Gartner Research

Publication Date: 8 February 2010 ID Number: G00174201

Ten Best Practices for Creating and Maintaining Effective Business Continuity Management Plans

Roberta J. Witty, Les Stevens

Having current and complete information during a crisis is vital for quick and effective response and recovery. However, a common complaint of many business continuity managers is that business continuity management (BCM) plans are outdated because they haven't been updated to account for current business availability needs, or they are stored in multiple places throughout the enterprise, making it hard to keep them current without a strong document management process. Having an enterprisewide BCM plan management strategy assisted by automation can ensure that BCM plans are current, viable and available during a crisis.

Key Findings

- Many organizations know that their BCM plans are outdated and are concerned that they won't be able to recover from a disaster if these plans are used.
- The complexity of the enterprise and the interrelatedness of information needed for response and recovery efforts further challenge successful recovery, and therefore, the long-term viability of the enterprise.
- Too few organizations are planning for an outage time frame longer than seven days.
- Automation can assist in developing, maintaining and exercising BCM plans according to business needs.

Recommendations

- Develop a distributed, collaborative BCM organizational model.
- Communicate the business value of BCM.
- Build BCM plan management into the business/project life cycle.
- Develop a structured framework of plans.
- Keep plans relevant to the purpose.
- Build simple but detailed plans to be used by the second-tier workforce.
- Establish a central repository and plan an administration process.
- Implement business continuity management planning (BCMP) and crisis/incident management tools.
- Exercise BCM plans once a year at minimum.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ANALYSIS

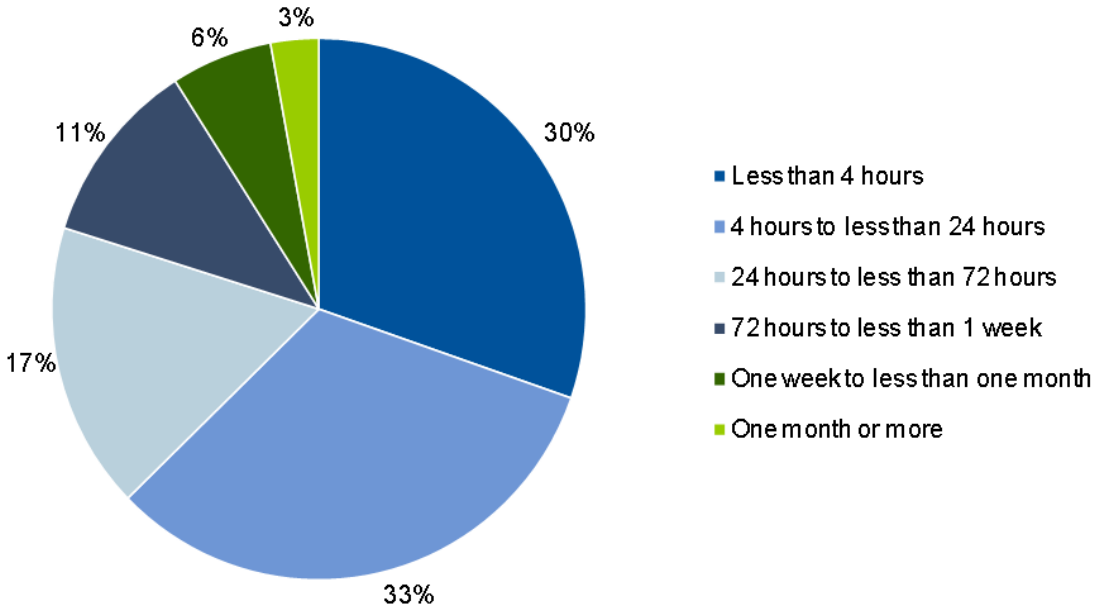
1.0 Introduction

Having current and complete information during a crisis is vital for quick and effective response and recovery. The creation and maintenance of effective response, recovery and restoration plans (hereafter referred to as "BCM plans") represents a strategic imperative for enterprises, because BCM plans that are outdated, inaccessible or otherwise inappropriate to enterprise-specific needs place the business at serious risk in the event of a crisis.

Gartner research shows that poorly designed and maintained BCM plans — plans that remain a "paper exercise" without real value — are a serious and commonplace problem for many enterprises.

Our 2010 Risk and Security Survey results (see Figure 1) confirm that recovery time objectives (RTOs) are shrinking: 63% of survey respondents told us that their RTOs for mission-critical business processes are under 24 hours. With such short RTOs, it is imperative that BCM plans are current and easily available during a crisis.

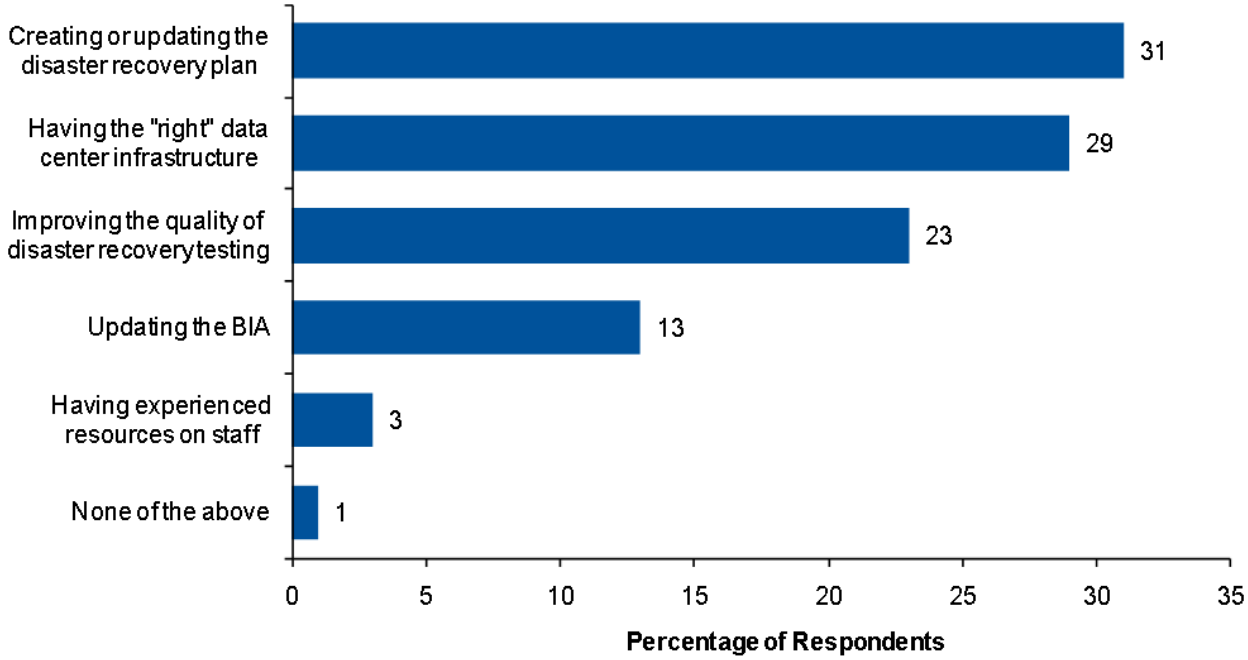
Figure 1. Business Functions and RTOs 2010 Risk and Security Survey, n = 133



Source: Gartner (February 2010)

In addition, participants at the 2008 Data Center Conference told us that creating and updating of IT disaster recovery plans is the area needing the most improvement (see Figure 2).

