CONTENTS

Introduction ........................................................................................................ v

Business Continuity Basics ............................................................................. 1
  1. What is business continuity management (BCM)? ........................................ 1
  2. BCM seems to include many different terms, some of which appear to be very similar. How are they similar or different? ............................................... 1
  3. Is there a best practice approach to business continuity planning (BCP)? ......... 2
  4. What BCM elements are included in ITIL – specifically, IT service continuity management? ............................................................. 2
  5. What is the relationship between business continuity and enterprise risk management (ERM)? ........................................................... 3

Overview of the Regulations and Standards Landscape ..................................... 4
  6. How should regulations and standards shape the development of a BCM program? .............................. 4
  7. What are ISO 22301 and ISO 22313? ...................................................... 4
  8. What is NFPA 1600? ................................................................................. 5
  9. There is a BCP requirement published by the U.S. Securities and Exchange Commission (SEC) regarding New York Stock Exchange (NYSE) members. Are all NYSE-listed companies required to follow these BCP guidelines? .............................................. 5
 10. Does the Health Insurance Portability and Accountability Act (HIPAA) include a requirement to implement BCM processes? ........................................ 6
 11. Does The Joint Commission require BCM for hospitals? ............................ 7
 12. What guidance does the Federal Financial Institutions Examination Council (FFIEC) provide specific to BCP? ............................................................. 7
 13. What BCM standards exist in the COBIT standard? ................................... 8
 14. Are these the only BCM mandates an organization should consider? .............. 8

Executive Management Support and Sponsorship .......................................... 10
  15. Who is the right person in the organization to own the BCM process? ............ 10
  16. How can a BCM team gain management buy-in? ....................................... 10
  17. How can executive management be “sold” on business continuity? ............... 11
  18. What is the value to an organization in designing and deploying BCM programs? ............................................................. 12
  19. What are the critical elements of a business continuity policy? ....................... 13
 20. How should an internal business continuity function/planning team be structured? ............................................................. 14

Risk Assessment and Business Impact Analysis (BIA) .................................... 15
  21. What are the most common approaches to executing a risk assessment? ......... 15
  22. What are the most common approaches to executing a BIA? ......................... 15
  23. Should key vendors be included in the BIA? ............................................ 16
  24. What is a recovery time objective (RTO)? ............................................... 16
  25. What is a recovery point objective (RPO)? ............................................... 16
  26. Are questionnaires necessary when planning for business continuity? .......... 17
  27. Are there ways around completing a formal BIA and risk assessment? .......... 18
<table>
<thead>
<tr>
<th>Question</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Strategy Design</td>
<td>19</td>
</tr>
<tr>
<td>28. What are the key considerations when developing recovery strategies?</td>
<td>19</td>
</tr>
<tr>
<td>29. How far apart should primary and alternate sites be?</td>
<td>19</td>
</tr>
<tr>
<td>30. What are the key considerations for pursuing an internal versus a third-party recovery solution?</td>
<td>21</td>
</tr>
<tr>
<td>31. What is a “mobile recovery center”?</td>
<td>22</td>
</tr>
<tr>
<td>32. What is an emergency operations center (EOC)?</td>
<td>22</td>
</tr>
<tr>
<td>33. What are the differences among cold, warm and hot sites?</td>
<td>23</td>
</tr>
<tr>
<td>34. What are key recovery considerations when negotiating a contract for a hosted solution or disaster recovery support (e.g., hot site contract)?</td>
<td>24</td>
</tr>
<tr>
<td>35. How is advancement in technology changing disaster recovery planning considerations?</td>
<td>25</td>
</tr>
<tr>
<td>Plan Development and Strategy Implementation</td>
<td>26</td>
</tr>
<tr>
<td>36. Is software necessary to develop a BCP?</td>
<td>26</td>
</tr>
<tr>
<td>37. What is the difference between crisis management and crisis communications?</td>
<td>26</td>
</tr>
<tr>
<td>38. What is a call tree?</td>
<td>27</td>
</tr>
<tr>
<td>39. Is there a way to make the plan more efficient and effective?</td>
<td>27</td>
</tr>
<tr>
<td>Training and Awareness</td>
<td>28</td>
</tr>
<tr>
<td>40. Are training and awareness the same?</td>
<td>28</td>
</tr>
<tr>
<td>41. What are some successful business continuity training approaches?</td>
<td>28</td>
</tr>
<tr>
<td>42. What are the available certification options?</td>
<td>29</td>
</tr>
<tr>
<td>43. What are the available BCM education options?</td>
<td>31</td>
</tr>
<tr>
<td>Testing and Maintenance</td>
<td>32</td>
</tr>
<tr>
<td>44. What are the prevailing practices regarding the storage of BCP documentation?</td>
<td>32</td>
</tr>
<tr>
<td>45. How often should business continuity-related documentation be updated and how should the organization keep the plans current?</td>
<td>32</td>
</tr>
<tr>
<td>46. How often should the BCP be tested?</td>
<td>33</td>
</tr>
<tr>
<td>47. What are the available testing options?</td>
<td>34</td>
</tr>
<tr>
<td>48. Should the organization expand testing beyond IT?</td>
<td>35</td>
</tr>
<tr>
<td>Compliance Monitoring and Auditing</td>
<td>36</td>
</tr>
<tr>
<td>49. Describe the connection (if any) between Sarbanes-Oxley and business continuity.</td>
<td>36</td>
</tr>
<tr>
<td>50. How do organizations mature their business continuity programs?</td>
<td>36</td>
</tr>
<tr>
<td>51. How often should the business continuity program be audited?</td>
<td>37</td>
</tr>
<tr>
<td>52. What is the optimal role for internal audit in the BCM process?</td>
<td>37</td>
</tr>
<tr>
<td>53. How does an organization review key vendor planning for business continuity compliance with industry best practices?</td>
<td>38</td>
</tr>
<tr>
<td>Social Media Considerations</td>
<td>40</td>
</tr>
<tr>
<td>54. Should social media be a component of an organization’s business continuity program?</td>
<td>40</td>
</tr>
<tr>
<td>55. What are the risks of using social media to support a business continuity program?</td>
<td>40</td>
</tr>
<tr>
<td>56. What are some best practices for monitoring social media during a crisis event?</td>
<td>41</td>
</tr>
</tbody>
</table>
Large-Scale Disasters and Potential Pandemic Events: Lessons Learned .......................... 42
57. What are some of the common lessons learned from large-scale natural disasters that organizations should be aware of when developing their own BCM programs? ................ 42
58. What can organizations do to prepare for a pandemic event? .............................. 44

Industry-Specific Considerations for BCM Programs .................................................. 46

Communications ........................................................................................................ 46
59. How well have we focused on the critical network infrastructure elements supporting our customers? What are our practices for ensuring BCM strategies and objectives for these environments are kept up to date as we continue to expand our infrastructure and/or upgrade critical network components? .......................................................... 46
60. Have we properly evaluated the risk of interruption from key suppliers (e.g., equipment and support, handsets, smart devices, programming and entertainment) that are critical to our ability to provide products and services to our customers and/or support essential internal business functions? ................................................................. 47
61. How well have we designed and tested alternative operational procedures for critical internal functions such as system maintenance, billing and mediation functions? ...................... 47
62. How would management handle customer support if a call center or key call center support systems were unavailable? Do we have appropriate failover capabilities for this type of event? .......... 47

Energy ..................................................................................................................... 48
63. Are there regulatory BCP requirements that typically affect the energy industry? .......... 48
64. What are the most common business processes affected by an outage? .................... 49
65. Energy-related companies typically have a program to manage environmental health and safety (EHS) at their work sites. Doesn’t that cover business continuity requirements? .......... 49
66. Energy companies often operate in politically sensitive areas and/or other areas overseas that experience frequent major natural disasters. What BCP-related precautions should be considered to reflect the risk of operating in those environments? ....................... 49

Financial Institutions .............................................................................................. 50
67. What regulatory guidance should financial institutions rely on? .............................. 50
68. Are organizations required to apply all aspects of business continuity guidance as outlined by the regulators? ................................................................. 50
69. Are financial institutions, such as banks, required to recover within a defined time period? ..... 51
70. Are business continuity standards for financial institutions set only by the regulatory agencies? .. 51
71. To what extent are financial institutions responsible for the business continuity of vendor-supported systems? ................................................................. 52
72. How can pursuing a single-source supply strategy affect my organization’s overall risk of business interruption? .............................................................. 54
73. Has management designed manual backup procedures to carry out manufacturing schedules and order releases? ................................................................ 54
74. How do companies that rely solely on single-site manufacturing or computer-aided manufacturing operations plan for the impact of a long-term outage?  ....................... 55
75. Where does a product recall procedure fit into a BCM program? ............................... 55
76. What are the core concerns regarding point-of-sale (POS) transactions in the event of an extended network outage with the central office? .............................. 56
77. What are some of the key business continuity considerations with respect to warehousing and distribution? ................................................................. 56
78. Is business insurance coverage based on geographic footprint and risk potential? Is there any business interruption insurance and is it adequate? .......................... 57
79. How much focus should be placed on customer service in a disaster situation? ........................ 57
80. How are buyers able to purchase products and supplies manually without the Electronic Data Interchange (EDI) up and running? .................................................. 57

About Protiviti ....................................................................................... 58
INTRODUCTION

“By the time you hear the thunder, it’s too late to build the ark.” – Unknown

Consider the following scenario:

A deadly monster storm hits heavily populated areas on the East Coast, leaving in its wake devastation and chaos. Sound familiar? Now consider the effects on two information technology (IT) data centers that lie in the path of that dramatic weather event.

The company operating Data Center A has a robust business continuity plan (BCP) in place, which includes focusing attention on proactive measures for responding to and addressing the short- and long-term effects of a disaster. In this case, the data center went to generator power before the power outage occurred. Its facilities remained fully staffed thanks to advanced resource planning and were operating as usual until utility power was restored and stable a few days later. The data center never went offline and there was no disruption in service.

Data Center B, meanwhile, had only an ad hoc BCP with poorly defined response measures. It lost electricity and remained offline for several days. There was significant disruption to its services. Several clients viewed this as a weakness and elected to make changes to their data center environment.

In today's global economy, where major supply chains are geographically dispersed yet highly interconnected, organizations don’t even have to be in the same region of the world for their operations to be affected adversely by a catastrophic event. A prime example: the Tohoku earthquake in Japan in 2011, and the tsunami and nuclear crisis that followed. Simply consider Japan’s dominance in the auto and semiconductor industries, and it’s not hard to imagine how these events created ripple effects for companies in Europe, the United States, and elsewhere. Many leading businesses suffered losses in the millions – and some in the billions – due to the triple disaster in Japan because they did not have enough control or visibility into their supply chain. The tragic events in Japan serve as a powerful reminder, especially to organizations with global supply chains that can include several tiers of product and service providers, that “any assessment of operational risk should be directed to understanding the risk of loss of any critical link in the supply chain.”

Extreme weather, crippling failure of mission-critical systems, cyberattacks, and pandemic risks are just some examples of events that can impact organizations adversely – and occur quite frequently, as any look at the news headlines can attest. In 2012 alone, there was an estimated US$186 billion in global economic losses from natural disasters and other catastrophes. Sadly, 2011 saw even greater financial losses and fatalities. And 2013 has brought devastating tornadoes in the Midwestern United States, massive flooding in Central Europe, continued unrest in the Middle East, a monster typhoon in the Philippines and other crises.


