

A call tree is a structured method to communicate with a larger group by assigning a few telephone calls to each person in a sequence. In the example below, Andy is responsible for calling Barbara, Connie and Duke. Each of those three also call three people and so on. In this way, a maximum number of people can be notified of an event in the minimum time possible. Call trees are usually built around normal organizational structures to the degree possible and include protocols on special circumstances, such as when to use home

or mobile numbers, when e-mail notification is appropriate and what to do if it is not possible to confirm contact with someone in the call tree.



In larger organizations, call trees work better in theory than they do in practice. This is usually because the large number of calls to be made interferes with the need to make rapid decisions. As a result, several software companies have developed automated call trees that can be pre-configured according to the nature and extent of an incident and follow custom scripts as the method of notification, including e-mail and paging systems. Most systems can use the receiver's touch-tone phone to confirm the notification. More elaborate systems can use a telephone notification to launch conference calls and conduct polls to make decisions, to name a few.

Call trees remain an effective tool for small groups and situations where sensitive information or decisions are involved. Call trees are also effective when timely notification is not required.

### 37. Is there a way to make the plan more efficient and effective?

Yes. We recommend the business continuity plan focus on the specific content necessary to enable effective response and recovery activities. The business continuity plan should also address the facilities and resources necessary to enable effective business continuity operations.

Consideration should be given to using checklists and flow charts to summarize response and recovery procedures, as opposed to longer narratives. Additionally, most organizations avoid scenario-specific planning; therefore, we recommend the development of plans that focus on a worst-case scenario (with the flexibility to scale back for less dramatic situations).

Lastly, we recommend using plan exercises as opportunities to “brake the plan” and identify areas for improvement. Note: Effective exercise of continuity plans requires careful planning and execution.

---

## Training and Awareness

### 38. Are training and awareness the same?

These terms are often used interchangeably but actually represent different levels of involvement as they relate to business continuity. Awareness pertains to having knowledge of or being cognizant of BCP activities. It does not necessarily require knowledge of how to execute a business continuity plan. Training pertains to the actual instruction, providing for proficiency in executing business continuity activities. This instruction may be provided through classroom, computer-based, test-based and/or instructional guides and templates. Plan testing and implementation activities are an inherent part of training. While training should involve the actual execution of business continuity testing activities necessary to evaluate the effectiveness or capabilities of the plan and/or a specific plan objective, awareness may be provided through workshops, instruction manuals, e-mail communication or other ad-hoc communication methods. Awareness is an inherent part of training; however, training is not necessarily part of awareness.

### 39. What are some successful business continuity training approaches?

The best approach to business continuity training is to review the documented roles and responsibilities to ensure what is documented meets business requirements. In many cases, especially in less mature programs, roles and responsibilities are rather boilerplate and may not fit the organizational structure or needs. After

ensuring the roles and responsibilities, as well as the assignments are correct, it is possible to perform a mini gap analysis to determine training content.

Content can be delivered in any number of ways, but the most important thing in larger organizations (i.e., those with more than one site) is that the same training is delivered everywhere. In an actual event, senior management needs to know that local decisions will be made consistently and that each person listed knows the company's preferred course of action. Various companies have used e-learning, seminars, working groups or webcasts to deliver their training.

For most organizations, some level of custom training is necessary. Not only do business continuity programs differ greatly from company to company, but the overall objectives will differ. In one company's culture, restoring operations could be seen as the most critical area of importance because it protects employees' livelihoods and the interests of customers and shareholders. In another firm, appearing sensitive to the workforce may trump production, even if it brings adverse consequences to the organization.

Many larger clients have found a matrix training system to be a very effective complement to facility-based training. In these approaches, crisis management, business resumption and IT disaster recovery personnel at each site are trained together, in addition to training augmentation with their peers across the enterprise. This approach improves standardization and dissemination of best practices without compromising the specificity required in plans covering a particular call center, manufacturing plant or other facility.

#### **40. What are the available certification options?**

Two organizations offer BCM certifications that are recognized worldwide: the Disaster Recovery Institute International, or DRI International (also known as DRII), and the Business Continuity Institute, or BCI. DRI International is active in North America and Asia, and BCI is active in Europe and Asia. Both organizations have begun to work together to continue to develop and refine worldwide professional practices.

DRII provides four certification levels:

- Associate Business Continuity Planner, or ABCP
- Certified Functional Continuity Professional, or CFCP
- Certified Business Continuity Professional, or CBCP
- Master Business Continuity Professional, or MBCP

Here is an overview of the requirements for achieving each level of DRII certification:

1. The Associate Business Continuity Planner (ABCP) certification is achieved by passing a certification exam with a score of 75 percent or better and submitting an application for certification. This application must be approved by DRI International to achieve ABCP certification.
2. The Certified Functional Continuity Professional (CFCP) certification (the newest of the four certification levels) is achieved by passing the certification exam with a score of 75 percent or better and submitting an application documenting at least two years of experience in three of the 10 categories of DRII professional practices. The application must include references, and it must be approved by the DRII Certification Commission to achieve CFCP certification.
3. The Certified Business Continuity Professional (CBCP) certification is achieved by passing the certification exam with a score of 80 percent or better and submitting an application documenting at least two years of experience in five of the 10 categories of DRII professional practices. Again, the application must include references, and it must be approved by the DRII Certification Commission to achieve CBCP certification.

4. The Master Business Continuity Professional (MBCP) certification, the fourth level, is achieved by passing the certification exam with a score of 85 percent or better, submitting an application documenting at least five years of experience in seven of the 10 categories of DRII professional practices, and passing a case study examination or conducting a pre-approved directed Masters-level Research Project. The application must include references, and it must be approved by the Certification Commission to achieve MBCP certification.