Figure 2. What Part of Your IT Disaster Recovery Management (DRM) Program Needs the Most Improvement, 2009 Data Center Conference, n = 70



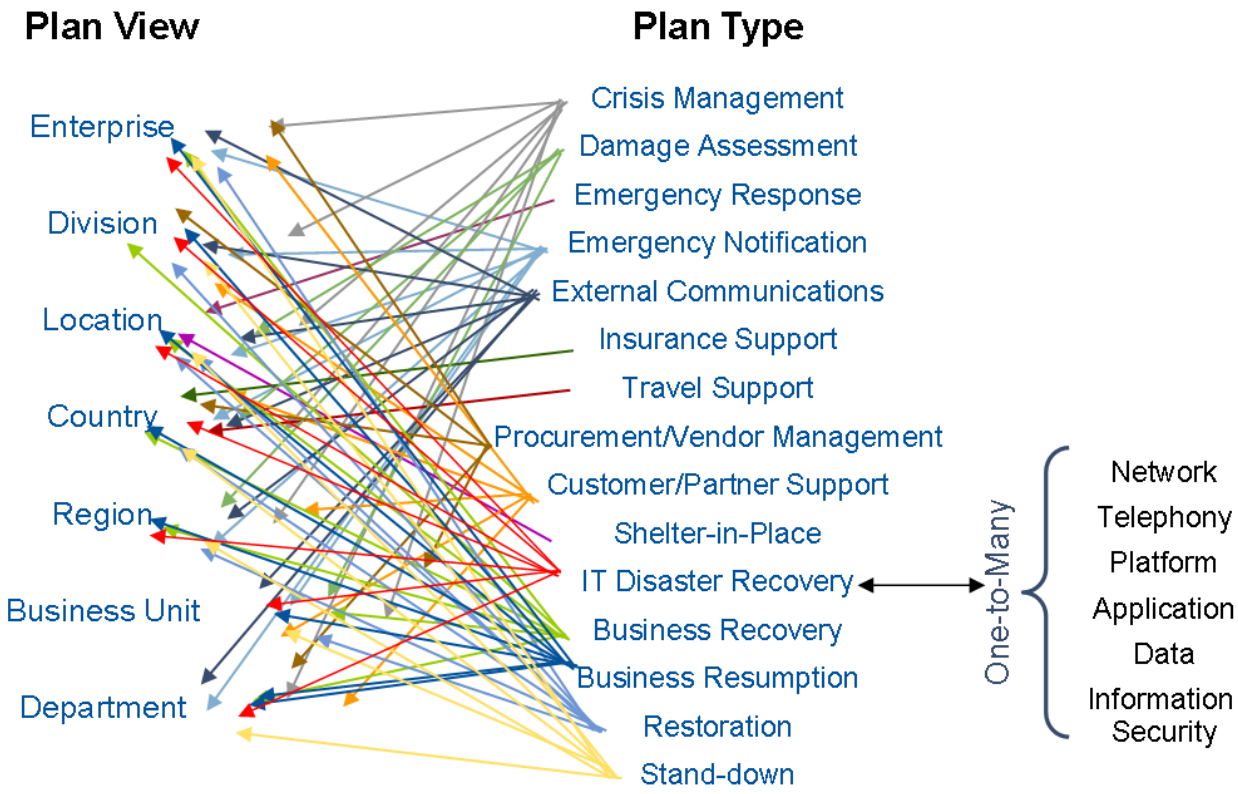
Source: Gartner (February 2010)

The most common approach that enterprises use to manage their BCM plans is to create them with office automation software and store them in folders in a file system or internal portal for access by recovery team members during a crisis. This approach does not lend itself to applying standardized practices for storing and distributing BCM plans, let alone creating, updating and securing them.

1.1 Why Are BCM Plans so Hard to Develop and Maintain?

BCM plans are a complex web of documents ranging from the crisis management plan, to the business recovery plan, to the IT DRM plan that must cover all aspects of current business operations and the organization model (see Figure 3). Each plan type has its own purpose, enterprise scope and scenarios that are being planned for.

Figure 3. BCM Plans Are a Complex Web of Documents



Source: Gartner (February 2010)

There are a number of challenges in developing and maintaining BCM plans that meet current business availability needs:

- The complexity of the enterprise and the interrelatedness of information needed for response and recovery efforts
- The absence of executive management sponsorship and adequate resources
- The lack of clearly defined accountability and responsibility over BCM program and plan management
- The lack of support from the business, for example, because recovery is seen as an IT-only responsibility and an expense not often, or ever, used
- Poor communications about BCM practices and their benefits
- Plan management process failures, such as:
    - Covering too short an outage time frame, which also means that you may not be including enough disaster scenarios in your plan development process
    - Not regularly exercising plans, especially at an integrated level
    - Not taking into account the interdependencies of business and IT processes and the RTOs of different stakeholders

- Not maintaining plans for changing business and IT processes
- Excessive complexity, leading to errors and confusion in exercising and execution

Having an enterprisewide BCM plan management strategy assisted by automation can ensure that the most current plans are available during a crisis. But creating and maintaining pragmatic and actionable BCM plans demand a level of skill, expertise and experience that many organizations find lacking in their workforces. While the availability needs for individual enterprises are unique, and a variety of different approaches may be legitimately employed, there is a common set of steps that should be followed when planning for BCM.

Gartner advises clients to adopt the following best practices for managing BCM plans to ensure that recovery team members have the most current information available to them during a crisis — the most trying and stressful time in the operations of the business, as well as in recovery team members' individual careers.

2.0 Best Practice No. 1: Executive Management Commitment Is Required for the BCM Program

Effective BCM planning requires commitment from all lines of business and all levels of management. Table 1 identifies the causes and consequences of not having that commitment.

Table 1. Causes and Consequences of a Lack of Support for the BCM Program

Problem	Cause	Consequence
No Executive Management Support	• Don't understand the risk • Don't see value to business • Consider BCM an IT issue	• Lack of financial resources • No willingness to change business processes to improve resilience • Low level of support from business management • Less likelihood of a sustainable BCM program
No Business Management Support	• All the above • No top management support • Inadequate communication and collaboration	• Lack of involvement in and support of planning processes, including awareness, training, development, exercising and reviewing • Inadequate validation of inputs and plans • Lack of support from staff
No Support From Staff	• All the above • No business management support	• All the above • Plans don't get developed or updated • No one shows up for recovery tests

Source: Gartner (February 2010)

To gain greater business continuity and IT disaster recovery visibility and commitment from executive management, BCM and IT DRM planners should initiate a multipart awareness campaign. To jump-start the campaign, BCM and IT DRM professionals should leverage compliance initiatives, industry regulations and recent disaster events. We also recommend working with line-of-business executives on an informal business impact analysis (BIA) or walkthrough test to shore up support.