Yet the reality is that many companies never see or fully consider potential threats to their business until the damage has been done. During such times, business can come to a standstill. Even routine activities such as employees coming to an office to work, accessing the corporate network, or meeting in person may not be possible in such circumstances. The impact on businesses can be staggering: Personal injury, the destruction of property, lawsuits due to alleged negligence, decreased production, missed service deadlines and delayed product announcements are only a small sampling of the unfortunate occurrences that can plague a company during a crisis.

Many of the aforementioned risks are evolving and presenting growing business continuity and disaster recovery challenges for businesses, particularly with regard to maintaining critical IT systems and processes. This is the focus of the third edition of Protiviti’s Guide to Business Continuity Management: Frequently Asked Questions. Our intention is to help companies get ahead of these risks by building sustainable BCPs.

Among the key areas covered in this guide are:

- The regulatory environment
- Business continuity strategy design
- Plan development and strategy implementation
- Training and awareness
- Testing and maintenance
- Compliance monitoring and auditing
- Industry-specific programs for business continuity management (BCM)

No one can predict when the next disaster or business disruption will strike; the only certainty is that something untoward will happen, at some time. Companies can prepare for the inevitable by making BCM a central part of their enterprise risk management efforts. At Protiviti, we take pride in being risk-intuitive and hope this guide will be useful toward that end.

Protiviti
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 significant loss to the enterprise.

BCM consists of three core elements:

a. **Crisis management and communications** 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 through effective planning, leadership and communication protocols.

b. **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.

c. **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. Some of this confusion is the result of differences in the BCM lexicon used by various industry and regulatory groups. A number of terms are similar to BCM, but with slightly different meanings. For example:

- **Disaster recovery** is a term reserved for the recovery and resumption of critical technology assets in the event of a disaster. Disaster recovery can include tasks such as resuming individual systems or recovering all critical aspects of the IT environment. Disaster recovery is a component of an overall BCM program.

- **Resumption planning** is reserved for the recovery of critical business functions separate from IT. Examples of resumption planning include resuming call center functions, manufacturing processes or payroll operations after a serious incident has occurred.

- **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. Is there a best practice approach to business continuity planning (BCP)?

This question is often asked and while vague, 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 varies):

- **BCM program design and deployment** – including the 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 (BIA)** – 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 and driven by the results of the BIA and risk assessment.
- **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.

4. What BCM elements are included in ITIL – specifically, IT service continuity management?

The IT Infrastructure Library, or ITIL®, is an IT service management (ITSM) framework that provides guidance for applying disciplined processes to manage IT services. ITIL publications generally define how ITSM can be applied, and the framework can be customized to fit the needs of a specific organization.

The ITIL (version 3) consists of five primary publications based on the five ITIL life cycle phases: service strategy, service design, service transition, service operation, and continual service improvement.

IT service continuity management is one of the processes addressed in the service design life cycle phase. Other processes described in this ITIL volume include:

- Service catalog management
- Service level management
- Capacity management
- Availability management
- Information security management
- Supplier management
From an ITIL perspective, continuity management is the process by which plans are put in place and managed to ensure IT services can recover and continue should a serious incident occur. ITIL goes beyond reactive measures to address proactive measures as well, with the objective of reducing the risk of a service disruption.

ITIL’s service continuity management process focuses on the recovery of the business services being delivered by the IT function, not just the IT infrastructure used to deliver IT services. For that reason, many businesses utilize the ITIL framework guidance 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.

ITIL service continuity management involves many of the basic steps outlined in other BCM standards and methodologies including:

• Prioritizing core business processes and IT applications that must be recovered by conducting a 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

5. What is the relationship between business continuity and enterprise risk management (ERM)?

In its Enterprise Risk Management – 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 the entity’s 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 a core aspect within ERM.

OVERVIEW OF THE REGULATIONS AND STANDARDS LANDSCAPE

6. How should regulations and standards shape the development of a BCM program?

Since 2001, nearly every BCM regulatory requirement or standard has been enhanced or expanded to address increases in the threat environment, as well as focus on corporate governance.

Both regulations and standards are used by organizations as a guide to support an approach for BCM program development, or as a measure of adherence or a tool to assess process maturity. While regulations and standards often provide guidance on required or suggested areas of focus and approaches to BCM, they rarely dictate content-specific items, formats or levels of detail in planning documentation.

In our view, the universal theme we have seen across various regulations and standards typically encourages organizations to consider their continuity-specific risks carefully and make reasonable judgments on the composition and content of their BCM programs.

The next few questions address the more common regulations and standards in the marketplace.

7. What are ISO 22301 and ISO 22313?

ISO 22301:2012 Societal security – Business continuity management systems – Requirements was published by the International Organization for Standardization (ISO) in June 2012, with the intention of establishing an international standard that would assist organizations in better preparing for disasters and increasing overall resilience. As with other ISO standards, it applies the Plan, Do, Check, Act (PDCA) model, but is focused on the business continuity life cycle. Likewise, organizations seeking certification of their BCM program can do so by engaging an accredited third-party certification group. The ability to certify and provide a degree of assurance to third parties (e.g., clients, management, regulatory bodies) with respect to the structure of an entity’s BCM program is an attractive proposition for a number of organizations.

With the introduction of ISO 22301, BS 25999-2 (developed by the British Standards Institution [BSI]) has essentially been replaced. In fact, many view ISO 22301 as an upgrade because it places greater emphasis on the understanding of requirements, setting of objectives, and the measuring of performance. Ultimately, organizations that have previously aligned their programs with the BSI standard should have a fairly straightforward transition to ISO 22301.

ISO 22313:2012 Societal security – Business continuity management systems – Guidance complements ISO 22301 by clarifying the concepts introduced in ISO 22301 and providing explanations and examples to assist organizations during deployment. While ISO 22313 does not introduce any new concepts or requirements, it provides a better sense of what an ISO 22301 BCM program looks like and how it can be applied.

ISO 22301 was designed to be sufficiently generic and applicable to all types of organizations. The principles will appear familiar to seasoned BCM professionals and how the requirements are ultimately applied will depend on the risk environment in which the organization operates, and management’s goals and objectives.
8. What is NFPA 1600?

The National Fire Protection Association (NFPA) is a standards-making body headquartered in Massachusetts. Their most popular work is the Life Safety Code NFPA 101, which 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 1995 and most recently updated in 2013. 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). When first published, this standard was three pages long and included elements of prevention, preparedness, response and recovery. Today, NFPA 1600 is a complete emergency management and business continuity standard that includes guidance on crisis communications, emergency operations center (EOC) management, and family preparedness.

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 (H.R. 4830) to direct the U.S. Secretary of Homeland Security to develop and implement a program to enhance private sector preparedness for emergencies and disaster preparedness. The U.S. Department of Homeland Security (DHS) initiative is also known as “Ready Business” and includes its own endorsement of NFPA 1600. In 2009, NFPA 1600 received designation and certification as anti-terrorism technology under the SAFETY Act, which was enacted by Congress as a part of the Homeland Security Act of 2002.

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

In 2010, the NYSE and National Association of Securities Dealers (NASD) made a rule change to adopt Financial Industry Regulatory Authority (FINRA) Rule 4370, requiring members and member organizations to create and maintain BCPs and provide FINRA with emergency contact information. FINRA Rule 4370 supersedes the prior business continuity rules NYSE Rule 446 and NASD Rule 3510.

The FINRA requirement mandates a plan that addresses:

- 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
- Assessment of critical business constituent, bank and counterparty impact
- Regulatory reporting
• Communications with regulators
• How the member or member organization will assure customers have prompt access to their funds and securities in the event the member determines it is unable to continue its business

FINRA Rule 4370 states that:

Each member must address the above-listed categories to the extent applicable and necessary. If any of the above-listed categories is not applicable, the member’s business continuity plan need not address the category. The member’s business continuity plan, however, must document the rationale for not including such category in its plan. If a member relies on another entity for any one of the above-listed categories or any mission critical system, the member’s business continuity plan must address this relationship.

The rule further requires a member of senior management (registered principal) to approve the plan on an annual basis.

10. Does the Health Insurance Portability and Accountability Act (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:

• Risk analysis (required)
• 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 designated as either required or addressable. In terms of HIPAA, addressable does not equate to optional. Addressable simply means the organization must assess whether the requirement makes sense in their environment; if not, then a similar provision should be in place to act as a compensating control with the intent of performing the same type of safeguard. According to the U.S. Department of Health and Human Services (HHS), decisions made regarding addressable specifications must be documented.

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

A common misconception is that the HIPAA requirements are focused exclusively on IT. Although most of the Final HIPAA Security Rule can be perceived to be focused heavily on IT, PHI is found in many forms, and the Emergency Mode Operation plan is not truly an IT issue at all. Rather, this requirement addresses how the provider will continue to protect PHI if normal IT controls are not available or functioning appropriately, which could have a significant impact on the organization's ability to continue operations in an acceptable manner, if not handled appropriately.
11. Does The Joint Commission require BCM for hospitals?

The Emergency Management standard for hospitals clearly states the healthcare organization (provider) must have an emergency management program that addresses continued patient/resident/client care in the event of an emergency situation. Healthcare organizations that offer emergency services or are designated as disaster receiving stations must have an Emergency Operations Plan that addresses both external and internal disasters. The requirement includes a Hazard Vulnerability Analysis (HVA) and general and specific responses to types of disasters likely to be encountered by the organization.

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. What guidance does the Federal Financial Institutions Examination Council (FFIEC) provide specific to BCP?

The FFIEC standard is one of the most aggressive standards in the U.S. marketplace. It places significant emphasis on governance, risk assessment, BIA, planning, testing and maintenance requirements. It also contains an entire section related to 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 business continuity. The standard was originally published in 1996, significantly expanded in 2003, and expanded further in 2008. Although still listed in the category of IT examination, the FFIEC standard states, “The business continuity planning process should include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components.”

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

- The effectiveness of BCP depends upon the involvement of the board and senior management;
- BCP involves a continuous, process-oriented approach that includes a BIA, a risk assessment, risk management, and risk monitoring and testing;
- A thorough BIA and risk assessment should form the foundation of a comprehensive BCP;
- The BCP and testing program should be developed on an enterprisewide basis;
- The effectiveness of the BCP should be validated through annual, or more frequent, testing;
- The BCP and test program should be thoroughly documented, evaluated by institution management, independently reviewed by an internal and/or external audit function, and reported to the board;
- The BCP and test program should be updated to reflect and respond to changes in the institution and gaps identified during continuity testing; and
- In addition to the BCP, other financial institution policies, standards, and processes should be integrated into the BCP process.

Interestingly, the FFIEC is not a series of “do's 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, “The BCP should be based on the size and complexity of the institution and should be consistent with the financial institution’s overall business strategy.”
13. What BCM standards exist in the COBIT standard?

Control Objectives for Information and Related Technology (COBIT) has been developed as a generally applicable and accepted standard for sound IT control practices. The standard provides a reference framework for management, users, and information systems (IS) audit, control and security practitioners. COBIT, issued by the IT Governance Institute and now in its fifth edition, provides tools to assess and measure an enterprise’s IT capability across five domains:

- Domain 1: Evaluate, Direct and Monitor (EDM)
- Domain 2: Align, Plan and Organize (APO)
- Domain 3: Build, Acquire and Implement (BAI)
- Domain 4: Deliver, Service and Support (DSS)
- Domain 5: Monitor, Evaluate and Assess (MEA)

Business continuity activities are addressed primarily in the DSS04 domain/process area. The “Manage Continuity” process, as described by COBIT, is to “establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.”