The BCI offers four market-recognized certification levels – Associate, Specialist, Member and Fellow. Each certification level is based on a combination of scored assessment and/or structured interview.

For additional information, see each organization’s website: [www.drii.org](http://www.drii.org) and [www.thebci.org](http://www.thebci.org).

#### **41. What are the available BCM education options?**

A growing number of educational opportunities are presented by business continuity-related organizations. DRI International and the BCI offer a wide variety of professional practice-oriented training covering all aspects of the planning process. The International Red Cross (and similar organizations) offers emergency response and first aid training. A significant number of public relations firms offer both crisis communications and media training. And finally, international, national and local business continuity conferences offer training on a wide variety of topics, normally presented by leading vendors and business continuity practitioners. National conferences include the Disaster Recovery Journal (DRJ), Continuity Insights, and Contingency Planning and Management (CPM).

Above all, participation in testing/exercises often proves to be the most useful training for response and recovery team members.

---

## **Testing and Maintenance**

#### **42. What are the prevailing practices regarding the storage of BCP documentation?**

Plan storage techniques range from storing printed plans off-site to electronic plans stored off-site and available via the Internet. In smaller organizations, up-to-date plans are printed, numbered (for control purposes, given the sensitive nature of plan content) and disseminated to personnel named in the business continuity plan. Employees in general may receive copies of emergency response procedures, to include evacuation procedures, first aid reminders and bomb handling procedures. When a plan becomes outdated, it is returned for an updated version. When an employee leaves the company, the plan is returned as part of the exit process. Key members of business continuity teams typically have copies of the plan available at home, at work, and pre-positioned at recovery locations.

BCP software, knowledge management platforms and off-site file servers have resulted in fewer hard copies and the growing use of electronic planning material. Technology has made it difficult to control plan dissemination and duplication, although the plans are much easier to store and update. Technology has also allowed plans to be segmented more easily, with team members receiving only those components of the plan that apply to them. Of note, for those organizations that do use electronic plans, management still stores hard copy documentation (typically in off-site storage) in the event of network downtime or a sustained power outage.

#### **43. How often should business continuity-related documentation be updated?**

In general, business continuity documentation should be reviewed and updated at least on an annual basis. However, a more frequent review and update process may be required as changes in the organization occur. The business continuity team should stay abreast of changes, such as mergers, divestitures, entry into new markets or the implementation of new technology, which may impact the current plan in place. Key review

and update activities to consider include the following:

- Business unit and associated function listing and validation of criticalities as determined in the BIA
- Risks/threats that may impact key business operations
- Business unit/function dependencies/inter-dependencies (IT and non-IT)
- Opening/closure of key office locations
- Key employee/vendor contact information (e.g., call tree)

#### **44. How should the organization keep the plans current?**

Given the decentralized nature of most business continuity programs, a cross-functional team should be responsible for maintaining the crisis management and crisis communications plans, as well as updating risk assessments and business impact analyses. Business function and technology owners should be responsible for their individual resumption plans.

Internal audit should enforce a defined review and plan maintenance schedule, as defined in the BCM policy.

Regardless of the process used to maintain the business continuity plans, maintenance should be based first on a defined schedule. Business continuity plans should be reviewed annually, or when significant changes to the business occur, whichever is sooner. If an organizational change management process is in place, BCM should be integrated into this program.

Human resources information, to include contact information, should be reviewed quarterly.

#### **45. How often should the business continuity strategy be tested?**

As often as possible. Management expectations, test objectives, the maturity of the planning process and system/process criticality are all factors when deciding how often to test. The majority of organizations test business continuity processes one or two times a year; however, this can be increased by such factors as:

- Changes in business processes
- Changes in technology
- Change in BCP team membership
- Anticipated events which may result in a potential business interruption

Organizations may also choose to conduct more tests or exercises if operations are decentralized across multiple locations. Additionally, some business continuity coordinators choose to conduct testing in stages given the size of their IT infrastructure, the size of the business, or their relative inexperience with BCM testing. Others want to rotate as many people as possible through the training experience given the valuable benefits. Regulatory requirements may also influence the number of tests performed annually.

No matter how many tests are conducted each year, be sure to schedule them in advance to ensure maximum participation. Develop a progressive, incremental schedule that includes a timetable of events.

*Note: The information printed in this answer was authored by Protiviti and originally published on the ISACA website (2003).*

**46. What are available test options?**

Conducting the same test twice a year will quickly lead to stagnant outcomes and bored participants. It’s important to mix it up. This section highlights the type of tests available to your organization, as well as the implications associated with each.