The best approach to getting management's attention and commitment is to make BCM relevant to the business by communicating the business benefits (reputation/brand preservation, revenue

preservation, regulatory, legal and contractual compliance, community support, life/safety protection and so forth). Linking key performance indicators (KPIs) to key availability risk indicators is an effective approach for communicating to business management the value of BCM so that they take ownership of BCM plan management and commit to the needed investments year over year to maintain the BCM program.

To develop your own BCM benefits communications program, use Gartner's Business Value Model and see "A New Approach: Obtain Business Ownership and Investment Commitment for Business Continuity and Resilience Management Through Key Performance and Risk Indicator Mapping." This research discussed how a BCM manager can map KPIs of the business to key risk indicators (KRIs) for availability to craft a message that business managers will understand. See Table 2 for examples of this mapping.

Table 2. KPI/Availability KRI Mappings With Impact Action Trigger

KPI	Availability KRI	Impact Action Trigger
On-Time Delivery	Suppliers' BCM Programs	More than 10% of single-source suppliers with no BCM program or one that requires more than 12 weeks to recover manufacturing operations leads to failure to meet contractual obligations.
R&D Success Index	Product Design	Less than 25% growth rate year over year in new products being delivered with no single-source component.
System Performance	Mission-Critical Personnel Turnover	A 15% turnover rate every six months in identified key positions impacts mission-critical system stability and efficiency, leads to failure to meet internal or external service-level agreements (SLAs), and delays recovery from disaster.
Agreement Effectiveness	Mission-Critical System Downtime	Products/services that represent 30% or more of revenue that have not exercised their recovery plans within the last six months lead to delays in meeting contractual obligations, SLAs and recovery from disaster.

Source: Gartner (October 2009)

Also, BCM and IT DRM managers should co-opt the support of other influential roles within the organizations to bolster their message. Functions such as corporate governance, corporate risk management and internal audit often have more influence at the executive level than the BCM leader. Building a "'coalition" of roles that share the same interests and, hence, communicate the same message regarding the importance of BCM greatly enhances the effectiveness of the communication. See the BCM charter note "Toolkit: Business Continuity Management Charter Best Practices and Template."

Lastly, build BCM plan management into many aspects of the business life cycle, such as new product/service development, business process changes, real estate changes, HR/workforce changes, the IT software development life cycle/project life cycle (SDLC/PLC) process, exercising and post-disaster post-mortems.

After trying these techniques, if a BCM or IT DRM planner still does not obtain the necessary management commitment, he or she should either accept the enterprise's lack of support for a BCM program (and document that management has accepted the risk and potential liability) or seek a position in an enterprise that cares — before a disaster strikes and damages your reputation.

3.0 Best Practice No. 2: Business Units Must Develop Their Own BCM Plans

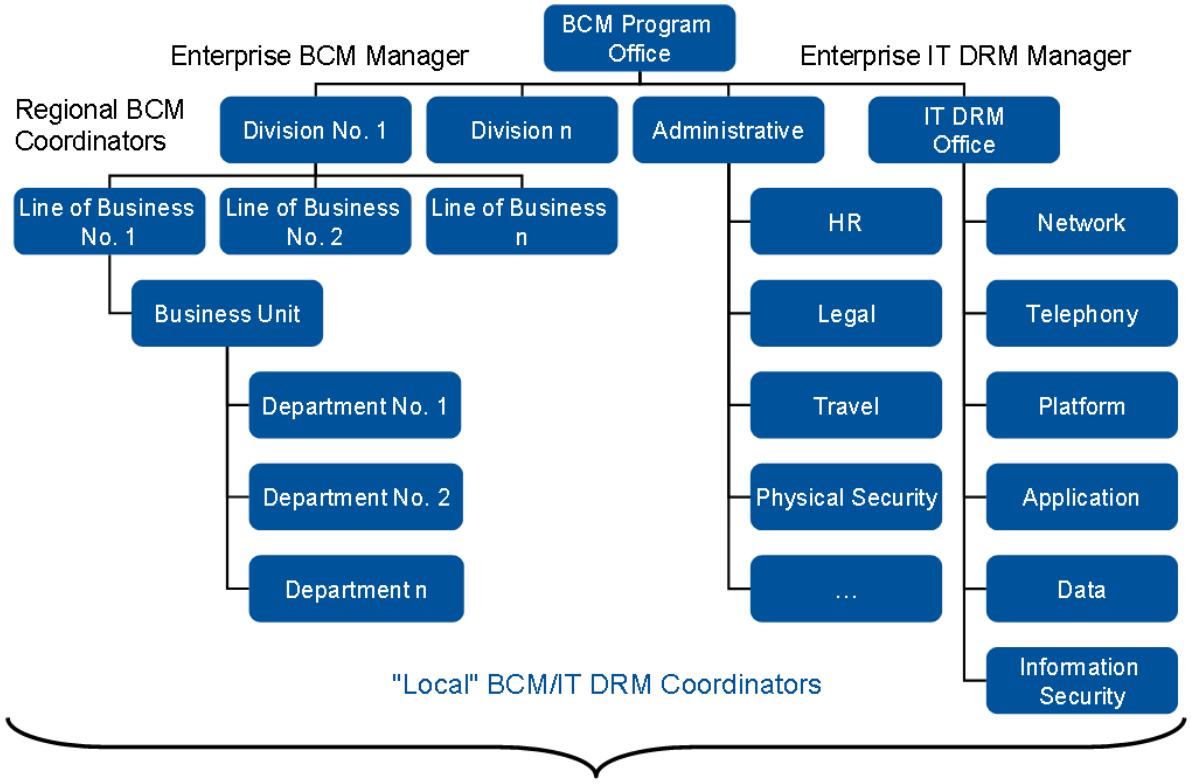
BCM plan development, maintenance and exercising is a collaborative effort involving the business, IT, and the supply chain; done in isolation, plans are bound to fail. BCM plans must be developed, maintained and exercised by those most knowledgeable about the business processes that need to be recovered. Plan ownership should be assigned to specific workforce members — by business process, technology to be recovered and so forth.

Plan owners are responsible for developing, maintaining and exercising plans to identify change requirements through:

- Normal business process changes
- HR data updates
- Asset management processes
- Real estate processes
- Workforce management changes
- SDLC/PLC integration
- Annual plan review cycle
- Exercise results

Organizations must foster collaborative relationships with key stakeholders to encourage business participation and to ensure that plans remain relevant to the business. They should develop a distributed, collaborative BCM organizational model (see Figure 4) that meets their culture so that they encourage business participation.