Although COBIT tends to be IT-focused in many process areas, the “Manage Continuity” process incorporates many of the required characteristics that include IT as well as business recovery activities.

14. Are these the only BCM mandates an organization should consider?

There are many more BCM requirements that apply to most companies. For example, Occupational Safety and Health Administration (OSHA) regulations place some crisis management requirements on the majority of U.S. employers. And the Federal Reserve Board, Office of the Comptroller of Currency (OCC), and the SEC worked together to design and publish the Interagency 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.

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 and control standards for business continuity and crisis management include (but are not limited to) the following:

- Prudential Standards
- Gramm-Leach-Bliley Act
- Dodd-Frank Wall Street Reform and Consumer Protection Act
- Commodity Futures Trading Commission
- State Environmental Health and Safety (EHS) regulations
- U.S. Food and Drug Administration (FDA) recall and safety requirements

---

• Critical Infrastructure Protection
• Federal Emergency Management Agency (FEMA)
• National Contingency Plan
• Federal Energy Regulatory Commission (FERC)
• North American Electric Reliability Corporation (NERC)
• State insurance departments
• Local high-rise emergency plan requirements
• USA PATRIOT Act
• Federal preparedness circulars
• Australian Prudential Regulatory Authority
• Homeland Security Act
• Basel Accords
• U.S. Department of Energy
• ISO/IEC 27001, ISO/IEC 27002 and ISO 27031
• National Institute of Standards and Technology (NIST)
• ASIS SPC.1-2009.5 (Organizational Resilience Standard)
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 BCM 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 executed throughout the organization

Sponsorship and BCM program ownership roles typically trend toward organizational elements with visibility across the entire business, as well as experience with risk management. Based on these trends, Protiviti has developed a list of effective sponsors and owners:

- **Finance** – The chief financial officer (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 (HR), or manager of corporate communications.
- **Operations** – The chief operating officer (COO) or a direct report, to include security and EHS.
- **Risk management** – A chief risk officer (CRO) or a designated, qualified business continuity resource within an organization’s risk management function.
- **IT** – The chief information officer (CIO) or a direct report in data center operations (some organizations have a program/project management office where BCM may reside).

As a matter of practice, Protiviti typically recommends that BCM program ownership lie within a business or operational department to provide for enhanced levels of visibility across the organization and to maintain a business risk perspective when developing and implementing continuity strategies.

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

Most organizations that have successfully obtained management buy-in have done so using one or a combination of the following seven 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 continue to be a key driver for business continuity. A number of regulatory requirements mandate senior management participation in the planning process.
3. **Customer demands** – It is becoming more common for customers to require (as part of the contract) that their suppliers and business partners have a BCP in place. A company may hold its suppliers accountable to maintain BCPs and protect its supply chain.

4. **Lessons learned from other companies** – Business continuity actions taken by other organizations (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 also can be true).

5. **Publicize successes and the corresponding value** – BCM 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.

6. **Insurance return on investment** – In certain circumstances, a tested, up-to-date BCM program can have an effect on business interruption insurance premiums.

7. **Internal audit** – Business continuity should be a core risk area identified during the annual risk assessment. Internal audit should be executing BCM- and disaster recovery-specific audits to highlight control gaps.

Unfortunately, it is still common for organizations to realize the importance of developing and maintaining an effective BCM program only after they experience a disruption themselves.

**17. How can executive management be “sold” 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 BCM program is using the results from a risk assessment and a 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. 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

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 implementing a tested BCM 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.” Valuing a BCM plan as
an asset makes the same economic utility sense as prepaid insurance. The BCM program is, in effect, prepaid preparedness. The organization has an up-front investment in an asset that serves to mitigate its risks. The economic value of the BCM plan can be calculated in the same way as projecting the annual economic value of insurance.

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 (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 February 2013, Protiviti published the 2013 IT Priorities Survey report. The survey itself received input from nearly 200 respondents, including CIOs, chief technology officers, chief security officers, and IT vice presidents and directors. “Business Continuity” was considered to be one of four high-priority areas for 2013. This was consistent with similar studies performed by research firms such as Gartner and Forrester.

In the wake of several recent catastrophic natural disasters, business and IT leaders are more mindful than ever of the need to plan for and respond to potential business disruptions and outages, and to evaluate the location of the backup facilities.

Organizations design and deploy business continuity solutions to manage:

- Regulatory risk
- Financial risk
- Reputation risk

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

The next risk category that drives BCM 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 BCPs and protect its supply chain. In the case of 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 an effective BCM program. 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 BCM program. Although the content and format of business continuity policies differ based on existing standards and the culture of the organization, we recommend the inclusion of key elements to drive this process toward an optimal level of maturity and preparedness:

- **Accountability** – Names the executive or executives accountable for 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 a disaster.
- **Analysis** – Establishes the need for and standards associated with risk assessments and business impact analyses (the cornerstones of the planning effort). Also establishes the criteria for the type and scale of incidents to be addressed.
- **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 (e.g., setting objectives, success criteria).
- **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.
- **Reference** – Provides linkage to other standards, guidelines, regulations or policies that the BCM program should consider within the organization.

Taken together, the elements of a business continuity policy mentioned above will assist an organization’s planning team in gathering the necessary support and resources to manage the BCM program effectively.
20. How should an internal business continuity function/planning team be structured?

Most companies assign one individual with ultimate responsibility for coordinating BCP 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 recover the business function or process fully. 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 BCPs remains within the business unit and relies on the time and expertise of the business unit staff. Outside experts, if utilized, 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 of them. All too frequently, companies delegate responsibility for BCP 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.
RISK ASSESSMENT AND BUSINESS IMPACT ANALYSIS (BIA)

21. 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, additional characteristics that may be factored into the prioritization effort are:

- **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?
- **Velocity to impact**: How quickly will downtime lead to a high-severity impact?

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 and velocity to impact. 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.

22. 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** – This includes IT 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 impacts drive the process, whereas in others, qualitative impacts are just as important. Types of impacts that should be considered include:

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

• **Reporting** – Text versus graphs, reports versus presentations. Corporate culture and audience should determine the exact format to ensure BIA 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 BCM project can effectively take place.

23. **Should key vendors be included in the BIA?**

A comprehensive BIA should assess all key inputs and outputs for critical processes. Vendors can be responsible for or considered critical inputs within a process or even a company’s supply chain.

When considering vendors and the supply chain, ask what would happen if any critical element of the supply chain were taken away. How long would the company be able to operate without that particular vendor? The emphasis should be on evaluating the velocity, persistence and response readiness of the enterprise in the event of a loss of any significant aspect of the supply chain. In addition to understanding the impact, the BIA should also understand the vendor’s current continuity capabilities and whether current SLAs are aligned to satisfy management’s risk threshold.

24. **What is a recovery time objective (RTO)?**

An RTO is the time period 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.

25. **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 People-Soft. 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 minimum).

Let’s examine three more examples 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 were 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.

26. 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). For more complex questionnaires, offer a question-and-answer session, as well as a “dry run” opportunity.
- **Keep it short and simple** – People generally 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 or no” questions, or those 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?”

27. **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 IT 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 that companies permanently substitute an abbreviated process for a more in-depth risk assessment and BIA. 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**

28. **What are the key considerations when developing recovery strategies?**

Before a specific strategy option can be developed, the planning team should first understand the following characteristics of the key processes to be recovered: (1) recovery objectives, (2) the order of recovery, (3) interdependencies, and (4) assumptions. These details should have been identified during the BIA and serve as a starting point for strategy development.

After recovery objectives and associated considerations are outlined, the actual strategy can be developed. Whether the focus is on crisis management, business resumption or IT, strategy options are developed based on industry practices and, in some cases, vendor recommendations. Industry trade shows, peer group discussions and experience will all factor into the development of a list of strategy options, as well as high-level implementation and maintenance cost estimates.

To ensure an accurate analysis of potential IT recovery costs in particular (which often represents the largest investment in a continuity program), an organization should consider the development and distribution of a request for proposal (RFP) to qualified vendors. The RFP should outline the system recovery goals of the organization and request that vendors provide options to meet those goals. This process can provide an organization with additional insight into potential recovery options and strategies that may not have been apparent based on the initial analysis. When combined, the BIA and strategy design process will provide the necessary elements of the cost-benefit analysis, which will aid in the decision-making process.

29. **How far apart should primary and alternate sites be?**

In terms of business continuity, a common discussion point 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 IT 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. The events of 9/11 continue to be instructive as the SEC, Federal Reserve and the OCC teamed to issue new regulations focused on lessons learned – one of which was geographic separation. Here is an excerpt from that 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.

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:

• Does the 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?
• Where is the client base located (locally, regionally, nationally, internationally), and what is the criticality of the company’s services during a local or regional event?
• Does the potential (local) alternate location employ adequate risk mitigation strategies to protect against the likely effects of a regional outage (e.g., redundant telecommunications paths, backup power generators, fuel storage, alternate transportation paths), and how long can the company continue to operate in this manner?

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 the 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).
30. What are the key considerations for pursuing an internal versus a third-party recovery solution?

When an organization determines the need to identify business continuity locations for response and recovery purposes, it should invest time and effort to understand clearly the 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.

While the internal versus third-party question is still valid, the dynamic has changed in recent years. Organizations now have additional options that allow them to tailor custom solutions that better address their specific recovery needs. In lieu of a fully outsourced approach, a company may decide to acquire third-party data center space while continuing to own and operate its own disaster recovery equipment. The continuing maturation of cloud solutions has provided a number of additional recovery options. In summary, increased options require a more thorough review of the advantages and disadvantages of available solutions.

That said, the decision to insource or outsource is not purely an economic consideration. The ability to react and adapt to changes in the business, and 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.

- **Cost** – It is often suggested that outsourcing provides a cost-effective alternative to providing recovery services in-house. While outsourcing can be more cost-effective, this is not always the case. Costs can vary widely and will depend on an organization’s overall IT strategy (whether it maintains its own data center space, capacity for its current infrastructure, available IT skill sets, and the type of recovery technologies to be employed). The cost-effectiveness of an insourced versus an outsourced solution rarely can be determined without thorough investigation.

- **Sharing the risk** – When an organization outsources its business continuity solutions, it essentially shares the risk with its 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 potential cost-effective element of outsourcing.

- **Scalability** – The end-state solution needs to be positioned to meet the 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 staff both a primary and an alternate location adequately, whereas a third party may be better positioned to assist with initial recovery operations in the absence of personnel (if they are impacted by the event, or traveling to the alternate site).
• **Maintaining control and accountability** – Just because certain services and activities are provided by a third party, it does not mean the organization is no longer responsible and accountable for them. Rather, make sure the right roles and responsibilities are in place internally not only to manage the vendor, but the service provided as well. Also ensure that the right service level agreements (SLAs) are in place and metrics are used to measure vendor performance.

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

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

Based on lessons learned from 9/11 and storm cycles throughout 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, which are preconfigured with power, environmental systems, IT 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 SLAs and the size of the fleet relative to the subscription base.
- The availability of a location to “park” the trailer.
- A fully functional mobile unit, capable of housing a healthy amount of infrastructure, may require pre-installation of a “hitching post” at the designated recovery location.
- Large, third-party providers that provide recovery space often provide mobile solutions, as well; this additional service can be added at a discount as a “package deal.”
- Like other third-party data center recovery services, mobile recovery testing should occur on a regular basis and be included in the contract.

### 32. 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. While an EOC is a physical location, most organizations understand the difficulty of centralizing their key decision-makers, especially during a disaster scenario. Careful thought should be given to ensuring multiple virtual options are also available (e.g., conference call options, video chat, hard line and cellular options).

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

While the terms continue to evolve and the solutions tend to overlap, the terms “hot site” and “cold site” are still regularly used in the BCM industry. Are these terms or technologies outdated? Yes and no.

New solutions are out there that have, in some instances, superseded these recovery constructs; however, the terms defined below continue to be relevant and vital to many organizations. The following table defines and highlights the differences/implications associated with cold, warm and hot sites (both internal and third-party outsourced solutions).

<table>
<thead>
<tr>
<th>Recovery Option</th>
<th>Description</th>
<th>Pros</th>
<th>Cons</th>
<th>Data Delivery Method</th>
<th>Minimum Recovery Time Supported</th>
<th>Maximum Length of Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal Hot Site</strong></td>
<td>A facility with preplaced server, computer, telecommunications and environmental infrastructure (all in a standby mode).</td>
<td>Guaranteed availability and unlimited testing. Always under control of the organization.</td>
<td>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.</td>
<td>Tape Backup</td>
<td>17 Hours</td>
<td>Unlimited</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Disk Backup Replicaion</td>
<td>7 Hours</td>
<td>Unlimited</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Replication</td>
<td>Real Time – 2 Hours</td>
<td>Unlimited</td>
</tr>
<tr>
<td><strong>External Hot Site</strong></td>
<td>A third-party facility with preplaced server, computer, telecommunications and environmental infrastructure (all in a standby mode).</td>
<td>Can be purchased as a service, no additional capital expense is required. Multiple recovery locations provide increased protection.</td>
<td>No guaranteed availability. Limited usage.</td>
<td>Tape Backup</td>
<td>24 – 72 Hours</td>
<td>30 Days</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Disk Backup Replicaion</td>
<td>7 – 36 Hours</td>
<td>30 Days</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Replication</td>
<td>Real Time – 24 Hours</td>
<td>30 Days</td>
</tr>
<tr>
<td><strong>Internal Warm Site</strong></td>
<td>A raised-floor facility with full environmental infrastructure. Limited server infrastructure and communication lines are also typically present.</td>
<td>Provides guaranteed space and avoids the purchase of recovery hardware.</td>
<td>Requires an investment in floor space, infrastructure and communications. Relies on the shipment of third-party hardware.</td>
<td>All</td>
<td>5 – 20 Days</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>
While the use of a cold, warm or hot site may still be a viable alternative, many organizations have designed their technology infrastructure across multiple data centers, where key systems can operate at any given time across a particular set of locations. Such a solution may be required for those organizations that have a very low tolerance for system latency or technology disruptions.

### 34. What are key recovery considerations when negotiating a contract for a hosted solution or disaster recovery support (e.g., hot site contract)?

IT hosted solutions are becoming far more prevalent in today’s business environment. As organizations consider the advantages and disadvantages of “transferring risk” to a third party, or relying on a third party to support the organization in the event of a disruption (e.g., hot site), Protiviti recommends addressing the following considerations:

- In advance of the vendor selection process, develop and weigh selection criteria.
- To execute a focused vendor selection process, use a Request for Information (RFI) to select three finalists, and an RFP to select a partner.
- Based on a BIA, define detailed recovery objectives and associated recovery configurations. Share recovery strategy configurations with potential technology partners (following the RFI process).
- When considering a third-party recovery contract, consider the performance needs of the organization’s application portfolio.
• In the case of a hot site contract, consider a shorter 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 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.

• Integrate data backup solutions (with an RPO of less than 24 hours and an RTO of less than 48 hours) with the solution provider to take advantage of economies of scale.

• Include terms allowing termination of the contract in the event a similar internal capability is developed.

35. How is advancement in technology changing disaster recovery planning considerations?

Today’s technology delivery models have advanced and include X as a Service (XaaS) (e.g., infrastructure, application, platform) to provide core infrastructure, business applications, development platforms, and software delivery provided by third-party organizations or internally via private cloud. While there is an element of resiliency built into these delivery models due to redundant locations and more high availability architecture, it is still important to have a plan that addresses what happens when one of the redundant nodes upon which business services are built becomes unavailable. Additionally, third-party providers or alternate company locations may be located geographically in different regions than main company operations, so the risk assessment must be adjusted accordingly. From a service perspective, it is important to establish service-level expectations and agreements that ensure accountability is placed appropriately with both the service provider (vendor/partner or internal) and internal teams, and that communication channels are adequately defined to facilitate recovery operations when an event occurs.
36. Is software necessary to develop a BCP?

No. The majority of organizations elect to develop BCPs 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. In addition, a number of organizations are using pre-existing tools such as SharePoint to organize, share and maintain BCPs.

Although software solutions can add value, management should address three important considerations 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.

37. What is the difference between crisis management and crisis communications?

Crisis management is an entity’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, EHS, HR, 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 a product recall to a 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, HR 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 not deemed credible. However, the general counsel advises the chief executive officer (CEO) that it’s not worth taking the chance. The CEO decides to close down all facilities. The executive vice president of HR decides the organization
needs to pay employees regardless. The corporate controller notes the financial impact of the decision. The CRO 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.

38. 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 illustrated below, Andy is responsible for calling Barbara, Connie and Duke. Each of those three people 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 email 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 email, text 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.

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

Yes. We recommend the BCP focus on the specific content necessary to enable effective response and recovery activities. The BCP 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 “break the plan” and identify areas for improvement. Note: Effective exercise of continuity plans requires careful planning and execution.
TRAINING AND AWARENESS

40. 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 simply implies that one possesses knowledge of the BCM program or related activities. For example, the company may distribute an email communication pointing employees to an internal repository that houses BCP-related documents and ask that they familiarize themselves with such documents. Awareness does not necessarily imply that one has knowledge of “how” to execute the BCP. Training, on the other hand, is a stricter regimen that pertains to receiving specific instruction on how to execute BCP activities, and solidifying that instruction with actual proficiency exercises. This instruction may be provided through classroom, computer-based, test-based, and/or instructional guides and templates.

Some organizations utilize BCP testing exercises as a means of training their employees, but beware of the potential pitfalls of doing so. It is not uncommon for testing exercises to reveal flaws or weaknesses in the BCP program that need to be addressed. Thus, if the organization is simultaneously training its employees on a BCP activity that will be updated later, this could lead to confusion about which procedure to follow during an actual disaster event.

While training should involve the actual execution of business continuity testing activities necessary to evaluate the effectiveness or capabilities of the plan, awareness may be provided through workshops, instruction manuals, email communication or other ad hoc communication methods. Awareness is an inherent part of training; however, training is not necessarily part of awareness.

41. What are some successful business continuity training approaches?

The best approach to business continuity training is to review the formal 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 gap analysis to determine training content. Organizations should remain cognizant that certain individuals will be responsible for executing various BCP activities as part of the multifaceted program.

For example, a vice president of IT may be a member of the company’s crisis management team, responsible for initiating an IT disaster recovery response and serving as a building evacuation leader. As such, the training regimen that an organization chooses to employ should address the roles and responsibilities employees will be performing throughout all relevant components of the company’s program.

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 customized training is necessary. Not only do business continuity programs differ greatly by company, but the overall objectives also 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 organizations 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.

42. What are the available certification options?

A variety of organizations exist that offer training, resources, and even certifications. However, only a handful of these are recognized by practitioners as being accredited. For instance, four organizations that offer BCM certifications recognized worldwide include:

1. The Disaster Recovery Institute International, or DRI International (also known as DRII)
2. The Business Continuity Institute (or BCI)
3. The Business Continuity and Disaster Recovery Education and Certification Institute (or “The BCM Institute”)
4. International Organization for Standardization (ISO)

**DRII:** The DRII offers a number of professional certifications, specialty certifications, and vendor certifications:6

**Certified Professionals**

- **Associate Business Continuity Planner (ABCP):** This certification is geared toward those who are new to the industry with limited or entry-level proficiency in BCP. Obtaining this certification requires passing the qualifying exam and completing the application process, which must be approved by DRII.

- **Certified Functional Continuity Professional (CFCP):** The CFCP level of certification is for individuals who have demonstrated business continuity knowledge and working experience in a specific skill or focus (e.g., BIA). This certification is achieved by passing the certification exam 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 be approved by the DRII Certification Commission.

- **Certified Business Continuity Professional (CBCP):** The CBCP is one of the most widely recognized business continuity certifications. This certification is achieved by passing the certification exam and submitting an application documenting at least two years of experience in five of the 10 categories of DRII professional practices. The application must include references and be approved by the DRII Certification Commission.

---

6 For more information on DRII certifications, go to: [www.drii.org](http://www.drii.org).
• **Master Business Continuity Professional (MBCP):** The MBCP is DRII’s highest level of certification and is reserved for individuals with significant demonstrated knowledge and skill in the business continuity/disaster recovery industry. The certification is tailored to individuals with at least five years of industry experience and demands a high level of industry commitment, as well as additional and continual enhancement of knowledge and skill level. Applicants must pass the certification exam and a master case study exam, and submit an application documenting at least five years of experience in seven of the 10 categories of DRII Professional Practices. The application must include references and be approved by the DRII Certification Commission.

**Certified Specialists**

• **Certified Business Continuity Auditor/Certified Business Continuity Lead Auditor (CBCA/CBCLA):** The CBCA certification is for those professionals who can verify the effectiveness of an organization’s business continuity program against the landscape of standards, guidelines and industry regulations. Generally, applicants have two years of experience, must attend a prerequisite course, pass the qualifying exam, and provide references to verify the candidate’s experience. The CBCLA certification is very similar, except that it requires five years of relevant experience. The application must include references and be approved by the DRII Certification Commission.

• **Associate Public Sector Continuity Professional (APSCP)/Certified Public Sector Continuity Professional (CPSCP):** The APSCP certification supports entry-level proficiency with some knowledge in Public Sector Recovery planning. Applicants of the APSCP certification only need to pass the qualifying exam and complete the application process. Qualified CPSCP applicants should have two or more years of experience and must be able to demonstrate specific and practical experience in at least five of the subject-matter areas of the DRII Professional Practices. In addition to passing the qualifying exam, the CPSCP application must include references and be approved by the DRII Certification Commission.

• **Associate Healthcare Provider Continuity Professional (AHPCP)/Certified Healthcare Provider Continuity Professional (CHPCP):** The AHPCP certification supports entry-level proficiency with some knowledge in healthcare continuity planning. Applicants to the AHPCP certification only need to pass the qualifying exam and complete the application process. Qualified CHPCP applicants should have two or more years of experience and must be able to demonstrate specific and practical experience in at least five of the subject-matter areas of the DRII Professional Practices. In addition to passing the qualifying exam, the CHPCP application must include references and be approved by the DRII Certification Commission.

**Certified Vendor**

• **Business Continuity Vendor Certification (BCVC):** The BCVC certification was established to provide those individuals who, as vendors, recognize the importance of business continuity best practices in the field, but are not necessarily working planners. BCVC applicants must pass the qualifying exam and complete the application process.
BCI offers a “Certificate of the BCI,” which can only be achieved by passing an exam that tests a candidate’s knowledge of the prescribed body of knowledge: the Good Practice Guidelines.  