Test Type	Description and Implications
<b>Desk Check (a.k.a. Boardroom Style or Tabletop Testing)</b>	Assemble recovery team members and walk through the plan using test scenarios and a series of test scripts. Tabletop testing is the safest to do, but least useful because recovery strategies are not really tested or operationalized. Visualizing the BCP in action is part of the development process, but the value is limited. A more in-depth simulation will provide a stronger understanding of how the response teams work together, as well as a sense of the time needed for recovery and restoration activities.
<b>Simulation (a.k.a. Full Scale Interdependency Testing and Walkthroughs)</b>	Simulate a disaster and determine how well the plan responds to the specific event in the operational environment. This method may be the most costly testing method and also the most dangerous to the business if not isolated properly.
<b>Procedure Verification Test (a.k.a. Business Function Testing)</b>	Limited in scope to a specific process or business unit, procedure verification testing evaluates the logic of a specific procedure to determine if a deficiency exists through a combination of desk checks and simulations. This approach is useful following an isolated business continuity test failure.
<b>Communication (Call Tree Testing)</b>	Communication is a key component of a BCM process. Test the accuracy and completeness of the organization’s employee call tree, customer contact information channels and critical supplier/vendor/business partner contact information as part of a tabletop exercise or simulation, or potentially as a stand-alone activity.
<b>IT Environment (Systems and Application) Walkthrough</b>	Conduct an announced or unannounced disaster simulation and execute documented system recovery procedures. The primary objective: Verify that critical systems and backup data can be recovered based on a specific timeline and documented application interdependencies. This scenario exercises “active-active” and “active-backup” IT continuity models.
<b>Alternate Site Testing</b>	A test of all restoration/recovery components at an alternate site. This should include a test of the organization’s ability to relocate staff to the alternate site, as well as a validation that recovery processes and IT assets operate.
<b>End-to-End Testing</b>	A test of alternate site facilities, to include both business and IT. An end-to-end test differs from an alternate site in that critical suppliers/business partners and customers – internal or external – are included within the scope. This test typically validates connectivity to the business’ production site.

Regardless of the type of test employed, incorporate actual data and simulate real-world conditions whenever possible. Additionally, develop the test scenario based on the results from the risk assessment. Choose a likely risk to which the organization may be vulnerable. And if you or your organization are new to business continuity plan testing, start small. As your business continuity process matures, increase the size and complexity of the test.

Business continuity coordinators also have the responsibility to be original and capture the interest of test participants. We have observed one coordinator who operates his tests like a MONOPOLY game, using chance cards to insert anticipated variables into the test process. Others insert a bit of realism by randomly selecting personnel to “sit out” and observe tests to see how the rest of the team reacts. These are just a few ideas to add realism and keep exercises interesting.

*Note: The information printed in this answer was authored by Protiviti and originally published on the ISACA website (2003).*

#### **47. Should the organization expand testing beyond IT?**

Absolutely. There are several options available to expand testing throughout the organization, although a necessary first step is to involve end users in IT disaster recovery tests. We recommend the creation of a testing policy that dictates standards and guidelines for exercise participants and a schedule to include crisis management, business resumption and IT disaster recovery.

Use a variety of methods for exercising plans:

- Exercises that address or integrate product recall, aviation incident emergency response, human impact and other types of atypical issues
- Incident-specific scenarios on unplanned exercise dates with unexpected exercise scenarios
- Walkthroughs of existing plans with recovery teams
- Cooperative exercises with key partners and customers
- Industrywide exercises administered by local industry organizations or service bureaus
- Local response procedures to a regional crisis
- Exercise interdependent recovery plans simultaneously

Require internal audit participation for each test. Internal audit and business continuity personnel should perform the following tasks:

- Document observations
- Perform follow-up (within three months of when major deficiencies are noted)
- Repeat until noted issues are satisfactorily resolved, as per internal audit's observations

#### **48. Why does it take so long to adequately plan for an IT disaster recovery test?**

Often, one of the best ways to measure the adequacy and completeness of IT disaster recovery strategies and documentation is the ease of test planning. Although coordination with business functions potentially impacted by a test is critically important (and when a third-party is utilized, coordination is needed there as well), planning for available technical resources should be eased due to defined, up-to-date recovery strategies, recovery teams and recovery/verification/restoration procedures. Some organizations struggle with test planning because they “reinvent” the IT disaster recovery strategy for each test – going so far as writing recovery procedures from scratch to meet the scope of the test – as opposed to defining and maintaining an “everyday” IT disaster recovery process.

If the organization is investing six months of employees' and management's time for each test, our recommendation would be to reallocate that time into developing repeatable procedures with necessary resources that could enable recovery strategies designed to meet business-validated RTOs.

Lastly, organizations should ensure that each test focuses on validation of business continuity strategies and supporting plans – “Test the plan, not the people.”

---

## Compliance Monitoring and Auditing

### 49. Describe the connection (if any) between Sarbanes-Oxley and business continuity.

Beginning with the passage of the Sarbanes-Oxley Act (SOA), management and auditors alike have struggled with defining the scope of business continuity as an internal control related to financial reporting. Some executive managers have advocated business continuity-related processes independent of SOA because they're viewed as good business practices. Others have stated business continuity is not an internal control consideration related to financial reporting, while some have adopted a "minimalist" view and developed IT disaster recovery strategies focused exclusively on the systems that consolidate financial data and generate financial reports. External audit firms have struggled as well, providing conflicting guidance mirroring management's struggles.

Arguably, the confusion and struggle are behind us now that the Public Company Accounting Oversight Board (PCAOB) has elected to exclude business continuity and contingency planning from Section 404 compliance requirements. What will this mean for business continuity? With the exception of the "minimalist" organization that may now have to struggle for management support and funding for business continuity, the primary effect is the exclusion of the auditor's review of business continuity as a "current period" internal control over financial reporting. However, as a business issue and management priority, the importance of business continuity will not diminish. Simply put, you must have confidence that your financial reporting process, and all supporting systems, can survive a business interruption.

### 50. Is the PCAOB position on business continuity right or wrong?

Based on our preliminary discussions with a wide variety of business managers and industry practitioners, the feedback is mixed. Many agree with the statement regarding future periods and controls. However, others point out that the failure of key financial applications, data sources and business functions related to the consolidation and generation of financial statements would impact the completeness, accuracy and availability of the financial report. Specifically, the key financial reporting processes that could be affected by a business interruption include:

- Capturing, authorizing and processing transactions
- Processing cut-offs
- Developing disclosure data
- Consolidation
- Fair-value information pricing
- Trading position and current market exposures

James DeLoach, managing director for Protiviti and a leader of the company's Sarbanes-Oxley compliance practice, stated in a report\* on PCAOB Auditing Standard No. 2:

*While the Board concluded that business continuity and contingency planning did not affect a company's current abilities to initiate, authorize, record, process or report financial data, it is important to recognize that systems which are vital to the sustainability of the business may also have significant financial reporting implications. Management has a responsibility to ensure that data needed to facilitate the initiation, authorization, recording, processing and reporting of financial information is available when needed, both now as well as in the future. The problem is, no one knows when events triggering the need for a disaster recovery plan will occur. If a significant, priority system goes down and a company loses large amounts of data that is critical to financial reporting because of the absence of effective disaster recovery capabilities, there will be a lot of explaining to do if the lost data results in*

*missed reporting deadlines or causes the certifying officers to refuse to sign certifications because critical information isn't available. Perhaps these are extreme examples, but they can occur and, if they did, I wouldn't want to be the one facing the audit committee trying to explain why disaster recovery isn't important to financial reporting.*

\* Source: Protiviti PCAOB Flash Report, "PCAOB Adopts Final Standard for Audits of Internal Control Over Financial Reporting," March 9, 2004 (available at [www.protiviti.com](http://www.protiviti.com)).

## **51. How do organizations mature their business continuity programs?**

Business continuity maturity is increased based on a number of factors, including:

- Executive management sponsorship, which includes clear accountability/responsibility, as well as the definition of a budget
- A formal business continuity policy, driving compliance with industry standards
- Recurring risk assessments and business impact analyses
- Formal training and awareness programs
- Recurring program maintenance activities, focused on updating strategies and plans
- Business continuity test execution, which increases awareness and identifies business continuity program weaknesses
- Compliance auditing, based on a defined internal policy

## **52. How often should the business continuity program be audited?**

The answer is organization-specific, based on the internal standards and regulatory requirements faced by the company. In most cases, an audit should be conducted every 12 to 24 months in order to ensure compliance with internal policies and procedures, with particular emphasis on the execution of testing, training and maintenance activities. In a growing number of organizations, internal audit is an observer of all major testing activities, as opposed to a reviewer of test summary documentation. As such, the frequency of audit-related activities increases.

The Institute of Internal Auditors published Practice Advisory 2110-2, *Internal Audit's Role in the Business Continuity Process*. The optional guideline does not prescribe an internal audit frequency; however, it states business continuity-related audit activity should take place "on a regular basis."

## **53. What is the optimal role for internal audit in BCP?**

Because of its role in the organization, the internal audit department is positioned to add considerable value in terms of BCM. Here are a number of ways:

- The Internal Sales Person – Assists with making the case for business continuity through participation in the Risk Assessment and BIA processes (tasks that internal audit traditionally addresses through the development of annual audit plans).
- Business Continuity Policy Creation – Internal audit, because of its familiarity with policies, controls and the key components associated with a BCM process, can assist with the development of initial policies and standards (in line with reasonable maturity levels and business objectives).
- Project Management Standards – Similar to the development of business continuity policies, internal audit is also familiar with project management standards and project risk management programs.

- Focus – In addition to scoping the process from a business and technology perspective, internal audit can assist in focusing the effort on a program development perspective, as opposed to a sole focus on plan documentation. Specific attention also should be paid to the planning and execution of business continuity tests and exercises. Internal audit should observe such tests and ensure that anomalies are addressed.
- Audit the Business Continuity Program – Regarding internal and industry standards/requirements, internal audit is positioned to review the planning process and strategies to ensure compliance. Internal audit can develop recommendations to address opportunities for improvement as well.
- Management Communication – Internal audit can formally communicate program status and capability to management to ensure expectations are met.

#### **54. Can an internal audit department – internal or outsourced – participate in BCP activities?**

Because BCM is a management-owned process, whereby management is responsible for all decision-making regarding the design of the BCM program, internal audit can be an active participant and advisor to the organization's business continuity project sponsor and steering committee. In many cases, BCM-related skills, experiences and core competencies reside within internal audit departments given the availability of training, as well as the day-to-day mindset of managing risk – continuity or otherwise.

The Institute of Internal Auditors, or The IIA, also clarified the issue in June 2003 with the release of Practice Advisory 2110-2, Internal Audit's Role in the Business Continuity Process. In it, The IIA states that internal auditors should not only evaluate business continuity readiness, but also participate in the following activities:

- Internal auditors can play a role in the organization's planning, to include the risk assessment (it is typical for internal audit to help with an assessment of an organization's internal and external environment).
- Evaluate the BCP/DRP during planning and development (internal auditors have a thorough understanding of the business, the individual functions and interdependent relationships, and contribute to the BCP process).
- Review the proposed business continuity and disaster recovery plans for design, completeness and overall reasonableness/viability.

#### **55. How does an organization review key vendor planning for business continuity compliance with industry best practices?**

An organization could review key vendors' continuity plans using three different approaches:

1. Make vendor inquiries and ask if they comply with the key provisions found in your business continuity policy.
2. Request a copy of the business continuity plan and perform a review.
3. Issue a questionnaire addressing the following topics:
  - Does your organization have a documented, tested BCM process?
  - Have you conducted a formal Risk Assessment based on your industry and locations of operations?
  - Have you conducted a formal BIA based on your industry and locations of operation (to include an interdependency analysis)?
  - Are you comfortable your company is adequately prepared to handle unplanned business interruptions?