Figure 4. Sample BCM Program Office Organization Model



Source: Gartner (February 2010)

Do not create a bottleneck situation by having BCM plans developed by the enterprise BCM office or IT DRM office. In each division, line of business, business unit or department, a person must be assigned the responsibility for recovery activities. The role of the enterprise BCM office is to develop the framework, procedures for plan creation and management, and the toolset to be used to develop all BCM plans.

4.0 Best Practice No. 3: BCM Plans Must Follow a Standard Process and Formality, and Not Be Done on an Ad Hoc Basis

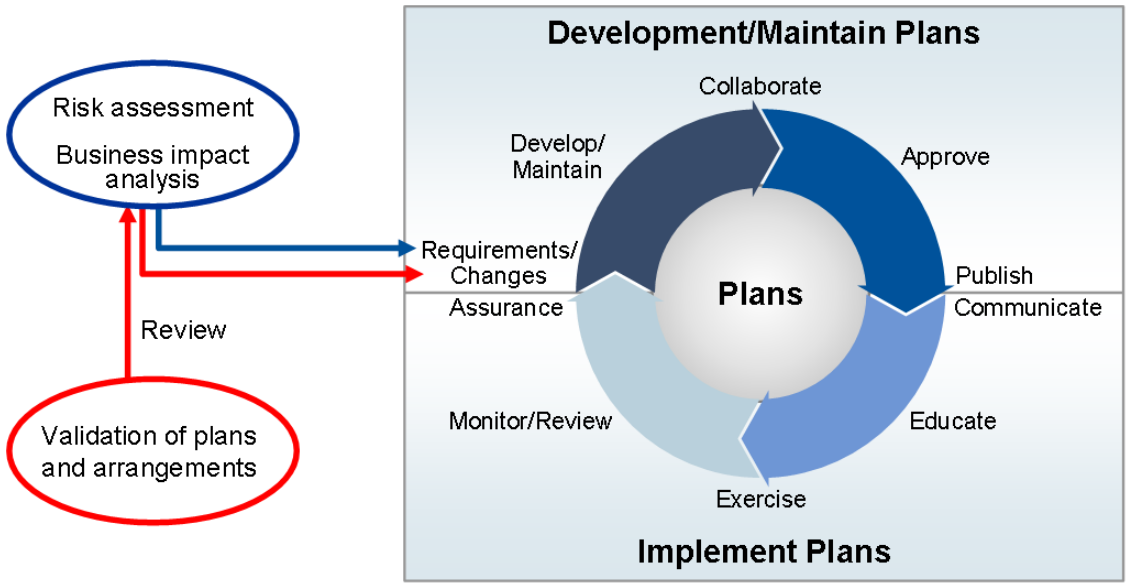
A formal, process-oriented BCM plan management strategy will ensure that BCM plans address the availability risks and needs of the business. Issues included in the strategy are:

- Establishing what the availability risks and needs are, including compliance requirements and identified control weaknesses.
- Considering who the audience will be. A BCM plan for end users is likely to use different terminology than a BCM plan geared to IT system administrators. Express the BCM plan in such a way that they can see the benefit to them.
- Establishing a process to ensure that there is early consensus by business, IT and other stakeholders on BCM plan content.
- Defining a standard and structure for BCM plan documents and for standards, procedures and guidelines.

- Obtaining and understanding a cross-functional culture.
- Defining a BCM plan repository.

The initial requirements for BCM plan development are obtained through risk assessments to identify what can cause disruption, and through a BIA to establish the impact and recovery resource needs should there be a disruption. Both practices require input from business process owners. Information from the risk assessment and BIA is used to subsequently develop a recovery strategy and to implement recovery arrangements, including recovery teams, alternate processing sites and recovery infrastructure (see Figure 5).

Figure 5. BCM Plan Management Strategy

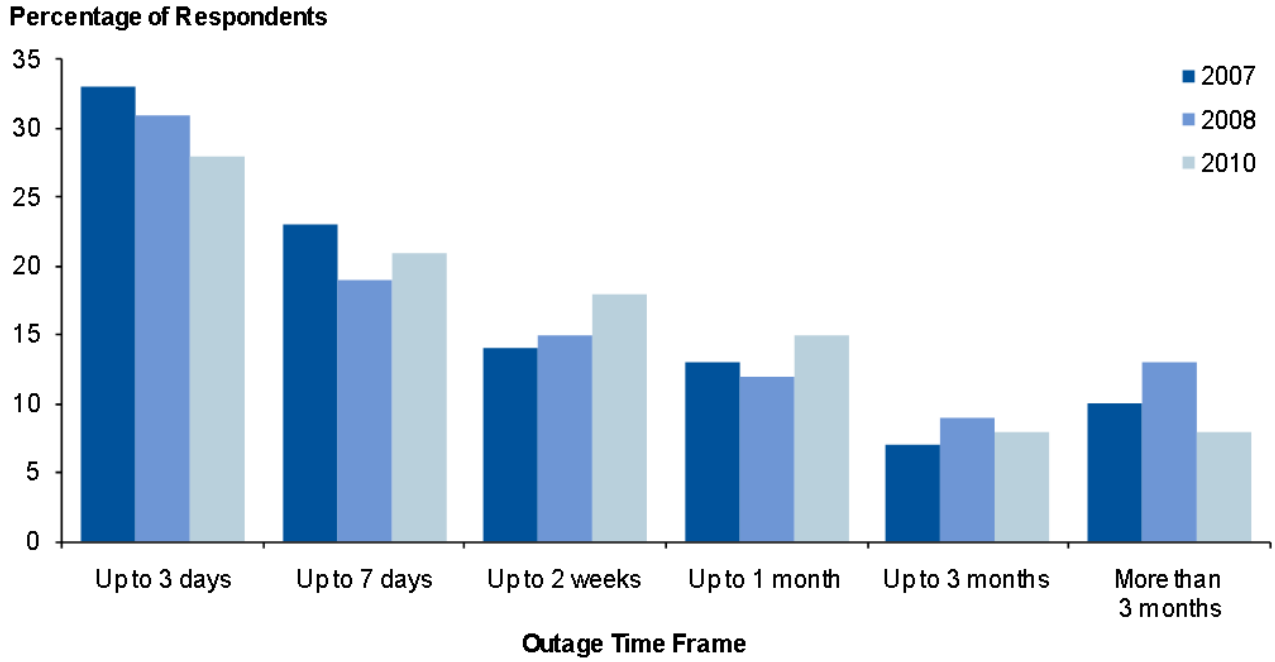


Source: Gartner (February 2010)

5.0 Best Practice No. 4: BCM Plans Must Be Developed to Cover a Longer Outage Time Frame

Another reason why BCM plans are not effective is because they are built for an outage time frame that is too short; they don't include enough business processes and associated resources to cover a crisis that lasts longer than expected. Results from our last three Risk and Security Surveys show that almost 60% of organizations plan for their longest outage to be seven days only. Although the number of firms planning for longer outage time frames is increased during the past three years, it is still too short a time frame. The impact of a disaster that lasts more than one week can have enormous negative effects on your revenue, reputation and brand. Regional incidents, terrorism, service provider outages and pandemics can easily last longer than seven days. The more mature your program, the longer the time frame of your worst-case scenario for which you've planned should be (see Figure 6).