The BCM Institute offers the following certification options:

- Business Continuity Certified Planner (BCCP)
- Business Continuity Certified Specialist (BCCS)
- Business Continuity Certified Expert (BCCE)
- Disaster Recovery Certified Planner (DRCP)
- Disaster Recovery Certified Specialist (DRCS)
- Disaster Recovery Certified Expert (DRCE)
- Business Continuity Certified Auditor (BCCA)
- Business Continuity Certified Lead Auditor (BCCLA)
- Crisis Management Certified Planner (CMCP)
- Crisis Management Certified Specialist (CMCS)
- Crisis Management Certified Expert (CMCE)

To receive certification, each candidate must satisfy all educational and experiential requirements established by The BCM Institute, and successfully pass the associated qualifying examinations for each certification level.

Additional organization-level and individual certification options are available through the ISO 22301 standard.

43. What are the available BCM education options?

A growing number of educational opportunities are presented by business continuity-related organizations. As discussed in the answer to the previous question, the DRII, The BCM Institute, and BCI offer a wide variety of professional, practice-oriented training covering all aspects of the BCP 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 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, Contingency Planning and Management (CPM), and BCM World Conference and Exhibition.

Above all, participation in testing and exercises often proves to be the most useful training for response and recovery team members. This includes coordinated simulation exercises, with participation by local police and fire department personnel.

---

7 For more information on BCI’s Good Practice Guidelines, go to: [www.thebci.org](http://www.thebci.org).
8 For more information on The BCM Institute’s certification options, go to: [wwwbcm-institute.org](http://www.bcm-institute.org).
44. What are the prevailing practices regarding the storage of BCP documentation?

Depending on the size, complexity and geographic dispersion of the organization, plan storage techniques can range from printed hard copy plans stored off-site, to sophisticated and highly customized BCM software that can be accessed by stakeholders from anywhere in the world. In smaller organizations, up-to-date plans (with version control identifiers) are printed and disseminated to personnel named in the BCP.

Employees may also receive copies of emergency response procedures (e.g., evacuation procedures, first aid reminders), or awareness displays may be placed in high-traffic areas such as cafeterias or break rooms. Obviously, as plan materials are updated or become out of date, they must be replaced and/or disseminated to employees again. Key members of business continuity teams from smaller organizations typically have copies of the plan available at home, at work, and pre-positioned at recovery locations.

BCP software, knowledge management platforms (e.g., SharePoint), and off-site file servers have resulted in fewer hard copies and the growing use of electronic planning material in larger, more complex organizations. This technology typically facilitates plan segmentation, such that team members only receive 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) as a backup measure.

There is no “one size fits all” BCM documentation storage approach; that is, not every organization requires the “Cadillac” BCM software package. But by the same token, only distributing printed hard copies of a BCM plan may not be the right choice either. Management should carefully evaluate the BCM risks and challenges inherent to their organization and select a documentation storage solution that will work best.

45. How often should business continuity-related documentation be updated and how should the organization keep the plans current?

In general, business continuity documentation should be reviewed and updated at least annually. 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; organizational restructuring; or the implementation of new technology, which may impact the current plan. Key review and update activities to consider include:

- Business unit and associated function listing and validation of criticalities as determined in the BIA, including reassessment of RTO and RPO figures
- Risks/threats that may impact key business operations
- Business unit/function dependencies/interdependencies (IT and non-IT)
- Opening/closure of key office locations
- Key employee/vendor contact information (e.g., call tree)
• Resource requirement matrices
• Data, intellectual property and documentation storage locations
• Changes to regulatory/reporting requirements

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, which tend to focus more on recovery of an individual process or set of processes.

Internal audit should enforce a defined review and plan maintenance schedule, as defined in the BCM policy, and can assist with validating plan completeness and accuracy.

HR information, to include contact information, should be reviewed quarterly.

Regardless of the process used to maintain BCPs, maintenance should be based first on a defined schedule. If an organizational change management process is in place, BCM should be integrated into this program.

46. How often should the BCP 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 once or twice a year; however, this can be increased due to such factors as:

• Changes in business processes
• Changes in technology or facilities
• Changes in BCP team membership
• Changes in executive management
• Anticipated or planned 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. Lastly, IT environments change very rapidly. Plan coordinators should ensure IT disaster recovery procedures are updated in tandem with established technology change management procedures.

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.9

---

9 Note: The information in the answer to Question 46 was authored by Protiviti and originally published on the ISACA website (2003).
47. What are the available testing options?

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

<table>
<thead>
<tr>
<th>Test Type</th>
<th>Description and Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desk Check (a.k.a. Boardroom Style or Tabletop Testing)</td>
<td>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.</td>
</tr>
<tr>
<td>Simulation (a.k.a. Full-Scale Interdependency Testing and Walk-throughs)</td>
<td>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.</td>
</tr>
<tr>
<td>Procedure Verification Test (Business Function Testing)</td>
<td>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.</td>
</tr>
<tr>
<td>Communication (Call Tree Testing)</td>
<td>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.</td>
</tr>
<tr>
<td>IT Environment (System and Application) Walk-through</td>
<td>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 time-line and documented application interdependencies. This scenario exercises “active-active” and “active-backup” IT continuity models.</td>
</tr>
<tr>
<td>Alternate Site Testing</td>
<td>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.</td>
</tr>
<tr>
<td>End-to-End Testing</td>
<td>A test of alternate site facilities, to include both business and IT. An end-to-end test differs from an alternate site test in that critical suppliers/business partners and customers – internal or external – are included within the scope. This test typically validates connectivity to the business’s production site.</td>
</tr>
</tbody>
</table>

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. That is, choose a likely risk to which the organization may be vulnerable. And if the organization is new to BCP testing, start small. As the organization’s business continuity process matures, increase the size and complexity of the test. For example, management could start by having “tabletop” discussions regarding various recovery scenarios with the business. From there, management could enhance the test to include a coordinated, sample-based recovery of applications/processes/departments, and ultimately, graduate to performing a fully simulated test involving restoring major components of the business and the supporting IT environment at once.
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 the Monopoly board game, using “chance cards” to insert unanticipated variables into the test process. It is not uncommon for a localized or regional disaster (e.g., tornado or hurricane) to render key BCM team members out of communication. Consider inserting realism into testing exercises by asking key personnel to “sit out” and observe tests to see how the rest of the team reacts to that situation. These are just a few ideas to add realism and keep exercises interesting.10

48. 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, such as:

- 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
- Walk-throughs 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 after major deficiencies are noted)
- Repeat until noted issues are resolved satisfactorily, as per internal audit’s observations

---

10 Note: The information in the answer to Question 47 was authored by Protiviti and originally published on the ISACA website (2003).
49. Describe the connection (if any) between Sarbanes-Oxley and business continuity.

When the Sarbanes-Oxley Act (SOX) was passed in 2002, management and auditors alike struggled with defining the scope of business continuity as an internal control related to financial reporting. However, as SOX compliance became more commoditized for public companies over the past decade and as the Public Company Accounting Oversight Board (PCAOB) issued additional guidance (e.g., Auditing Standard No. 5), management and external audit firms alike have been able to come to a middle ground on this topic.

The most common IT general controls in this area relate to system/data backups and periodic restorations. In other words, external auditors mainly want to gain comfort that management is backing up their key financial systems on a regular basis, and have methods of detecting and addressing backup failures should they occur. Additionally, some of the external audit firms also want to confirm that management can restore systems or critical files from backup media, should the situation call for it. This can be evidenced by performing and documenting targeted restoration activities and proving that backed-up data is accessible and intact.

Regardless of how BCM and IT disaster recovery topics are treated within regulations such as SOX, most executive managers continue to advocate business continuity-related processes because they’re viewed as good business practices. For service-oriented organizations (e.g., payroll services, business process outsourcing, cloud computing) business continuity is a topic that remains very near the top of the list when clients perform their annual vendor audits or issue related audit questionnaires.

50. 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 BCM program weaknesses
- Compliance auditing, based on a defined internal policy

Organizations looking for a baseline against which to rate program maturity can utilize tools such as a Capability Maturity Model (CMM), which includes the following levels:

1. **Initial (ad hoc)** – The starting point of a new BCM process.
2. **Repeatable** – The BCM process is documented sufficiently; BIA completed and baseline plans have been developed.
3. **Defined** – The BCM process is a standard business practice; baseline plan testing is performed.

4. **Managed** – The BCM process is quantitatively managed in accordance with agreed-upon metrics.

5. **Optimizing** – The BCM process includes process optimization/improvement components.

**51. 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 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 firms, 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 IIA published *Global Technology Audit Guide (GTAG) 10: Business Continuity Management*, which states that BCM-related audit activity should take place “on a regular basis” and can include:

- Playing 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).
- Evaluating the BCP and disaster recovery plan during planning and development (internal auditors have a thorough understanding of the business and the individual functions and interdependent relationships, and contribute to the BCP process).
- Reviewing the proposed business continuity and disaster recovery plans for design, completeness and overall reasonableness/viability.

**52. What is the optimal role for internal audit in the BCM process?**

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 salesperson** – 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 anomalies are addressed.
- **Audit the BCM program** – Regarding internal and industry standards/requirements, internal audit is positioned to review the planning process and strategies to ensure compliance. Internal audit also can develop recommendations to address opportunities for improvement.
• **Management communication** – Internal audit can formally communicate program status and capability to management to ensure expectations are met and that the BCM program continually matures over time.

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 adviser 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 due to the availability of training, as well as the day-to-day mindset of managing risk – continuity or otherwise.

53. **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 one or more of the following approaches:

• Make vendor inquiries and ask if they comply with the key provisions found in the business continuity policy. This is especially pertinent when a vendor plays a very specific role in the organization’s recovery plan procedures and/or supply chain. A vendor’s detailed responses will usually reveal the adequacy of its BCM planning.

• Request a copy of the vendor’s BCP and perform a review. Most organizations may be hesitant to provide such documentation, especially in the event that it contains sensitive or proprietary information; however, they may be willing to provide redacted versions to satisfy client demands.

• Request a recent copy of the vendor’s Statement on Standards for Attestation Engagement No. 16 (SSAE16)/Service Organization Controls 1 (SOC 1) report validated by an accredited firm in accordance with the requirements of the American Institute of Certified Public Accountants (AICPA). A SOC 1 report will often contain information related to an organization’s business continuity preparations specific to the service being provided.

Alternatively, depending on the nature of the services being provided, a vendor may pursue a SOC 2 report. SOC 2 reports often will include business continuity details as required by the Availability Trust Service Principle. If issues were noted by the service auditor in either of these types of SOC reports, management may want to further inquire as to the remediation activities undertaken to address identified gaps.

• 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 operations (to include an interdependency analysis)?
  - Are you comfortable your company is adequately prepared to handle planned and 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)?

– 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 those facilities from your primary operating site?

– Does your organization maintain a crisis communications plan, which includes having designated people trained to speak to the media?

– Has your organization ever tested its BCP?

– Does your organization offer a formal training and awareness program to familiarize employees with your BCP?

In the absence of adequate BCM programs, companies may need to consider mitigating controls and/or recovery strategies, or alternate vendors should be identified for key products and services.
SOCIAL MEDIA CONSIDERATIONS

54. Should social media be a component of an organization’s business continuity program?

Social media is a compendium of many highly accessible media – corporate blogs, video-sharing sites such as YouTube, social networks like Facebook, micro-blogging tools such as Twitter, rating/review sites, wikis allowing many authors to simultaneously edit and create a source of knowledge, and crowdsourcing, among others. These communication channels present significant opportunities for companies to connect in real time with customers, the media, suppliers and others, especially in times of crisis.

Social media also provides effective tools (e.g., online training via social platforms) for educating employees about business continuity management practices, as well as keeping them informed in the event of an emergency (e.g., through Twitter or Facebook updates). Many organizations have already made the use of social media an integral part of their business continuity programs for facilitating both internal and external communications.

55. What are the risks of using social media to support a business continuity program?

Communicating through social media channels presents a range of potential risks that companies need to monitor, in general. Vigilance about information sharing through social media is even more important during a crisis event due to the sensitive nature of communications. However, when an organization is operating in a crisis mode, communications tend to be streamlined and may not incorporate the same level of controls as would be applied during normal operations.

Following is a list of potential social media-related risks that companies should be aware of, particularly during a crisis event:

- **Compliance violations** – There is a risk of sharing information that results in the violation of applicable laws and regulations, including infringement of trademarks and copyrights, data security issues, employment issues, violations of privacy rights, and mismanagement of electronic communications that retention regulations or e-discovery requirements may impact.

- **Reputation loss** – Because consumer opinions can spread quickly through social media, companies need effective response plans when a crisis occurs. Self-inflicted reputation damage may result from inappropriate employee behavior; setting unrealistic product or customer service expectations; rogue tweets of inappropriate messages intended for internal or personal use; or the inability to measure up to the openness, straight talk and transparency expected by customers and prospects seeking to engage with the company. Customers or other parties can use social media to say negative things about the company and, if the company doesn’t engage or isn’t paying attention, it won’t be able to manage the potential fallout – and may overlook necessary improvements to products and processes.

- **Safety loss** – Release of information about company responsibilities, travel plans and other employee activities can create the risk that outsiders will use that information to the detriment of employees’ personal safety.
56. What are some best practices for monitoring social media during a crisis event?

The following is a summary of various best practices for mitigating, preventing and remediating a social media public relations crisis:

- Validate social media with sponsorship from executives in the organization.
- Be transparent with the company’s actions to the general public, employees and other stakeholders. Showcase not just what the company does, but why and how an action is executed.
- Protect the organization’s social media investment by promptly responding in a social media crisis.
- Increase staffing within social media channels and address any issues in real time. 24/7 monitoring may be necessary to dispel damaging information, gauge tone of conversations, and engage with the masses.
- Ensure consistency in all the company’s crisis response statements.
- Resolve conflicting messages. Make sure a marketing campaign is not contradicting the crisis messaging.
- Allow for dissent. A clear set of house rules sets guidelines for what is appropriate. There needs to be a consistent standard for the removal of posts.
- Watch for shifting narrative in the community and respond.
- Develop relationships with detractors.
- Cultivate proactive conversations with influencers.
- Document all engagement, conversations and other efforts during a crisis.
- Build a framework for handling a social media crisis:
  - Determine the importance of the issue. Determine if the issue is a conflict or incident vs. a full-blown crisis.
  - Select a response team. Combine the forces of legal, compliance and public relations to form messaging. Designate one person or team to be at the helm.
  - Establish a messaging approval process and determine the chain of escalation.
  - Document methods of outreach. Determine the methods for engaging online, offline, publicly, privately, via email and phone, and so forth, and establish dedicated service lines for each channel.
  - Focus strategies on objectives and outcomes. Seek to address the root cause of an incident and not just attend to the reaction.
LARGE-SCALE DISASTERS AND POTENTIAL PANDEMIC EVENTS: 
LESSONS LEARNED

57. What are some of the common lessons learned from large-scale natural disasters that organizations should be aware of when developing their own BCM programs?

• **Availability of employees** – Most business continuity planning assumes employees will return to work to support business recovery; however, employees without a strong economic incentive who are forced to evacuate an area for an extended period are less likely to return. 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.

• **Early evacuation** – It is not uncommon for people to spend 24 hours or more trying to leave a pending disaster area. When a hurricane or other disaster 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 near the business recovery site and that they may retrieve any necessary materials and equipment before they evacuate.

• **Government support** – While government support can provide some immediate relief and assistance during a large regional disaster, businesses cannot rely on government aid for long-term business resumption, and it is not a substitute for solid business continuity planning. 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.

• **Supporting infrastructure services** – Basic services such as utilities, trash collection and publicly accessible healthcare can be interrupted for an extended period. Frequently, following regional disasters, some organizations recover their own operations only to find the supporting infrastructure – sanitation, utilities, mass transit, telecommunications, hotels, restaurants, and so on – are not as well prepared. Determine in advance how the organization will compensate for the absence of such services, including contracting with third-party vendors in the private sector to provide these basic services to employees until supporting infrastructure services resume.

• **Permanent relocation of business** – In the weeks following a large-scale disaster, basic services can be delayed for an extended period 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. Identifying a “Plan B” location not only allows the organization to pre-position resources, train staff at that location, and facilitate an orderly relocation of affected employees, but also lets it acquire potentially limited resources at that location before the inevitable post-disaster rush to find scarce goods and services.

• **Distance to alternate location** – In recent years, there have been several surveys 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, recent disasters have 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 locations are not fully outfitted as recovery sites. See the answer to Question 29 for additional discussion on this topic.

- **Decentralize critical processes** – Companies located in disaster-prone regions whose critical processes (e.g., information systems, call centers, distribution centers, manufacturing) are 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.

- **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, and shipping providers – which occurs after a massive event, or they fail to consider the difficulty in obtaining custom or highly specialized equipment, such as in the manufacturing industry. 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. Businesses also must anticipate and plan for secondary damage (e.g., flooding, fires, and theft). This includes obtaining the appropriate insurance to assist with recovery.

- **Actionable plans** – When disaster strikes, it is not uncommon for businesses to ignore their plans. This is because plans might be too general, overloaded with detail, or 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 the information is complete, accurate, comprehensive and actionable. This will help ensure the plan reflects the current state of the business and can serve as a useful guide during a disaster and its aftermath.

- **Emergency funds** – Disaster events prove that the old adage “cash is king” is still correct. In the absence of 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 cash will be made available in a secure fashion to meet the needs of the 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.

- **Communications** – Communication efforts must be streamlined before an event occurs 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 or need to communicate with other cities. To prepare for disruption of local infrastructure, businesses should identify major 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, and other correspondence are all valuable exercises that provide a baseline for senior management to use as they make decisions following an event.

- **Planning for long-term outages** – It is common for companies to plan for only a 30-day outage of the primary facility. However, following Hurricanes Katrina and Rita, Superstorm Sandy, and other recent crisis events, 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 affected areas may be impossible for an extended period.

- **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 potentially impacted areas. While companies may or may not be affected by the event, critical suppliers and customers in the affected region may be. Therefore, 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.

58. **What can organizations do to prepare for a pandemic event?**

Since it is uncertain whether a large-scale pandemic flu event will ever occur, it is difficult to argue that an organization should make wholesale changes to the way it operates day to day in anticipation of such an occurrence. However, prudence dictates that at minimum all organizations evaluate a pandemic event in their regular risk analysis and BIA activities. The following points should be considered:

- Consider the possibility that employees will not come to work during a pandemic and the impact to the organization 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 naive to believe that parents will choose work over caring for their sick children; therefore, what accommodations can and should be made? Where possible, consider how employees could be utilized while working from home. Do they have access to the necessary technologies and vital records to continue working for several weeks during an outbreak?

- Work with the HR 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. 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 influenza.

- Decide how the business continuity response would change if multiple facilities were affected concurrently. Many BCM programs are built around the risk of a catastrophic event affecting one operation at a time. Documented or not, the assumption is that the rest of the enterprise’s resources will be
available to assist one affected location. This is a realistic assumption for normal business continuity exposures, but unrealistic for pandemic flu.

• Evaluate the impact on demand for the organization’s products or services in the event of 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 likely will use during a pandemic (e.g., Internet, call centers).

• Contact key business partners and vendors to determine their level of attention to this matter. If defined SLAs are in place, determine whether the preparations the business partner has taken realistically will allow them to meet the agreement. If not, and they cannot be convinced to enhance their preparations, outline contingency plans for their failure during a pandemic flu event. If they are a critical vendor, develop a more comprehensive contingency plan.

• Consider how the organization 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 suspension of all business travel for an extended period (several weeks to several months or longer).

• If the business has a retail arm, determine the cost and benefit of voluntary closure. If it is determined that customers and employees are unlikely to come to the location, it may be better to close the location voluntarily 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 employees now about the steps the organization has taken to prepare for a pandemic flu event. It is unrealistic to believe that employees, having never heard of the preparations before a pandemic, will be able to listen attentively when one occurs.

Build a disease pandemic component into the organization’s BCM program, both at the executive crisis management planning level and the tactical business resumption level. As this component is developed, the following issues should be considered:

• 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, and so on – it is especially important that an organization’s crisis management program has a system to gather and interpret information quickly 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.

• The use of the Business Pandemic Influenza Planning Checklist11 can be an effective way for organizations to determine any gaps in existing BCPs 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.

---

INDUSTRY-SPECIFIC CONSIDERATIONS FOR BCM PROGRAMS

Communications

Communications companies are under extraordinary pressure to provide reliable, high-quality and diverse services to customers who have increasingly high expectations – and little brand loyalty in a marketplace filled with alternative providers. As communications companies become more reliant/dependent upon third-party suppliers and vendors to meet these demands and expand into new markets, it is becoming increasingly more important and challenging to appropriately identify and address potential risks that could lead to costly and/or reputation-damaging disruptions.

Protecting critical enterprise infrastructure is also paramount. Communications providers must pay special attention to designing, maintaining and testing restoration procedures, failover strategies, and critical supplier/vendor service disruption strategies that help them not only provide products and services to customers but also critical support to internal business functions. Companies in this sector also must fully consider the potential impact of natural disasters, pandemics, energy shortages/outages, or man-made disruptions (e.g., sabotage, security breaches) on their ability to deliver services to customers – and plan appropriately.

While this guide cannot present the many details surrounding each potential variable that communications organizations may want to take into account when developing and/or assessing the strength of their BCM programs, following are examples of questions that communications executives may want to consider as they develop an effective BCM program for their organizations (in addition to the industry-independent considerations already discussed in this publication).

59. How well have we focused on the critical network infrastructure elements supporting our customers? What are our practices for ensuring BCM strategies and objectives for these environments are kept up to date as we continue to expand our infrastructure and/or upgrade critical network components?

In today’s market, with customers continually looking for the best deals, rates and carriers, maintaining adequate networks and providing coverage to customers should be viewed as a critical business function. Providing the appropriate amount of coverage and focus on network uptime from a BCP perspective is critical. Customers view the availability of technology as an expectation of service with short tolerances for disruption. While most companies maintain insurance coverage for some disruptive events, the potential liabilities associated with these events could far exceed the insurance coverage maintained.

As major changes and/or enhancements are made to the network infrastructure, BCP should be a key consideration. Key questions to ask include, but are not limited to, the following:

- How will the change impact the overall network infrastructure and disaster recovery strategy?
- Does the change warrant an update to recovery plans and/or a new test to validate that strategies and plans remain viable and are aligned with recovery requirements?
60. Have we properly evaluated the risk of interruption from key suppliers (e.g., equipment and support, handsets, smart devices, programming and entertainment) that are critical to our ability to provide products and services to our customers and/or support essential internal business functions?

Communications companies often rely on third-party vendors to perform critical functions. But communication providers are often so preoccupied with internal risks that they fail to measure risks to critical outsourced vendors. Communications companies therefore should identify which critical tasks have been outsourced and develop strategies that would mitigate the impact of a business interruption that affects key vendors.

61. How well have we designed and tested alternative operational procedures for critical internal functions such as system maintenance, billing and mediation functions?

These types of internal services within communications companies are typically supported around the clock by a unique blend of IT and business professionals. These professionals are dealing with the daily challenges and requirements necessary to maintain a business. From an IT perspective, this includes, but is not limited to, preventing and/or responding to regular security threats, performing infrastructure maintenance, monitoring internal and external network resources, and implementing new technologies to maintain a competitive edge. From a business perspective, this includes, but is not limited to, back-office billing and collection processes, accounting, financial reporting, sales, marketing, HR, legal and strategic planning.

Given the dependencies on these resources, effective BCP from both a “people” and “process” perspective should not be undervalued or underestimated. If the focus of recovery planning for a communications-based company is placed solely on the IT department and does not take into account the people and processes that support these areas, revenue generation may continue for a short period after a disruption. However, it will not take long for services to degrade and customers to seek competitors’ services.

Similar to customer-facing processes, enterprise applications and the network infrastructure are instrumental to supporting internal services. Consequently, many companies have implemented an internal disaster recovery plan or worked with a third-party vendor to also protect their internal enterprise infrastructure. Unfortunately, many companies often fail to test these internal 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 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.

62. How would management handle customer support if a call center or key call center support systems were unavailable? Do we have appropriate failover capabilities for this type of event?

The communications industry follows the general trend toward outsourcing of customer call center functionality. Many companies have either outsourced or taken a co-sourced approach to call center functionality (i.e., on-shore call centers during normal business hours and then routing to an off-shore call center after hours). While these arrangements can simplify the resumption of BCM, communications providers must still ensure that SLAs are documented in the vendor contract, as well as continue to verify that the vendor’s continuity program, as a whole, is sufficient in meeting their needs.
When it comes to maintaining business continuity, the energy sector faces complex challenges – including meeting regulatory demands and managing environmental health and safety issues. Energy companies also must meet very high customer expectations: Because the services they provide are so essential, a short-term operational disruption has the potential to affect millions of people and businesses adversely. Outages at oil and gas companies or at utility organizations reliant on equipment and systems that require 24/7 uptime (e.g., SCADA systems), for example, can be very visible and affect a large number of customers, business partners, and other third parties, such as royalty owners.

Many energy companies also possess a unique risk profile based solely on the geographic area in which they operate. For instance, exploration, production and refining operations located in politically sensitive areas of the world, such as the Middle East, need crisis management plans to protect personnel and respond to political events. Natural disasters are also a key concern. In the United States, for example, many refineries are located in the Gulf Coast region, which is subject to hurricanes and flooding. (Houston, the energy capital of the world and home to many leading energy companies, is also affected by this risk profile.) Given recent, dramatic weather events in the region, like Hurricane Katrina, it has become even more critical for energy companies operating there to maintain up-to-date emergency response procedures and technical recovery plans.

While this guide cannot present the many details surrounding each potential variable that energy companies may want to take into account when developing and/or assessing the strength of their BCM programs, all energy executives should at least consider the following questions (in addition to the industry-independent considerations already discussed in this publication).

**63. Are there regulatory BCP requirements that typically affect the energy industry?**

There are general regulations, such as SOX, which affect all publicly traded companies. Depending on the nature of the organization and the external auditor requirements, SOX generally only evaluates high-level backup and recovery controls and does not explicitly require business continuity measures. For those energy companies involved in the trading of swaps and derivatives, a disaster recovery plan is required based on the Dodd-Frank Act. Additionally, there are other regulatory requirements, such as from NERC, which has specific BCP requirements but is targeted only to those systems directly involved in managing the flow of electricity to the grid. Although none of these regulations comes close to mandating a comprehensive BCP, most major energy companies recognize the risk involved and have enacted the basic components of a plan.
64. **What are the most common business processes affected by an outage?**

When energy-focused organizations assess their environment, we typically recommend they segregate business functions between corporate administrative functions and those performed “in the field.” At field locations, we would recommend focusing efforts on maintaining field operations (e.g., drilling, production, transportation, processing) and continuing volume measurement. For corporate activities, the answer is generally derived by evaluating processes that are the most real-time in nature. Performing a BIA is critical to identifying those essential business processes and the recovery timelines involved. For companies performing marketing and energy trading activities, there is little tolerance for downtime due to the potential financial risks involved. Thus, those related business processes are critical. Otherwise, we generally find the most common administrative processes involve payroll and cash management, with enterprise resource planning (ERP) recovery quickly following in order to support the next tier of corporate accounting functions. Each organization is different and should rely on the BIA to capture appropriately management’s tolerance for downtime respective to each business function.

65. **Energy-related companies typically have a program to manage environmental health and safety (EHS) at their work sites. Doesn’t that cover business continuity requirements?**

Only partially. Typical steps included in an EHS program entail life-safety measures and actions to take directly after an incident occurs, usually at a remote field location. In business continuity nomenclature, it would be comparable to an incident response plan (or crisis management plan) for that specific location. The remaining BCP steps associated with recovering critical business processes, ensuring appropriate recoverability of IT resources, communication plans, and linkage into broader corporate BCPs, are often absent. Thus, to implement a comprehensive approach, it is important to ensure each BCP component is considered across the entire enterprise.

66. **Energy companies often operate in politically sensitive areas and/or other areas overseas that experience frequent major natural disasters. What BCP-related precautions should be considered to reflect the risk of operating in those environments?**

Companies operating in geographically sensitive areas should perform a risk assessment to evaluate risks associated with items such as political unrest, public riots, terrorism, and earthquakes and tsunamis. These factors can impact what specific response plans should be in place to respond to high-risk events. For instance, companies may need a site-specific country evacuation plan, require data backup plans that send data to geographic “safe sites” on a real-time or daily basis, or have medical supplies on hand and emergency procedures in place to respond to terrorism or large life-safety events. Performing a site-specific risk assessment will assist in understanding the risk posture of that location so that a specific risk mitigation strategy can be considered.
Financial Institutions

The global, 24/7 nature of today’s marketplace makes it imperative for financial institutions to ensure they can continue to conduct trading operations, carry out key transactions, and interact with and support customers in the event of a disruption, such as a system outage, or a disaster – natural or man-made. And two trends underscore the importance of IT disaster recovery planning, specifically, for financial institutions: the number of financial transactions being conducted electronically is growing, and the IT systems of financial institutions around the globe are increasingly being targeted by politically and/or financially motivated hackers. Regulators and standard-setting bodies also want financial institutions to take BCP seriously – and some have issued guidance for organizations to apply as they work to create an effective BCM program that can help them recover from an untoward event.

While this guide cannot present the many details surrounding each potential variable that financial institutions may want to take into account when developing and/or assessing the strength of their BCM programs, following are examples of questions that financial executives may want to consider as they develop an effective BCM program for their organization (in addition to the industry-independent considerations already discussed in this publication).

67. What regulatory guidance should financial institutions rely on?

While depository institutions may find themselves subject to various regulatory bodies (e.g., Board of Governors of the Federal Reserve System [FRB], the Federal Deposit Insurance Corporation [FDIC], the National Credit Union Administration [NCUA], the Office of the Comptroller of the Currency [OCC], and the Consumer Financial Protection Bureau [CFPB]) depending on the type of organization, the guidance from a business continuity standpoint is straightforward, as the FFIEC has produced a standard booklet outlining expectations from a business continuity perspective, including regulatory guidance and expectations related to pandemic planning. The regulators assume financial institutions are reviewing and applying this guidance (as deemed applicable) and when assessing an organization, will benchmark them accordingly.

Non-depository financial institutions should look to the guidance provided by the U.S. Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Financial Industry Regulatory Authority (FINRA), some of which have issued guidance (e.g., the joint review and advisory www.sec.gov/about/offices/ocie/jointobservations-bcps08072013.pdf published after Hurricane Sandy) on an interagency basis. Websites for each of the agencies also contain agency-specific information on business continuity and pandemic preparedness requirements for supervised firms.

68. Are organizations required to apply all aspects of business continuity guidance as outlined by the regulators?

Regulatory guidance generally provides for the individual financial institution to make the determination of what aspects of the guidance should be applied based on a detailed risk assessment and BIA activities. Accordingly, examiners will adjust their own review approach based on an organization’s analysis and its reasonableness. As would be expected, however, the larger and more mature financial institutions should anticipate establishing a more comprehensive program.

69. Are financial institutions, such as banks, required to recover within a defined time period?

This is a common question as banks, for example, sometimes assume standard recovery time objectives with which they must comply have been established. However, the expectation is that an organization applies the guidance as outlined in the FFIEC booklet. The recovery time objective of processes and systems should be established through a BIA. As determined through the BIA, recovery objectives ultimately would be determined based on the risk and cost benefit to the organization. An examiner would typically assess the work performed and determine whether the conclusions reached are reasonable.

70. Are business continuity standards for financial institutions set only by the regulatory agencies?

The U.S. Department of Homeland Security (DHS) also offers guidelines to the financial services sector, which it defines as “a vital component” of U.S. critical infrastructure. In 2010, the agency, in partnership with the U.S. Department of the Treasury, published a sector-specific plan that details how the National Infrastructure Protection Plan (NIPP), which provides a risk management framework designed to enhance the safety of U.S. critical infrastructure, is implemented within the financial services sector.

The Banking and Finance Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan from the DHS “provides a description of the complex nature of the sector and an overview of the sector’s provision of products and services, which are: 1) deposit, consumer credit, and payment systems; 2) credit and liquidity products; 3) investment products; and 4) risk transfer products (including insurance).” The plan underscores the interconnectedness of the financial services sector to other critical infrastructure sectors, including communications and IT, which, if disrupted, could undermine the financial services sector’s ability to conduct normal business.

This document lays out three goals for the financial services sector to work toward to meet the following vision statement on business continuity: “To continue to improve the resilience and availability of financial services, the Banking and Finance Sector will work through its public-private partnership to address the evolving nature of threats and the risks posed by the sector’s dependency upon other critical sectors.” The three goals outlined in the document are:

1. Achieve the best possible position in the face of myriad intentional, unintentional, man-made, and natural threats against the sector’s physical and cyber infrastructure;
2. Address and manage the risks posed by the dependence of the sector on communications, IT, energy and transportation systems sectors; and
3. Work with the law enforcement community, financial regulatory authorities, the private sector, and counterparts outside the United States to address threats facing the sector.


---

71. To what extent are financial institutions responsible for the business continuity of vendor-supported systems?

Regulators expect that financial institutions will ensure that acceptable business continuity plans are in place for all systems required to perform a financial institution’s key activities, including, but not limited to, systems relied upon for customer-facing, financial reporting and compliance (e.g., AML transaction monitoring and sanctions screening). For vendor-supported systems, financial institution due diligence procedures should consider the vendor’s business continuity standards and their alignment with the financial institution’s needs, contracts with vendors should reflect obligations and expectations, and financial institutions should consider, as appropriate, participating in vendor business continuity tests or, at minimum, requiring evidence (such as an SSAE 16 report) that the program has been tested.
Healthcare

Healthcare is a unique and heavily regulated industry. Providers, payers, pharmaceutical companies and biotech firms all face multiple challenges in the development and maintenance of effective BCM strategies – from increasing regulatory scrutiny to better informed patients/members looking for more communication from their providers. Additionally, the significant push for increased adoption of health information technology (HIT) and continuous change in the healthcare industry itself have organizations struggling to ensure all bases are covered when evaluating the sufficiency of their BCM programs.

While this guide cannot present the many details surrounding each potential variable that healthcare organizations may want to take into account when developing and/or assessing the strength of their BCM programs, all organizations should at least consider the following points (in addition to the industry-independent considerations already discussed in this publication):

• For healthcare providers, continuity of care and crisis management are of obvious and paramount importance. Ensuring that patients continue to receive appropriate care and healthcare providers are able to respond to major events in the community are driving forces behind much of what a healthcare organization’s BCM program entails. The clinical implications of having an effective or ineffective BCM program are too numerous to be addressed in this document. However, these are not the only components of a successful program. Many organizations do not give sufficient consideration to back-office operations, administrative processes, and other vital functions, which all must be factored into overall BCM initiatives.

• The use of Electronic Health Records has altered the healthcare landscape significantly. The line between continuity of care and traditional IT disaster recovery is becoming less and less clear while upstream and downstream interdependencies are increasing in importance. This is leading to more interrelated BCM plans.

• Federal regulatory requirements are often supplemented by a variety of very complex state-specific mandates, accreditation requirements, and more. A healthcare organization’s geographical reach and the breadth/depth of its strategic initiatives must be taken into consideration in its BCM efforts.

• A healthcare organization’s risk analysis efforts as required by the HIPAA Security Final Rule must take into consideration the availability of electronic protected health information (ePHI), in addition to the confidentiality and integrity of that data.

• The type and extent of testing required to ensure a healthcare organization’s BCM program is designed effectively and that everyone involved is aware of their responsibilities may vary significantly based upon the type of organization and the state(s) in which it operates.
Manufacturing

Manufacturers, no matter how lean or streamlined their processes, face risks throughout their supply chain, from potential product defects to IT system failure. Just one unexpected event can create significant disruption and leave manufacturers scrambling to bring operations back to normal to meet customer demands and expectations. For manufacturers that maintain a global supply chain and work with multiple suppliers, managing risks that can threaten business continuity – such as political uncertainty, natural disasters or supplier reliability – can be even more challenging and resource-intensive.

Manufacturers must look deep within their supply chain, and to every supplier that helps to support it, to assess risk fully, and determine alternatives to replace any essential “cogs” in the machine should they fail. Additionally, as part of their business continuity planning process, manufacturers must consider the potential for a product recall – which can be a devastating event with long-term business consequences – and prepare for the possibility as they would any other significant crisis event.

While this guide cannot present the many details surrounding each potential variable that manufacturers may want to take into account when developing and/or assessing the strength of their BCM programs, all manufacturers should at least consider the following questions (in addition to the industry-independent considerations already discussed in this publication).

72. How can pursuing a single-source supply strategy affect my organization’s overall risk of business interruption?

Supply strategies are complex by nature. There are many instances where a single-source supply strategy is the right business decision even when alternate sources of supply exist. In instances where a company is reliant on a sole-source supplier, finding alternates is more daunting, as it may require changing product specifications or working closely with other key suppliers to develop alternatives. Neither of these approaches is typically fast. However, moving to an alternate supplier may carry the risk of quality issues and must be managed carefully. Supplier relationships honed over a period of years cannot be replaced overnight with an expectation of comparable performance levels.

As manufacturers streamline their supply chains and rely more heavily on single- and sole-source suppliers, they are discovering new organizational risks they have not measured. Even in cases where companies do measure the financial risks of a certain supplier (e.g., credit risk), they may not have taken into account business interruption risks stemming from a man-made or natural disaster. Manufacturers should include single- and sole-source vendors in their risk assessment, BIA, continuity strategy and BCP. These critical vendors need to be treated like critical functions or processes. Political and natural disaster risks as well as the impact to revenue and operations should be measured, lead time for finished products needs to be understood, alternate sources for critical supplies should be identified, and strategies to mitigate the impact of business interruptions occurring among key suppliers need to be developed.

73. Has management designed manual backup procedures to carry out manufacturing schedules and order releases?

Most modern manufacturers have switched to automated manufacturing resource planning (MRP) and ERP systems. Therefore, many have not considered manual workarounds to carry out manufacturing schedules and order releases during an outage. If management does not have the confidence in the resumption capabilities of its IT systems, it should consider developing manual backup procedures to facilitate the continued operation of critical manufacturing processes.
74. How do companies that rely solely on single-site manufacturing or computer-aided manufacturing operations plan for the impact of a long-term outage?

Over the last two decades, globalization, outsourcing, increased cross-border sourcing, IT, and shared services centers have encouraged many organizations to consolidate facilities and streamline processes to eliminate nonessential and redundant activities as well as focus and automate remaining activities. The waves of total quality management, process re-engineering and Six Sigma process improvements have created a bias for strong supplier relationships and tight coupling with supply chains with the objective of driving costs out of processes and products while preserving quality standards.

The decision to decrease inventory levels, have a sole-source or single-source strategic supplier in any country of the world, and adopt just-in-time manufacturing and delivery techniques versus higher inventory levels, multiple suppliers and other buffers in the process, involves trade-off decisions where quality, time and cost considerations often win out over business continuity considerations.

As manufacturers become leaner, leveraging single manufacturing locations and automated processes, it is critical that they investigate existing customer SLAs to ensure what, if any, their liabilities are 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, in the correct quantity and in acceptable condition. Ultimately, the only options a lean manufacturer has to recover operations are to delay the impact through inventory controls, expedite partial manufacturing throughput and undertake full resumption. Certainly, excess inventory, intermediary warehousing, contract manufacturing, and redundant locations 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-intensive. Therefore, a significant amount of analysis usually is required to justify any strategy.

75. Where does a product recall procedure fit into a BCM program?

Every manufacturer should have a robust and tested product recall procedure as part of its standard operating procedures; it also should be integrated into the crisis management plan. A good product recall plan should address procedures to pull product in the event an issue is discovered due to safety or quality concerns; to communicate to customers and stakeholders about the issue; to trace and isolate the product defect root cause; to track mechanisms to determine defective product marketplace proliferation and elimination; and to dispose of the product 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 significant and potentially devastating crises that can occur since they can affect not only finances and operations, but also brand and reputation and people’s health and safety. Management of a product recall should be handled no differently than 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.
Retail

For any retailer, the inability to make a sale is a key risk. To win consumers’ business – and loyalty – retailers must keep in-demand products on store shelves, or deliver orders from warehouses to customers exactly when and in the condition expected. They also must provide consumers with convenient ways to complete their transactions, including by debit or credit card, in-store or online. The ability to provide outstanding customer service – at all times, but especially during a crisis – is also business-critical for any retailer. And to maintain competitive advantage, retailers must do all of the above in a way that allows them to be profitable while also providing high-quality goods and services at prices that meet their customers’ expectations. Problems in receiving product from suppliers; in storing or distributing goods; at the point of sale; in back-end processing; or in keeping customers satisfied and well-informed all have the potential to erode a retailer’s market share – or even put it out of business permanently.

While this guide cannot present the many details surrounding each potential variable that retailers may want to take into account when developing and/or assessing the strength of their BCM programs, following are examples of questions that retail executives may want to consider as they develop an effective BCM program for their organization (in addition to the industry-independent considerations already discussed in this publication).

76. What are the core concerns regarding point-of-sale (POS) transactions in the event of an extended network outage with the central office?

The lifeblood for most retailers 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 to satisfying 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 a central or third-party processor has been severed. It is important for companies to (1) create redundancies between stores and central offices, and understand the alternates 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 stores are prepared for the worst by arming them with the procedures they need to operate during an outage, including manual credit card machines.

77. What are some of the key business continuity considerations with respect to warehousing and distribution?

Bigger is better, but sometimes bigger also can be riskier. As companies formulate and execute distribution strategies, they must give sufficient thought to the availability risk of their primary warehousing and distribution facilities. A strategy of greater warehouse centralization makes a great deal of sense from an efficiency and cost-minimization perspective. However, it also can limit the organization in the event of a disaster when one of the few large warehouses is affected and remaining locations are neither equipped nor geographically available to pick up the slack. Business continuity and supply chain risks should be weighed appropriately during the cost-benefit analysis when these types of centralization strategies are considered. A number of organizations with few warehouses, or even a single warehouse, will tend toward a heavy focus on environmental control considerations. When an organization puts all its eggs in one basket, key environmental risks such as seismic and flood risks, structural soundness of the facilities, and risk of fire based on volatility of product will figure heavily and require an increased focus and standard of care.
78. Is 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 the financial impact of 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 monitored consistently to ensure 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. How much focus should be placed on customer service in a disaster situation?

The customer is paramount. 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 about the products they sell. This translates into strategies that ensure 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 purchase products and supplies manually without the Electronic Data Interchange (EDI) up and running?

An organization’s EDI is a critical link to suppliers and vendors that provide products and raw materials. Companies should ensure product supply and delivery will continue even when the EDI is unavailable by maintaining sufficiently detailed manual procedures and vendor lists to re-establish delivery links. Additionally, by having conversations with suppliers before an outage, retail management can understand capabilities and expectations when critical links are out. This will go a long way toward a quick recovery and peace of mind. That said, we often suggest the EDI be designed with high availability in mind. This includes a heavy focus on the redundancy of supporting technologies, sufficient monitoring, and regular independent review to ensure key availability risks are identified.
ABOUT PROTVITI

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our Business Continuity Management Practice

Protiviti’s Business Continuity Management (BCM) service offers solutions to organizations to assist them in the analysis, development and implementation of comprehensive business continuity plans to ensure the availability of critical business processes.

An increasing number of organizations and their executive management are recognizing the need for continuity planning, resiliency and crisis management as part of an overall risk management program. Many governmental – and virtually all regulatory – bodies around the globe have recognized and incorporated business continuity and crisis management planning into their requirements. Investors, as well as boards of directors, are increasingly interested in management’s capability to continue critical operations through a disruption and their plans to ensure a resilient enterprise.

Our approach to BCM is business-oriented and based upon the risks related to an organization’s key business-process drivers. We focus on the analysis and evaluation of strategies, development of approaches, and testing and implementation of plans that meet an organization’s continuity needs from a people, processes and IT infrastructure perspective. Our business continuity approach incorporates industry best practices and is constantly monitored to ensure adherence to regulatory requirements.

Contacts

Kurt Underwood  
Global Leader – IT Consulting  
+1.503.889.7771  
kurt.underwood@protiviti.com

Jonathan Bronson  
+1.213.327.1308  
jonathan.bronson@protiviti.com

Michael Porier  
+1.713.314.5030  
michael.porier@protiviti.com

Jeffrey Weber  
+1.412.402.1712  
jeffrey.weber@protiviti.com

Jonathan Wyatt  
+44.7747.487644  
jonathan.wyatt@protiviti.co.uk