- Have you performed a supply-chain continuity assessment?
- Who in your organization “owns” the BCM process?
- How much does your organization budget toward the development and maintenance of the BCM process (do not include IT asset costs, such as SAN implementations, etc.)?
- Do you have an alternate facility to recover operations in the event your main offices, production locations or distribution centers are inaccessible? If yes, how far away are their facilities from your primary operating site?
- Does your organization maintain a crisis communications plan, which includes having designated people who are trained to speak to the media?
- Has your organization ever tested its business continuity plan?
- Does your organization offer a formal training and awareness program to familiarize employees with your business continuity plan?
- Has your business continuity plan ever been benchmarked against industry standards/codes or your competitors?

In the absence of adequate business continuity programs, alternate vendors should be identified for key products and services.

---

## Industry-Specific Questions for BCM Programs

### *Manufacturing*

#### **56. Have you properly evaluated the risk of supply interruption from critical component suppliers?**

As manufacturers streamline their supply chains and rely more on single- and sole-source suppliers, they are discovering that they have not measured the additional risk this poses to their organizations. Even in cases where companies do measure the financial risks of a certain supplier (e.g., credit risk), they have not taken into account the risk of a business interruption stemming from a man-made or natural disaster. Manufacturers should identify alternate sources for their most critical supplies, lead time for finished product, political and natural disaster risk, and then develop strategies to mitigate the impact of business interruptions occurring among key suppliers.

#### **57. What major systems or applications support the operations, particularly ERP and MRP? Has management designed manual backup procedures to carry out manufacturing schedules and order releases?**

Most modern manufacturers have switched to automated MRP and ERP systems, and as a result, have not thought about creating manual workarounds to carry out manufacturing schedules and order releases during an outage. Furthermore, smaller companies (those with fewer than 250 employees) still do much of their scheduling on non-networked PCs, leaving themselves open to the possibility of losing critical documentation that resides on only one desktop.

#### **58. How would system outages prevent operations from accessing product configuration and inspection data? Are incoming inspection data available offline for use in receiving?**

In a fully automated MRP and ERP environment, all data are computerized, including inspection and configuration data. Manufacturers should have separate paper and common format digital copies of all configuration data that a contract manufacturer may use in cases of a total loss to recreate the original environment.

### **59. How do companies that rely solely on single-site manufacturing or computer-aided manufacturing operations plan for the impact of a long-term outage?**

As manufacturers become leaner, leveraging single manufacturing locations and automated processes, it is critical that they investigate existing customer service-level agreements (SLAs) to ensure what, if any, are their liabilities during a long-term outage. In many cases, there is simply no longer a “sister plant” to transfer a meaningful portion of the work. Even where these plants do exist, they are almost always capacity constrained by operational, environmental or logistics limitations.

Even without a formal SLA, manufacturers’ customers expect that products will arrive on time, with the correct quantity and in acceptable condition. Ultimately, the only three options a lean manufacturer has to recover operations are to delay the impact through inventory controls, and expedite partial manufacturing throughput and full resumption. Certainly excess inventory, intermediary warehousing, contract manufacturing and redundant location are all possible solutions. However, from management’s perspective, business continuity strategies could nullify the efficiencies they intentionally built into the operations, since these options are all capital intense. Therefore, a significant amount of analysis usually is required to justify any strategy.

### **60. Can purchasing access MRP data offline to continue ordering products with key suppliers?**

Most outages last an average of 4.5 days. These are obviously not total-loss scenarios but smaller outages. Manufacturers should make sure they have access to MRP data offline to ensure the continual ordering of products with key suppliers.

### **61. Where does my product recall procedure fit into a BCM program?**

Every manufacturer should have a robust and tested product recall plan to address the need to pull products from the marketplace due to safety or quality concerns. A good product recall plan addresses not only how product would be pulled in the event an issue is discovered, but how a product defect would be “traced” and the root cause isolated, tracking mechanisms to determine how much of the suspect product is out of the marketplace and plans to address how returned products would be disposed of in a financially and environmentally responsible manner. Many industries are regulated to develop and test these plans.

For a manufacturer, a product recall is among the most serious crises that can occur since they can affect not only finances and operations, but also reputation and people’s health and safety. The management of a product recall should be handled no differently than the management of any other significant crisis event. We recommend that the same interdisciplinary team of business unit and corporate senior managers making decisions take into account all facets of managing the crisis.

## ***Healthcare***

### **62. What should be the focus of my business continuity plan?**

Most healthcare providers take their initial direction on business continuity management from the JCAHO Environment of Care standard. This requirement focuses first on patient care and safety. These plans are often developed in silos; as a result, resources are not coordinated across all departments. For example, plans may state that patients will be temporarily relocated to another primary care facility, but they may not cover continuity of care, medical records management during the relocation, access to electronic patient data during the transfer period or how the provider would transition back to normal, with daily census going from 0 percent to full capacity in a very short period of time.

In your business continuity plan, focus on the most important asset that you have: your staff. Make sure that your business continuity plan has provisions to recover staff and take care of their needs during an emergency. This could include their families’ needs as well, and may involve allowing employees to work from home, take additional sick time and/or rely on your assistance in finding appropriate healthcare, if necessary. Because a

regional disaster that affects a healthcare provider is also likely to result in an increase in patient needs and the loss of community infrastructure, it is important to plan for the possibility that your staff will be unable to return to their homes for an extended period. In the aftermath of a disaster, you should also make sure that your human resources technology systems allow access to employee contact information, payroll and the job skills database. Doing so will enable you to maximize cross-trained personnel and quickly identify skill shortages during a disaster.

Review your essential healthcare data and application systems. Electronic medical and health records (EMR) are increasingly common, but you should make sure that you have redundant EMR systems in place. Next, make sure to consider backup and off-site storage – options to ensure that data are accessible during the emergency. Consider an alternative facility in another geographic location that allows you to replicate data and communication services. In the age of HIPAA, it is not enough to simply plan to recover these applications and data – it must be done in a manner that is equally secure and as private as the normal operating procedure.

Finally, inoculate your supply chain. Healthcare providers are using just-in-time (JIT) inventory strategies in much the same way manufacturers have for years. This is obviously an issue when it comes to pharmaceuticals and clinical supplies, but don't overlook mundane items such as bed linens and cafeteria stockpiles. During a disaster it is important to maintain as much normalcy for patients and staff as possible and the routine aspects of their day – coffee, cafeteria service, vending machines, clean sheets, etc. – can be critically important. Review the SLAs with large suppliers like McKesson and Cardinal, as well as smaller suppliers who are instrumental to the overall quality of care at your institution.

### **63. Should there be a separate plan for avian flu?**

There has been much discussion around what organizations, in particular healthcare, should do about avian flu as part of their business continuity plan. Healthcare providers are on the front lines for treating patients during a pandemic and are therefore likely to be affected operationally by high absenteeism and illness among their own staffs. Even so, most organizations do not develop “separate” pandemic plans, but rather create appendices for their strategic crisis management plans (used by executives) and tactical continuity plans (for business processes).

We recommend that you download the Business Pandemic Influenza Planning Checklist at [www.pandemicflu.gov/plan/checklists.html](http://www.pandemicflu.gov/plan/checklists.html) and answer the questions it contains. Once you've performed the self-evaluation, you'll know where your organization stands with respect to preparing for a pandemic. The checklist is a good resource to diagnose your readiness, but it does not provide specific solutions for many of the areas it covers.

Then, contrast your current business continuity plan with the self-evaluation, identify the gaps and expand your plan to fill them.

### **64. What type of testing should be performed and how often?**

Healthcare providers are required by JCAHO to perform internal and external disaster drills focused on the environment of care. This testing would fall under the emergency management portion of the business continuity plan and include drills for specific departments (ER, OR, specialty clinics), use of emergency power and lights, call tree testing, and procurement of food and water.

A separate test should be done on information technology systems, i.e., an IT disaster recovery test. This would include backup procedures, moving services (data/voice) and the building of servers and equipment. During the test, users should access the restored system(s) remotely to ensure that they can operate at an acceptable level with the current recovery resources. Restoring the pharmacy system off-site is of little value if admissions staff cannot access it to perform their key tasks in a disaster. Testing of this type is a requirement HIPAA deems “addressable,” meaning the institution is required to perform these tests or have a reasonable basis for why it does not perform them. Nearly every healthcare provider, insurer or clearinghouse should perform IT disaster recovery tests.

Finally, the organization should perform an all-encompassing exercise that includes both emergency management and IT disaster recovery. As with all these tests, the organizations would flow the lessons learned back into the business continuity plan for retesting. Emergency management plans/drills should be done on a quarterly basis, while IT disaster recovery plans should be done annually. These exercises must be conducted at the local, tactical level as well as at the senior-management, strategic level.

#### **65. Who should oversee and maintain the plan?**

Historically, the business continuity plan sponsor usually resided within Information Technology (IT). The reason is that the legacy disaster recovery programs were focused on the backup and restoration of data from mainframes and servers.

Healthcare companies are gradually embracing the trend of moving ownership of business continuity to the business units. This shift has already largely occurred in financial services, retail and manufacturing. Other organizations position the business continuity manager within Facilities Management, where the concern principally has been over buildings and equipment, or Finance, where it is seen as an extension of the insurance and risk management program.

#### **66. Have you properly evaluated the risk of interruption in automated information availability?**

Automation in healthcare now includes more than just billing, purchasing, payroll and accounting. Technology continuity issues now encompass records management, chart maintenance and medication dispensing, and most healthcare providers are moving to electronic imaging – all directly having an impact on patient care.

Inadequate availability of information has costs related to billings, collections and reputation of the organization. And as more organizations embrace the electronic health record (EHR), there are new costs related to direct patient care.

As healthcare organizations become more dependent on automated systems for everyday efforts, they become less aware of historical and potential manual workarounds. Given the risks associated with limited availability of information, healthcare organizations are facing the labor costs of manual workarounds sufficient to mitigate the risk to patient care.

#### **67. How do healthcare organizations consider technology downtime (especially unscheduled or extended downtime) in their business continuity programs?**

For healthcare organizations, technology reliance dramatically increases risk. Information availability is much more than just the ability to continue to process data in the event of a disaster. Organizations have to secure their business operations as well as consider the impact on their ability to provide quality patient care. To mitigate the risk, organizations need to consider:

- Having people available to operate in a fully manual environment, while still providing patient care
- How the institution can leverage the existence of enterprise applications to create standardized, quality controlled manual workarounds
- Developing processes and procedures to guide continued operations without IT availability
- Developing adequate IT general controls to ensure changes to systems do not cause interruptions
- How compliance with regulations, such as HIPAA Security and Privacy, and billing requirements could be impacted by a lack of IT availability

**68. How would system outages prevent operations from continuing to deliver medical care following emergencies?**

Having access to patient history can be critical in an emergency situation (e.g., knowing drug and food allergies, knowing about current medications that could negatively interact with emergency measures, awareness of living will requests, etc.). Having access to information in an emergency situation can be a matter of life or death.

Organizations must have processes in place that include all measures for accessing historical information about a patient, whether it is through family members, physician practices, hard copy records or other means. Other options may be to use heroic measures less likely to interact with other medications/treatments the patient is currently using.

Organizations should also consider having protocols for sending orders to the pharmacy and specimens to the lab. An alternate means of communication will be critical, whether internal or external.

**69. Does the organization rely on automated information systems to the extent that operations would cease during a long-term outage?**

Disaster preparedness for healthcare is more complex than for other industries because it involves continuity and recovery planning, in addition to traditional emergency response management.

JCAHO defines an emergency as “a natural or man-made event that suddenly or significantly disrupts the environment of care; disrupts care and treatment; or changes or increases demands for the organizations’ services.” For years, healthcare organizations have been aware of the need to plan for and test their ability to continue delivery of medical care following emergencies.

Healthcare organizations must focus their preparations on restoring critical services immediately, including communication systems and access to patient information. As a matter of course, “routine operations” would cease; however, emergencies would require that the facility be able to provide some level of critical care should the need arise.

In times of disaster, some businesses decide to close their doors until the situation becomes more stable. Healthcare organizations do not have this option. Given the current shortage of human resources in specific areas of healthcare and the highly competitive employment market, a healthcare company that ceased operations for several days or weeks would have a very difficult time rebounding. At the very least, even a brief temporary closure would have a negative public relations impact.

**70. Can providers access EHR data offline to continue treating patients?**

The goal of the EHR is to create a true continuum of care by eliminating the paper shuffle, creating immediate access to patient information (no matter where that patient presents for treatment) and facilitating sharing of information across the provider network. Therefore, while organizations do have some redundancies in place to provide limited information in the case of an IT interruption, significant information would not be available and, as a result of manual processes, other information could be lost.

Healthcare organizations should structure manual workarounds and put processes in place that continue until all information in the EHR is current and accurate. This can put a tremendous burden on the organization in terms of the availability and cost of labor.

## *Telecommunications*

### **71. Have you properly evaluated the risk of interruption from key vendors, such as invoicing support?**

Telecommunications companies often rely on third-party vendors to perform critical functions such as invoicing. Too often communication providers are so preoccupied with internal risks that they neglect to measure risk to critical outsourced vendors. Even when companies do measure financial risks, business interruptions stemming from man-made or natural disasters fly under the radar. Telecommunications companies should identify which critical tasks have been outsourced and develop strategies that would mitigate the impact of a business interruption that affects key vendors.

### **72. How would system outages impact the mediation function? Are call detail records backed up offline?**

The billing mediation platform is critical for collecting, collating and preparing data for the downstream systems. This not only drives billing for revenue, but is also a key component in capacity and network planning. Without a solid disaster recovery plan in place, a telecommunications company places itself at an unfair disadvantage by failing to mitigate basic risks in business continuity management.

### **73. Has management designed manual backup procedures for major systems or applications supporting the order, billing and mediation functions? If so, have they tested the plan?**

Enterprise applications are instrumental to any company. However, they take on even more importance in the telecommunications industry. Consequently, many companies have implemented an internal disaster recovery plan or worked with a third-party vendor to protect their enterprise infrastructure. Unfortunately, companies often neglect to test these plans. Without well-developed testing, companies can't know if the plan will be effective when the time comes to use it. Through testing of business continuity and disaster recovery plans, companies confirm that their plans are viable and executable. Testing also allows for continuous improvement over the BCM program and offers the capability to adjust the overall business continuity strategy if necessary.

### **74. How would management handle customer service if a call center were unavailable? Does the company have more than one call center?**

Customer service is critical in the highly competitive telecommunications industry. Although customer service call centers are not revenue generators, they are vital for maintaining a happy and satisfied customer base. If there is a call center interruption, the applications and databases may have been recovered, but with whom and how do you connect the customer? The right people need to be placed in the right place in a quick and effective manner after a disruption. This can be accomplished through a crisis management and business resumption plan.

### **75. Can billing operations access critical data offline to continue the billing function during a billing system outage?**

For many companies, the disaster recovery plan is nothing more than a good doorstop that collects dust. Or, it has been outsourced and is therefore out-of-sight, out-of-mind. Although the plan may be officially in place on paper, do your employees know how to utilize what's currently written down? For instance, critical billing data may be backed up at the third-party vendor, but does billing operations know how to access the data offline? To be effective, a business continuity or disaster recovery plan requires not only testing, but also employee training.

## *Retail*

**76. What concerns do retailers have about point of sale (POS) transactions in the event of an extended network outage with the central office? Do the same concerns exist with debit transactions, credit transactions, returns and other chain-specific transactions?**

The lifeblood for any retailer is the ability to conduct transactions at the store level. While cash transactions are an important part of the daily take, more than ever the ability to initiate debit/credit transactions is critical in order to satisfy customer preferences. Furthermore, the trend over the last decade has gone from store autonomy to heavy dependence on the central office for transaction support and real-time, back-end processing. This trend has increased the risk of stores being unable to continue doing business as usual once the link to central has been severed. Therefore, it is important for companies to (1) create redundancies between the stores and central offices, and understand the alternatives of connecting to stores and warehouses, (2) determine whether third parties can handle credit/debit card transactions more efficiently, while also providing better availability, and (3) ensure that stores are prepared for the worst by arming them with the procedures they need to operate during an outage, including manual credit card machines. The more transparent these strategies are to the customer, the better.

**77. What are the risks of self-distribution versus outside suppliers? What about the risk of larger, centralized distribution centers versus multiple smaller locations? If warehouses are limited to larger and less numerous sites, have retailers assessed and mitigated the environmental risks (e.g., fire, flood, etc.)?**

Big is better, but sometimes big can also be riskier. As companies formulate and execute distribution strategies, they must give sufficient thought to the availability risk of their primary distribution facilities. To mitigate the increased risk of warehouse loss due to increased levels of self-distribution and/or warehouse consolidation, environmental considerations should play a bigger role in strategic and tactical decisions. Businesses should recognize and sufficiently mitigate the following risks: seismic and flood risks, structural soundness of the facilities, risk of fire based on volatility of product, etc.

**78. Is the business insurance coverage based on geographic footprint and risk potential? Is there any business interruption insurance and is it adequate?**

A number of organizations leverage business insurance as an important piece of their comprehensive business continuity strategy, reducing those risks they cannot effectively manage themselves. Since retailers are regularly building new stores, warehouses and facilities to support their strategic vision, their risk profile is also changing. This shifting risk profile needs to be consistently monitored to ensure that the insurance coverage is adequate and reflects not only the potential loss of a facility, but also the business lost due to a significant disruption.

**79. What issues are there in regards to the customer service functions? Can customers' questions and concerns be addressed shortly after a disruption?**

The customer is king. This is true whether it's business as usual or during recovery from a major disruption. No matter the situation, retailers and consumer products companies need to ensure their customers are well-informed regarding the products they sell. This translates into strategies that ensure that the necessary IT infrastructure and customer service team members relocate to an alternate location when disruptions occur. Companies can take the additional step of establishing relationships with third parties that have the capabilities to take on the service function if needed.

**80. How are buyers able to manually purchase products and supplies without the EDI up and running?**

An organization's Electronic Data Interchange (EDI) is a critical link to the suppliers and vendors that provide products and raw materials. Companies should ensure that product supply and delivery will continue even when EDI is unavailable by maintaining sufficiently detailed manual procedures and vendor lists to reestablish

delivery links. Additionally, by having conversations with your suppliers before an outage, you will understand capabilities and expectations when critical links are out. This will go a long way toward a quick recovery and peace of mind.

---

## About Protiviti Inc.

Protiviti is a leading provider of independent risk consulting and internal audit services. We provide consulting and advisory services to help clients identify, assess, measure and manage financial, operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews.

Protiviti, which has more than 50 locations in the Americas, Asia-Pacific and Europe, is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

## *Business Continuity Management Services*

Protiviti creates Business Continuity Management (BCM) value by developing practical, cost-effective plans that can actually be executed during an interruption, and don't simply rely on mythical best practices. Our holistic approach has been proven in all industries and aligns with your investment in other pressing business, regulatory and compliance issues, including Sarbanes-Oxley.

We offer BCM services that are business-oriented and based upon the risks and impacts relevant to an organization's key business processes. Backup strategies alone are not enough anymore. Our planning focuses on the evaluation of those people, processes, technology and data that are vital to your operation. Our BCM methodology relies on the expertise of our Certified Business Continuity Professionals (CBCPs) when developing strategies and plans.

Our portfolio of BCM services includes risk assessments, business impact analyses, recovery strategy development, plan documentation, plan testing, training program development, and program audits and assessments.

Protiviti's BCM services add value for our clients in the following ways:

- **Business Alignment:** Helps match IT disaster recovery capabilities with business expectations and integrates with regulatory and compliance programs
- **Business Impact Analysis:** Identifies threats, risks, exposures and impacts relevant to your business
- **Strategy Design:** Focuses on the mitigation of threats, risks, exposures and impacts to a tolerable level
- **Testing and Maintenance:** Standardizes an approach for organizations to own, maintain and test their BCM programs
- **Holistic Approach:** Implements Business Recovery, IT Disaster Recovery and Crisis Management across the enterprise
- **Plan Development:** Builds, maintains and executes BCM content that produces consistent, repeatable BCM processes that can be applied across the enterprise on a recurring basis.
- **Automation:** Uses PACEmaker (a tool-set that applies an analytic approach and methodology to produce results, and serves as the key component of our knowledge transfer process) and Protiviti-designed plan templates to support effective plan development and maintenance (e.g., personnel information and recovery resources).

---

Notes

### *North America*

UNITED STATES  
+1.888.556.7420  
protiviti.com

CANADA  
+1.416.350.2181  
protiviti.ca

MEXICO  
+52.55.9171.1501  
protiviti.com.mx

### *Europe*

FRANCE  
+33.1.42.96.22.77  
protiviti.fr

GERMANY  
+49.69.963768.100  
protiviti.de

ITALY  
+39.02.655.06.301  
protiviti.it

THE NETHERLANDS  
+31.20.346.04.00  
protiviti.nl

UNITED KINGDOM  
+44.20.7930.8808  
protiviti.co.uk

### *South America*

BRAZIL  
+55.11.3443.7240  
protiviti.com.br

### *Asia-Pacific*

AUSTRALIA  
+61.3.9948.1200  
protiviti.com.au

CHINA  
+86.21.3401.4630  
protiviti.cn

INDIA  
+91.11.4051.4198  
protiviti.co.in

JAPAN  
+81.3.5219.6600  
protiviti.jp

SINGAPORE  
+65.6220.6066  
protiviti.com.sg

SOUTH KOREA  
+82.2.2198.2065  
protiviti.co.kr

Protiviti is a leading provider of independent risk consulting and internal audit services. We provide consulting and advisory services to help clients identify, assess, measure and manage financial, operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews.

*Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.*