Figure 6. Length of Worst-Case Scenario Outage Time Frames Being Planned for in BCM Programs — 2007 (n=218), 2008 (n=139), 2010 (n=174)



Source: Gartner (February 2010)

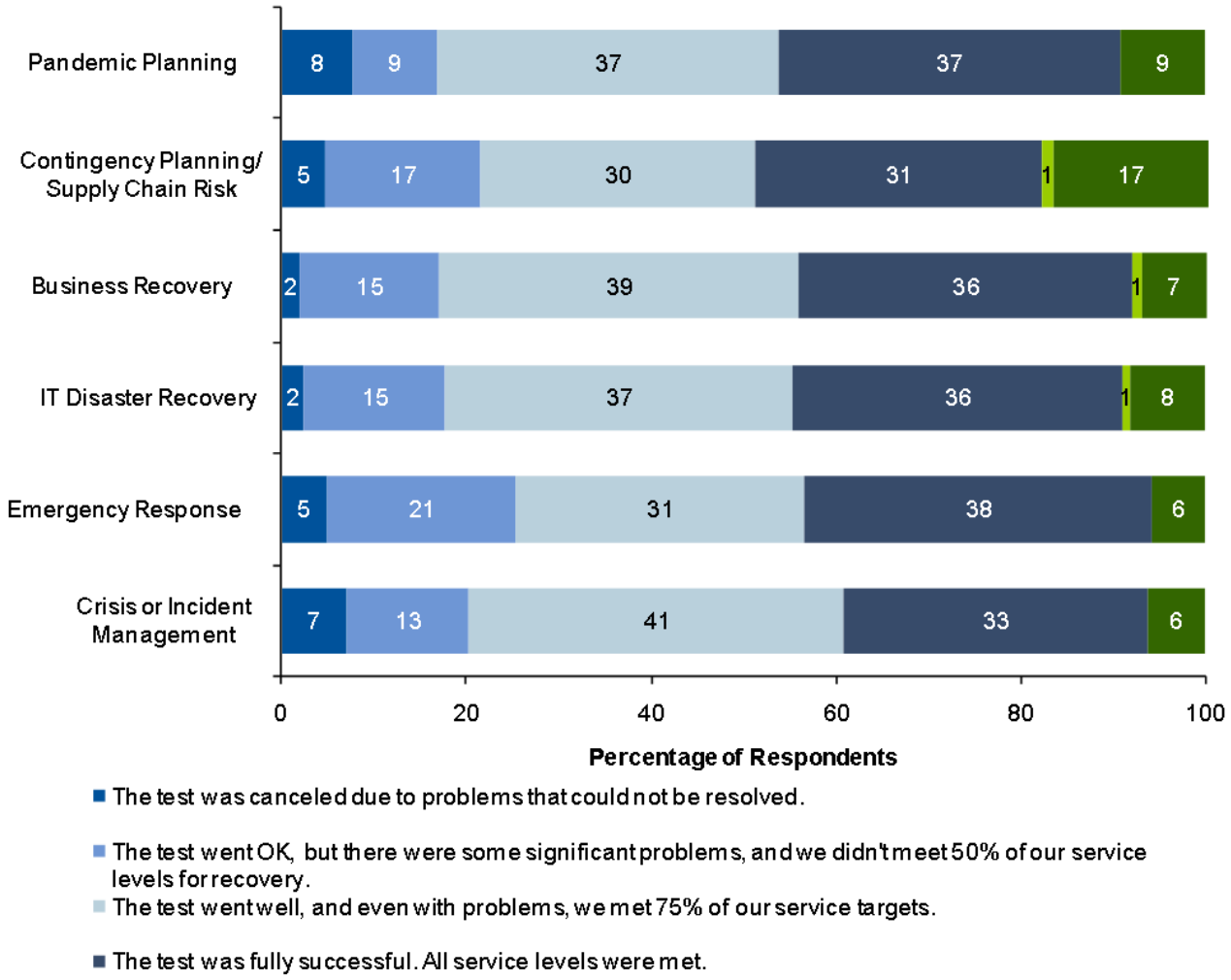
Planning for a longer outage time frame (at least 30 days) has multiple effects on the BCM/IT DRM plan. More people, technology and other corporate assets are required to be recovered, thereby increasing the overall cost of recovery.

6.0 Best Practice No. 5: BCM Plans Must Be Regularly Exercised

Having a plan is only a part of the maturity of the BCM/IT DRM program. Knowing that the plan works during an actual emergency is key to the survivability of the business. Testing, or exercising, of the BCM plans on a regular basis (for example, once a year) is the second most important part of a BCM program; conducting a BIA is the most critical process in the development of a recovery strategy and the development of associated BCM plans (see "Best Practices for Conducting a Business Impact Analysis"). Exercising BCM plans is the true test of whether or not plans meet availability requirements.

Among participants of Gartner's 2010 Risk and Security Survey, 35% report that their last plan exercise went well and met all their service targets (see Figure 7). Nine percent weren't sure of the outcome of their last plan exercise. That leaves 56% of survey participants reporting that they had problems with the exercise, which should not give any organization a good sense of security that their BCM or IT DRM program will meet business recovery needs when a crisis strikes. Therefore, do not rest on your laurels. Establish an annual IT DRM plan exercise schedule so that you don't risk underfunding the organization's overall BCM program.

Figure 7. Outcome of the Last Exercise (2010 Risk and Security Survey, n = 128)

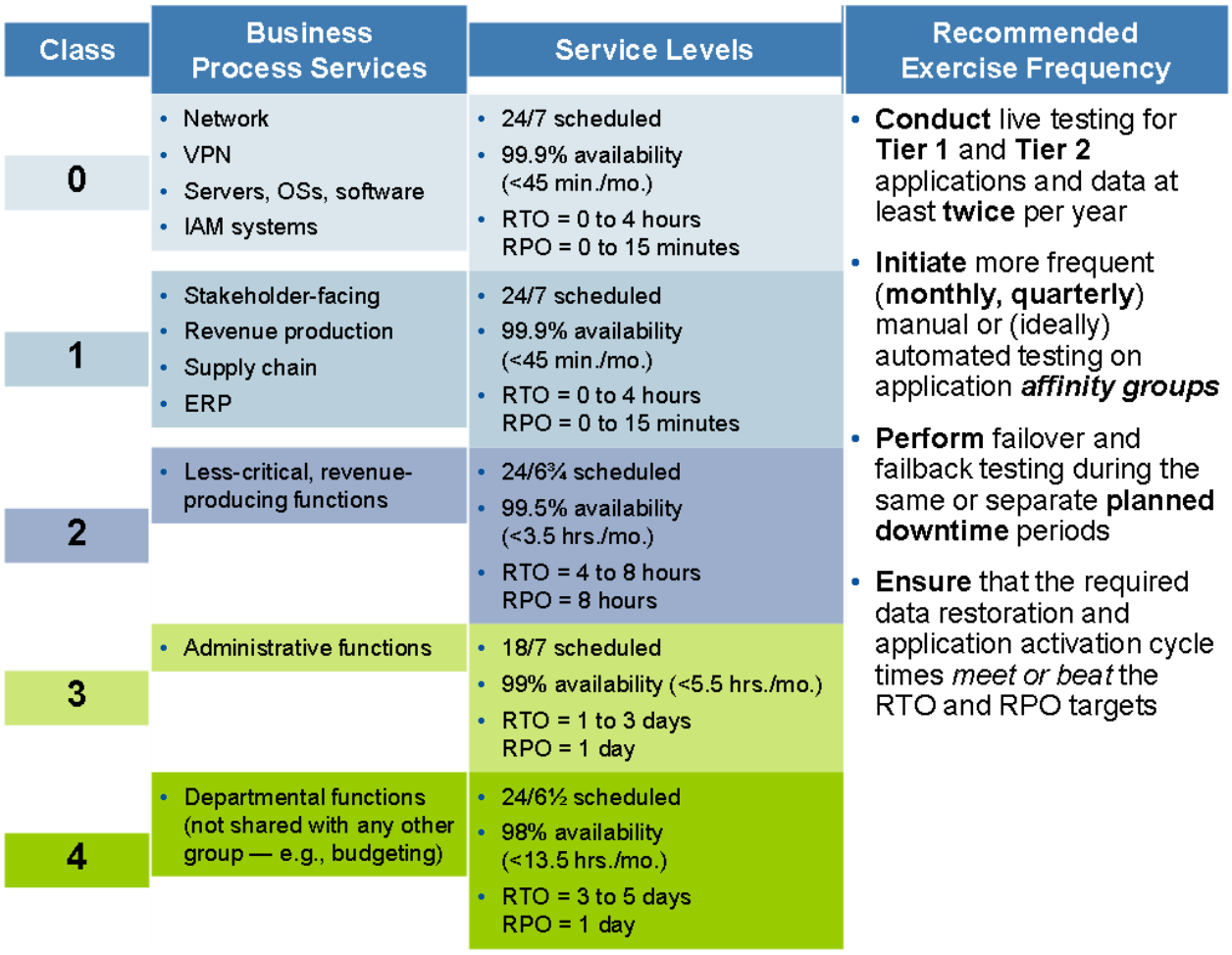


Source: Gartner (February 2010)

The investment made in exercising recovery plans cannot be overemphasized. Business units and IT organizations need to agree on the requisite number of exercises annually. Based on this exercising schedule, you must develop a specific budget and funding mechanism to ensure resource and site availability.

To develop the exercise budget and schedule, Gartner recommends that organizations develop a service-level classification system (see Figure 8). Service-level definitions should include scheduled uptime, percentage availability in scheduled uptime, and recovery-time and point objectives. For example, in Figure 8, Classes 0 and 1 application services have high availability requirements and also very low RTO and RPO targets, and the enterprise would suffer irreparable harm if these services were unavailable. Not all applications in a critical business process would be grouped in Class 1 — rather, only those deemed most critical or with the most downtime effect. The IT DRM architecture for Class 1, and even Class 2, would result in an implementation across two physical sites to meet availability/recovery needs. Once the processes have been classified, you can determine the type of exercise and frequency that would be most effective for that class of business service.

Figure 8. Sample IT DRM Plan Exercise Classification Scheme



Source: Gartner (February 2010)

7.0 Best Practice No. 6: Develop a Structured Framework of BCM Plans

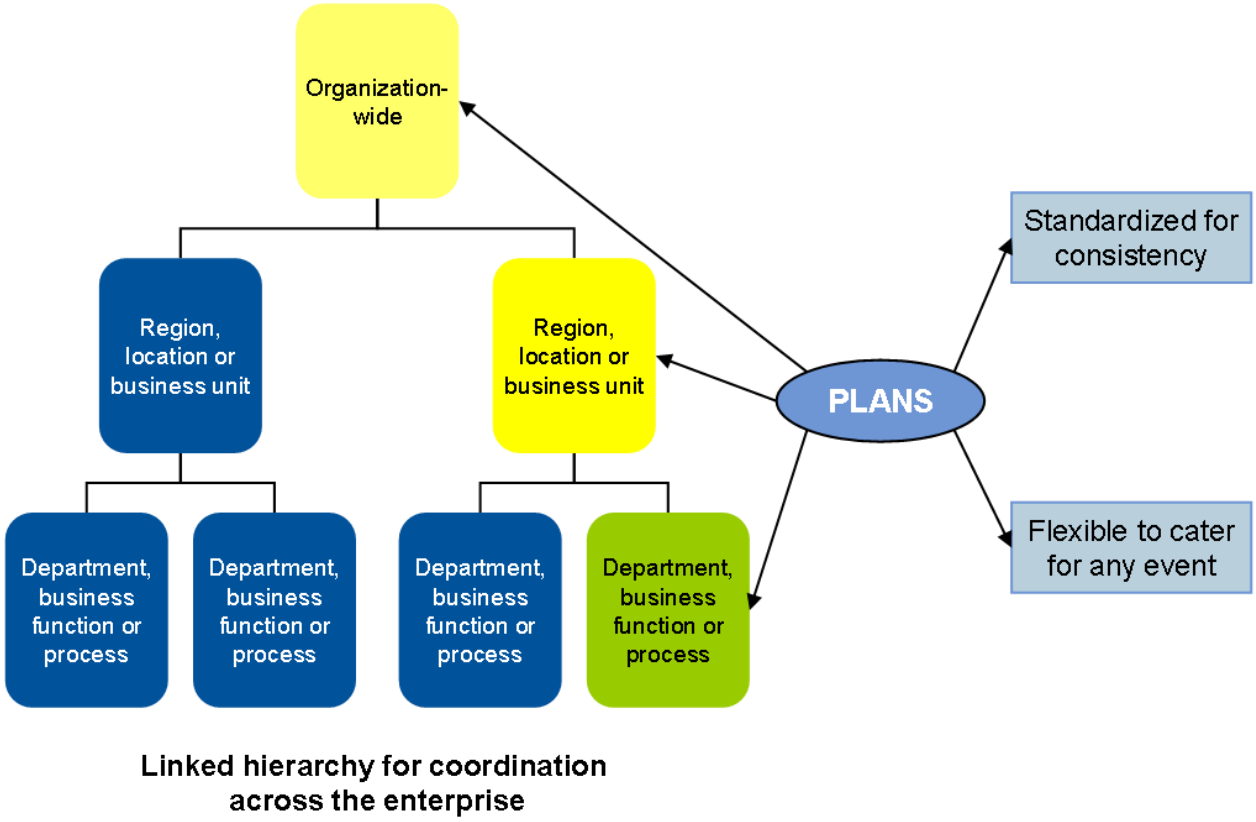
In most organizations, BCM plans refer to a framework of plans required to respond to an incident and restore business operations to a minimum acceptable service level within a specified time frame. They must be developed to reflect the organization's context and to provide the required capability to support the achievement of critical objectives. In some circumstances, regulatory requirements or industry standards will provide specific guidance on the content (for example, emergency management plans). However, for the majority of plans, there is no predetermined standard. The components and contents of BCM plans vary from organization to organization, and have a different level of detail based on the scale, environment, culture and technical complexity of the organization.

A highly decentralized organization with regional offices having autonomous and discrete processes should have a discrete set of plans for each office. Organizations with a single operating location most likely already has common processes for workforce management, so they are likely to have discrete crisis and emergency response plans, but with a common workforce

continuity plan. The BIA is a key input into deciding how to structure plans to focus on key processes.

Organizations must develop a structured framework of BCM plans (see Figure 9) to ensure that key processes can be recovered and that focuses on flexibility for resilience, rather than on specific scenarios. The structure should be designed for collaboration during development, and flexibility during exercising and incident response.

Figure 9. BCM Plan Structure

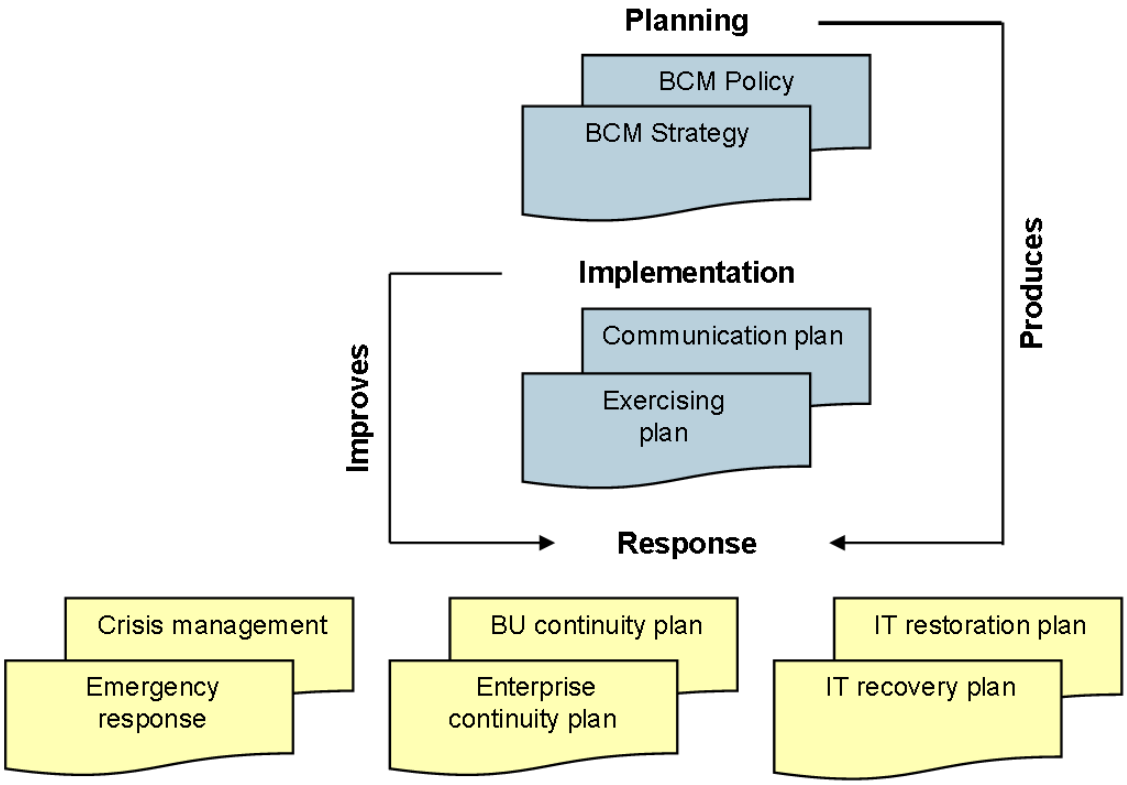


Source: Gartner (February 2010)

8.0 Best Practice No. 7: Keep BCM Plans Relevant to Their Purpose

The BCM program delivers numerous documents encompassing BCM strategy and planning documents, BCM implementation documents and BCM response, recovery, and restoration documents (see Figure 10). BCM plans (response, recovery and restoration plans — see Figure 1) are a set of related documents, but they do not include all the documents developed in BCM planning. They should be relevant to just that: responding to, recovering and eventually restoring from an event. For this reason, they need to be structured within a framework that simplifies maintenance, communication and exercising. They should not include superfluous policy and strategy-type information, or waffle to impress the auditors. Plans should be unambiguous and free of jargon, because the person applying them may not be familiar with the document or the business process at the time of an event.

Figure 10. BCM Program Documents



Source: Gartner (February 2010)

Organizations must:

- Keep information relevant to the objective of the plan; exclude superfluous strategy and policy-type information.
- Put details that change often into appendixes (such as call trees and technical specifications).
- Keep post-event procedures separate from BCM plans (such as post-mortem, expenditure analysis and reimbursement).
- Keep plans simple, and minimize jargon. Plans should be understandable by second-tier personnel, and, in some rare cases, someone unfamiliar with the process when they have to be used in a real disaster.

9.0 Best Practice No. 8: Provide Relevant Information in BCM Plans to Facilitate Recovery Within Defined Recovery Time Frames

The content of a BCM plan must include a minimum set of information to guide response, recovery and restoration processes within defined time frames, including:

- Contextual information defining the plan purpose, scope, business function, and processes and objective

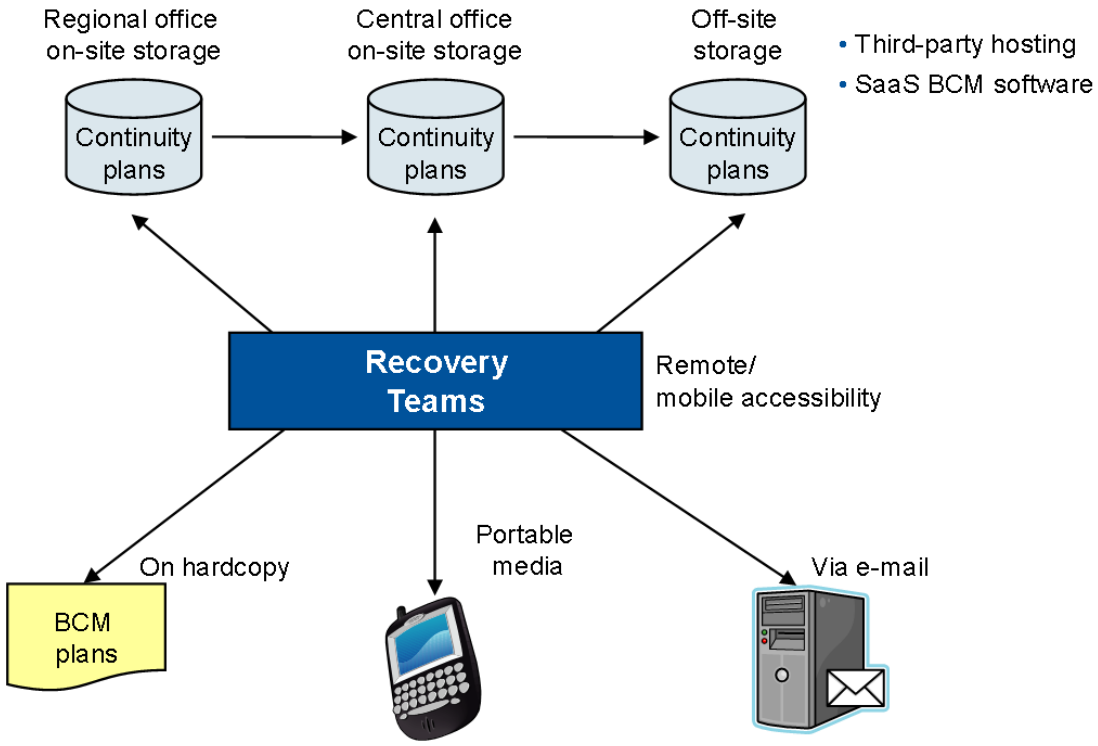
- Document management information, including version control, owner, review status, audit and previous activation dates
- Triggers/conditions and procedures for plan activation (which may differ according to plan purpose) and plan stand-down
- Compliance, regulatory, contractual or policy obligations
- Performance objectives, including RTO, RPO, critical success measures and timeline of execution to ascertain whether or not the recovery operation has been successful
- Resources, including emergency supplies and equipment, alternate premises, workforce recovery, technology and equipment, transportation, information, documentation, and vital records
- Roles (primary, secondary and tertiary roles for recovery purposes — you can't be sure that your A team will be available), responsibilities and contact details (including continuity teams, external parties and emergency services), as well as mobilization procedures, personnel locations and so forth
- Related documents needed for the execution of the BCM plan
- Internal and external communications
- Specific recovery and operational tasks to be used during the event as well as post-event

Day-to-day business and IT manuals are not part of a BCM plan. They should be available at the recovery site, but are not part of a BCM plan.

10.0 Best Practice No. 9: Establish a Central Repository and Administration Process for BCM Plan Maintenance

The use of a central physical repository managed by an enterprisewide document administration strategy for creating, updating, storing, distributing and reporting the status of BCM plans enforces a single authoritative source for every plan and ensures that plans are kept up to date; information that needs to be included in multiple plans across multiple offices is more easily updated and distributed, and document governance can be enforced. Each plan can then be shared as widely or as narrowly across the enterprise and on different storage devices, according to business need (see Figure 11). See "Q&A for Business Continuity Management: Best Practices for Plan Management" to read more about best practices for plan management.

Figure 11. BCM Plan Storage and Distribution



Source: Gartner (February 2010)

Ensuring that the most recent version of a BCM plan is always available to those who will need to use it requires the following actions:

- Establish a central repository for all BCM program documents, including BCM plans.
- Version and change management controls should be implemented to ensure that changes are only made to the most current version of the plan. Because plans are usually made up of multiple documents, keeping all the documents synchronized is crucial.
- A tracking method or workflow should be implemented to record which parts of the plan are complete, up-to-date and approved for use, as well as those in the process of being updated and those that need additional work.
- An audit trail, with notices sent to plan owners in some cases, should be kept to record plan document activities, such as plan creation, plan update, plan printing and, in some cases, access to plans that contain confidential organizational information.

The enterprise BCM Office is responsible for:

- Administering the central repository
- Facilitating and monitoring the BCM plan update process, that version control is applied, and that latest version is distributed
- Liaising with plan owners to monitor change requirements and the status of changes in progress

- Looking for ways to reduce redundancy
- Enforcing standardization of the BCM plan management strategy and practices

11.0 Best Practice No. 10: Use Automation to Mature BCM Plan Management

Organizations should investigate the use of automation for BCM plan management. As noted in the Introduction, the majority of organizations use office automation tools (word processors, organization charts, graphics development, project management and so forth) to develop, maintain and exercise BCM plans. However, BCMP tools are gaining adoption in BCM program offices because they help to enhance, streamline and enforce the implementation of BCM program and plan management practices across multiple lines of business and multiple locations in a collaborative manner. A caution: If you don't have a well-defined process for your BCM program already in place, using these tools can just make an ad hoc program much more visible to management, and therefore, you lose credibility for the program overall.

BCMP tools embed standard BCM planning practices and procedures (risk assessment, BIA, plan management, exercising and so forth) that would otherwise be done manually. By using such tools, BCM planners who are new to the field can take advantage of the planning methodologies of experienced planners. First, BCMP tools organize the planning process, speeding it along without losing important information. The long-term value of BCMP tools resides in their capabilities to keep BCM plans current and viable, preferably with automatically generated reminders to stakeholders with update responsibility. The tools allow updates be made to the plan quickly and efficiently (for example, automatically updating the plan's call-list records with the latest contact information of employees when the corporate HR database changes). The tools can automatically distribute plan updates to all recovery team members so that they have the most current version available to them — even on their PDAs.

In addition to BCMP tools, adoption is growing for the use of crisis/incident management software tools for governments and enterprises during an actual crisis. These tools are used to manage the execution of BCM plans; manage relationships with all organization stakeholders, as well as with the press; manage incident/situation tasks; manage expenses incurred during the recovery effort; communicate information internally, as well as externally; and provide reports for post-mortem reviews of the incident for process improvement efforts. These tools store BCM plans developed in office automation tools or BCMP tools so that they are available to all recovery team members.

Organizations should investigate and implement BCMP tools and crisis/incident management tools to manage activities during a crisis, as well as to make BCM plans accessible to recovery team members during an exercise or upon an actual crisis activation. More information regarding BCMP and crisis/incident management tools can be found in the "Hype Cycle for Business Continuity Management, 2009."

RECOMMENDED READING

"Activity Cycle Overview: Business Continuity Manager Role"

"Business Continuity Management Defined, 2008"

"Cool Vendors in Risk Management and Compliance, 2009"

"How the Business Continuity Management Professional Can Survive the Worldwide Economic Crisis"

"Hype Cycle for Business Continuity Management, 2009"

"Predicts 2009: Business Continuity Management Juggles Standardization, Cost and Outsourcing Risk"

"Q&A for Business Continuity Management: Best Practices for Plan Management"

"Toolkit: Business Continuity Management Charter Best Practices and Template"

"Toolkit: Risk Program Maturity Assessment 1.2"

"Predicts 2010: The Role of Business Continuity Management Continues to Expand and Extend"

"A New Approach: Obtain Business Ownership and Investment Commitment for Business Continuity and Resilience Management Through Key Performance and Risk Indicator Mapping"

"Best Practices for Aligning Recovery and Business-as-Usual Access Requirements"

"How to Understand and Select Business Continuity Management Software"

"Automate Recovery Planning With Business Continuity Planning Tools"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner