

## DATA SECURITY MANAGEMENT

# REENGINEERING THE BUSINESS CONTINUITY PLANNING PROCESS

Carl B. Jackson

## INSIDE

Continuity Planning: Management Awareness High — Execution Effectiveness Low; A Receipt for Radical Change: CP Process Improvement; The Process Approach to Continuity Planning; Moving to a CP Process Improvement Environment; How Does One Get There? The Concept of the CP Value Journey; The Need for Organizational Change Management; How Is Success Measured? Balanced Scorecard Concept; What about Continuity Planning for Web-Based Applications?

The initial version of this article was written for the 1999 edition of the *Information Security Management Handbook*. Since then, E-commerce has seized the spotlight and Web-based technologies are the emerging solution for almost everything. The constant throughout these occurrences is that no matter what the climate, fundamental business processes have changed little. And, as always, the focus of any business impact assessment is to assess the time-critical priority of these business processes. With these more recent realities in mind, this chapter has been updated and is now offered for the reader's consideration.

**PAYOFF IDEA**

The failure of organizations to measure the success of their continuity planning implementations has led to an endless cycle of plan development and decline. (The primary reason for this is that a meaningful set of continuity planning measurements has not been adopted to fit the organization's future-state goals.) Because these measurements are lacking, expectations of both top management and those responsible for continuity planning often go unfulfilled. This requires that organizations radically change how they implement continuity planning. This change should include adopting and utilizing a business process improvement approach. Finally, because Web-based business processes require 24x7 uptime, implementation of continuous availability disciplines are necessary to ensure that the continuity planning process is as fully developed as it should be.

**CONTINUITY PLANNING: MANAGEMENT  
AWARENESS HIGH — EXECUTION  
EFFECTIVENESS LOW**

The failure of organizations to accurately measure the contributions of the continuity planning (CP) process to their overall success has

---

led to a downward spiraling cycle of the total business continuity program. The recurring downward spin or decomposition includes planning, testing, maintenance, decline->>-re-planning, testing, maintenance, decline->>-re-planning, testing, maintenance, decline, etc.

In the past, *Contingency Planning & Management (CPM)/Ernst & Young Continuity Planning Benchmark* surveys have repeatedly confirmed that continuity planning (CP) is ranked as being either “extremely important” or “very important” to executive management. The most recent *2000–2001 CPM/KPMG Continuity Planning Survey*<sup>1</sup> clearly supports this observation. This study indicates that a growing number of CP professional positions are migrating from the IT infrastructure to corporate or general management positions; however, CP reporting within the IT organization is still the norm. Approximately 40 percent of CP professionals currently report to IT, while around 30 percent report to corporate positions.

### **Continuity Planning Measurements**

While the trends of this survey are encouraging, there is a continuing indication of a disconnect between executive management’s perceptions of CP objectives and the manner in which they measure its value. Traditionally, CP effectiveness was measured in terms of a pass/fail grade on a mainframe recovery test, or on the perceived benefits of backup/recovery sites and redundant telecommunications weighed against the expense for these capabilities. The trouble with these types of metrics is that they only measure CP direct costs, or indirect perceptions as to whether a test was effectively executed. These metrics do not indicate whether a test validates the appropriate infrastructure elements or even whether it is thorough enough to test a component until it fails, thereby extending the reach and usefulness of the test scenario.

Thus, one might inquire as to the correct measures to use. While financial measurements do constitute *one* measure of the CP process, others measure the CPs contribution to the organization in terms of quality and effectiveness, which are not strictly weighed in monetary terms. The contributions that a well-run CP process can make to an organization include:

- Sustaining growth and innovation
- Enhancing customer satisfaction
- Providing people needs
- Improving overall mission-critical process quality
- Providing for practical financial metrics

---

## **A RECEIPT FOR RADICAL CHANGE: CP PROCESS IMPROVEMENT**

Just prior to the millennium, experts in organizational management efficiency began introducing performance process improvement disciplines. These process improvement disciplines have been slowly adopted across many industries and companies for improvement of general manufacturing and administrative business processes. The basis of these and other improvement efforts was the concept that an organization's *processes* (Process; see [Exhibit 1](#)) constituted the organization's fundamental lifeblood and, if made more effective and more efficient, could dramatically decrease errors and increase organizational productivity.

An organization's processes are a series of successive activities; and when they are executed in the aggregate, they constitute the foundation of the organization's mission. These processes are intertwined throughout the organization's infrastructure (individual business units, divisions, plants, etc.) and are tied to the organization's supporting structures (data processing, communications networks, physical facilities, people, etc.).

A key concept of the process improvement and reengineering movement revolves around identification of process enablers and barriers (see [Exhibit 1](#)). These enablers and barriers take many forms (people, technology, facilities, etc.) and must be understood and taken into consideration when introducing radical change into the organization.

The preceding narration provides the backdrop for the idea of focusing on continuity planning not as a project, but as a continuous process, that must be designed to support the other mission-critical processes of the organization. Therefore, the idea was born of adopting a continuous process approach to CP, along with understanding and addressing the people, technology, facility, etc. enablers and barriers. This constitutes a significant or even radical change in thinking from the manner in which recovery planning has been traditionally viewed and executed.

### **Radical Changes Mandated**

High awareness of management and low CP execution effectiveness, coupled with the lack of consistent and meaningful CP measurements, call for radical changes in the manner in which one executes recovery planning responsibilities. The techniques used to develop mainframe-oriented disaster recovery (DR) plans of the 1980s and 1990s consisted of five to seven distinct stages, depending on whose methodology was being used, that required the recovery planner to:

1. Establish a project team and a supporting infrastructure to develop the plans.
2. Conduct a threat or risk management review to identify likely threat scenarios to be addressed in the recovery plans.

---

## EXHIBIT 1 — Definitions

---

**Activities:** Activities are things that go on within a process or sub-process. They are usually performed by units of one (one person or one department). An activity is usually documented in an instruction. The instruction should document the tasks that make up the activity.

**Benchmarking:** Benchmarking is a systematic way to identify, understand, and creatively evolve superior products, services, designs, equipment, processes, and practices to improve the organization's real performance by studying how other organizations are performing the same or similar operations.

**Business process improvement:** Business process improvement (BPI) is a methodology that is designed to bring about self-function improvements in administrative and support processes using approaches such as FAST, process benchmarking, process redesign, and process reengineering.

**Comparative analysis:** Comparative analysis (CA) is the act of comparing a set of measurements to another set of measurements for similar items.

**Enabler:** An enabler is a technical or organizational facility/resource that makes it possible to perform a task, activity, or process. Examples of technical enablers are personal computers, copying equipment, decentralized data processing, voice response, etc. Examples of organizational enablers are enhancement, self-management, communications, education, etc.

**Fast analysis solution technique:** FAST is a breakthrough approach that focuses a group's attention on a single process for a one- or two-day meeting to define how the group can improve the process over the next 90 days. Before the end of the meeting, management approves or rejects the proposed improvements.

**Future state solution:** A combination of corrective actions and changes that can be applied to the item (process) under study to increase its value to its stakeholders.

**Information:** Information is data that has been analyzed, shared, and understood.

**Major processes:** A major process is a process that usually involves more than one function within the organization structure, and its operation has a significant impact on the way the organization functions. When a major process is too complex to be flow-charted at the activity level, it is often divided into sub-processes.

**Organization:** An organization is any group, company, corporation, division, department, plant, or sales office.

**Process:** A process is a logical, related, sequential (connected) set of activities that takes an input from a supplier, adds value to it, and produces an output to a customer.

**Sub-process:** A sub-process is a portion of a major process that accomplishes a specific objective in support of the major process.

**System:** A system is an assembly of components (hardware, software, procedures, human functions, and other resources) united by some form of regulated interaction to form an organized whole. It is a group of related processes that may or may not be connected.

**Tasks:** Tasks are individual elements or subsets of an activity. Normally, tasks relate to how an item performs a specific assignment.

From Harrington, H.J., Esseling, E.K.C., and Van Nimwegen, H., *Business Process Improvement Workbook*, McGraw-Hill, 1997, 1–20.

- 
3. Conduct a business impact analysis (BIA) to identify and prioritize time-critical business applications/networks and determine maximum tolerable downtimes.
  4. Select an appropriate recovery alternative that effectively addressed the recovery priorities and time-frames mandated by the BIA.
  5. Document and implement the recovery plans.
  6. Establish and adopt an ongoing testing and maintenance strategy.

### **Shortcomings of the Traditional Disaster Recovery Planning Approach**

The old approach worked well when disaster recovery of “glass-house” mainframe infrastructures was the norm. It even worked fairly well when it came to integrating the evolving distributed/client/server systems into the overall recovery planning infrastructure. However, when organizations became concerned with business unit recovery planning, the traditional DR methodology was ineffective in designing and implementing business unit/function recovery plans. Of primary concern when attempting to implement enterprisewide recovery plans was the issue of functional interdependencies. Recovery planners became obsessed with identification of interdependencies between business units and functions, as well as the interdependencies between business units and the technological services supporting time-critical functions within these business units.

### **Losing Track of the Interdependencies**

The ability to keep track of departmental interdependencies for CP purposes was extremely difficult and most methods for accomplishing this were ineffective. Numerous circumstances made consistent tracking of interdependencies difficult to achieve. Circumstances affecting interdependencies revolve around the rapid rates of change that most modern organizations are undergoing. These include reorganization/restructuring, personnel relocation, changes in the competitive environment, and outsourcing. Every time an organizational structure changes, the CPs must change and the interdependencies must be reassessed; and the more rapid the change, the more daunting the CP reshuffling. Because many functional interdependencies could not be tracked, CP integrity was lost and the overall functionality of the CP was impaired. There seemed to be no easy answers to this dilemma.

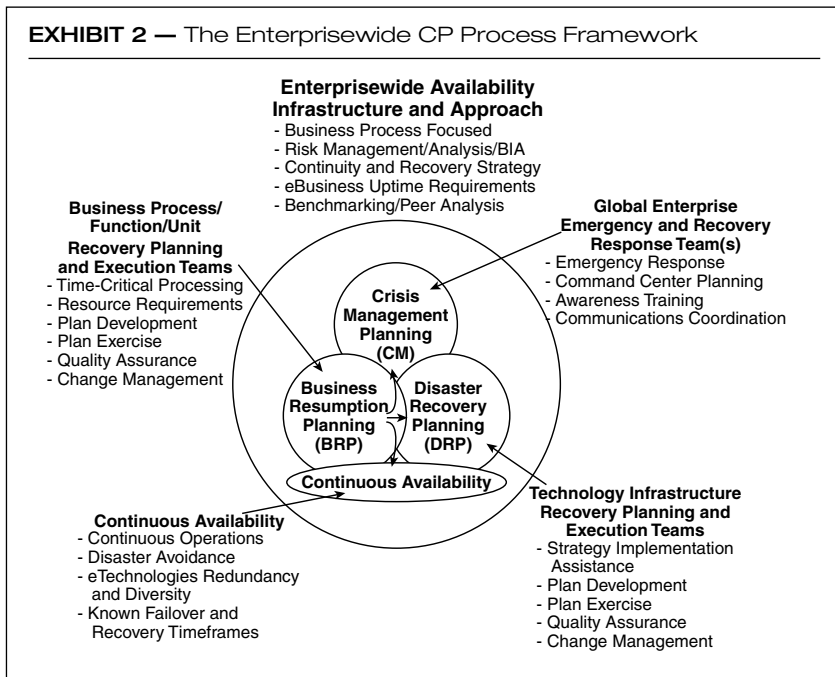
### **Interdependencies Are Business Processes**

Why are interdependencies of concern? And what, typically, are the interdependencies? The answer is that, to a large degree, these interdependencies are the business processes of the organization and they are of

concern because they must function in order to fulfill the organization's mission. Approaching recovery planning challenges with a business process viewpoint can, to a large extent, mitigate the problems associated with losing interdependencies, and also ensure that the focus of recovery planning efforts is one of the most crucial components of the organization. Understanding how the organization's time-critical business processes are structured will assist the recovery planner in mapping the processes back to the business units/departments; supporting technological systems, networks, facilities, vital records, people, etc.; and keeping track of the processes during reorganizations or during times of change.

**THE PROCESS APPROACH TO CONTINUITY PLANNING**

Traditional approaches to mainframe-focused disaster recovery planning emphasized the need to recover the organization's technological and communications platforms. Today, many companies have shifted away from technology recovery and toward continuity of prioritized business processes and the development of specific business process recovery plans. Many large corporations use the process reengineering/improvement disciplines to increase overall organizational productivity. CP itself should also be viewed as such a process. Exhibit 2 provides a graphical representation of how the enterprisewide CP process framework should look.



---

This approach to continuity planning consolidates three traditional continuity planning disciplines, as follows:

1. *IT disaster recovery planning (DRP)*. Traditional IT DRP addresses the continuity planning needs of the organizations' IT infrastructures, including centralized and decentralized IT capabilities and includes both voice and data communications network support services.
2. *Business operations resumption planning (BRP)*. Traditional BRP addresses the continuity of an organization's business operations (e.g., accounting, purchasing, etc.) should they lose access to their supporting resources (e.g., IT, communications network, facilities, external agent relationships, etc.).
3. *Crisis management planning (CMP)*. CMP focuses on assisting the client organization to develop an effective and efficient enterprisewide emergency/disaster response capability. This response capability includes forming appropriate management teams and training their members in reacting to serious company emergency situations (e.g., hurricane, earthquake, flood, fire, serious hacker or virus damage, etc.). CMP also encompasses response to life-safety issues for personnel during a crisis or response to disaster.
4. *Continuous availability (CA)*. In contrast to the other CP components as explained above, the recovery time objective (RTO) for recovery of infrastructure support resources in a 24x7 environment has diminished to *zero* time. That is, the client organization cannot afford to lose operational capabilities for even a very short period of time without significant financial (revenue loss, extra expense) or operational (customer service, loss of confidence) impact. The CA service focuses on maintaining the highest uptime of support infrastructures to 99 percent and higher.

## **MOVING TO A CP PROCESS IMPROVEMENT ENVIRONMENT**

### **Route Map Profile and High-Level CP Process Approach**

A practical, high-level approach to CP process improvement is demonstrated by breaking down the CP process into individual sub-process components as shown in [Exhibit 3](#).

The six major components of the continuity planning business process are described below.

**Current State Assessment/Ongoing Assessment.** Understanding the approach to enterprisewide continuity planning as illustrated in [Exhibit 3](#), one can measure the "health" of the continuity planning process. During this process, existing continuity planning business sub-processes are assessed to gauge their overall effectiveness. It is sometimes useful





---

to employ gap analysis techniques to understand current state, desired future state, and then understand the people, process, and technology barriers and enablers that stand between the current state and the future state. An approach to co-development of current state/future state visioning sessions is illustrated in [Exhibit 4](#).

The current state assessment process also involves identifying and determining how the organization “values” the CP process and measures its success (often overlooked and often leading to the failure of the CP process). Also during this process, an organization’s business processes are examined to determine the impact of loss or interruption of service on the overall business through performance of a business impact assessment (BIA). The goal of the BIA is to prioritize business processes and assign the recovery time objective (RTO) for their recovery, as well as for the recovery of their support resources. An important outcome of this activity is the mapping of time-critical processes to their support resources (e.g., IT applications, networks, facilities, communities of interest, etc.).

**Process Risk and Impact Baseline.** During this process, potential risks and vulnerabilities are assessed, and strategies and programs are developed to mitigate or eliminate those risks. The stand-alone risk management review (RMR) commonly looks at the security of physical, environmental, and information capabilities of the organization. In general, the RMR should identify or discuss the following areas:

- Potential threats
- Physical and environmental security
- Information security
- Recoverability of time-critical support functions
- Single-points-of-failure
- Problem and change management
- Business interruption and extra expense insurance
- An offsite storage program, etc.

**Strategy Development.** This process involves facilitating a workshop or series of workshops designed to identify and document the most appropriate recovery alternative to CP challenges (e.g., determining if a hotsite is needed for IT continuity purposes, determining if additional communications circuits should be installed in a networking environment, determining if additional workspace is needed in a business operations environment, etc.). Using the information derived from the risk assessments above, design long-term testing, maintenance, awareness, training, and measurement strategies.

---

**Continuity Plan Infrastructure.** During plan development, all policies, guidelines, continuity measures, and continuity plans are formally documented. Structure the CP environment to identify plan owners and project management teams, and to ensure the successful development of the plan. In addition, tie the continuity plans to the overall IT continuity plan and crisis management infrastructure.

**Implementation.** During this phase, the initial versions of the continuity or crisis management plans are implemented across the enterprise environment. Also during this phase, long-term testing, maintenance, awareness, training, and measurement strategies are implemented.

**Operate Environment.** This phase involves the constant review and maintenance of the continuity and crisis management plans. In addition, this phase may entail maintenance of the ongoing viability of the overall continuity and crisis management business processes.

#### **HOW DOES ONE GET THERE? THE CONCEPT OF THE CP VALUE JOURNEY**

The CP value journey is a helpful mechanism for co-development of CP expectations by the organization's top management group and those responsible for recovery planning. To achieve a successful and measurable recovery planning process, the following checkpoints along the CP value journey should be considered and agreed upon. The checkpoints include:

- *Defining success.* Define what a successful CP implementation will look like. What is the future state?
- *Aligning the CP with business strategy.* Challenge objectives to ensure that the CP effort has a business-centric focus.
- *Charting an improvement strategy.* Benchmark where the organization and the organization's peers are, the organization's goals based on their present position as compared to their peers, and which critical initiatives will help the organization achieve its goals.
- *Becoming an accelerator.* Accelerate the implementation of the organization's CP strategies and processes. In today's environment, speed is a critical success factor for most companies.
- *Creating a winning team.* Build an internal/external team that can help lead the company through CP assessment, development, and implementation.
- *Assessing business needs.* Assess time-critical business process dependence on the supporting infrastructure.
- *Documenting the plans.* Develop continuity plans that focus on ensuring that time-critical business processes will be available.

- 
- *Enabling the people.* Implement mechanisms that help enable rapid reaction and recovery in times of emergency, such as training programs, a clear organizational structure, and a detailed leadership and management plan.
  - *Completing the organization's CP strategy.* Position the organization to complete the operational and personnel related milestones necessary to ensure success.
  - *Delivering value.* Focus on achieving the organization's goals while simultaneously envisioning the future and considering organizational change.
  - *Renewing/recreating.* Challenge the new CP process structure and organizational management to continue to adapt and meet the challenges of demonstrating availability and recoverability.

### **The Value Journey Facilitates Meaningful Dialogue**

This value journey technique for raising the awareness level of management helps to both facilitate meaningful discussions about the CP process and ensure that the resulting CP strategies truly add value. As discussed later, this value-added concept will also provide additional metrics by which the success of the overall CP process can be measured.

### **The Need for Organizational Change Management**

In addition to the approaches of CP process improvement and the CP value journey mentioned above, the need to introduce people-oriented organizational change management (OCM) concepts is an important component in implementing a successful CP process.

H. James Harrington et al., in their book *Business Process Improvement Workbook*,<sup>2</sup> point out that applying process improvement approaches can often cause trouble unless the organization manages the change process. They state that, "Approaches like reengineering only succeed if we challenge and change our paradigms and our organization's culture. It is a fallacy to think that you can change the processes without changing the behavior patterns or the people who are responsible for operating these processes."<sup>3</sup>

Organizational change management concepts, including the identification of people enablers and barriers and the design of appropriate implementation plans that change behavior patterns, play an important role in shifting the CP project approach to one of CP process improvement. The authors also point out that, "There are a number of tools and techniques that are effective in managing the change process, such as pain management, change mapping, and synergy. The important thing is that every BPI (Business Process Improvement) program must have a very

comprehensive change management plan built into it, and this plan must be effectively implemented.”<sup>4</sup>

Therefore, it is incumbent on the recovery planner to ensure that, as the concept of the CP process evolves within the organization, appropriate OCM techniques are considered and included as an integral component of the overall deployment effort.

#### HOW IS SUCCESS MEASURED? BALANCED SCORECARD CONCEPT<sup>5</sup>

A complement to the CP process improvement approach is the establishment of meaningful measures or metrics that the organization can use to weigh the success of the overall CP process. Traditional measures include:

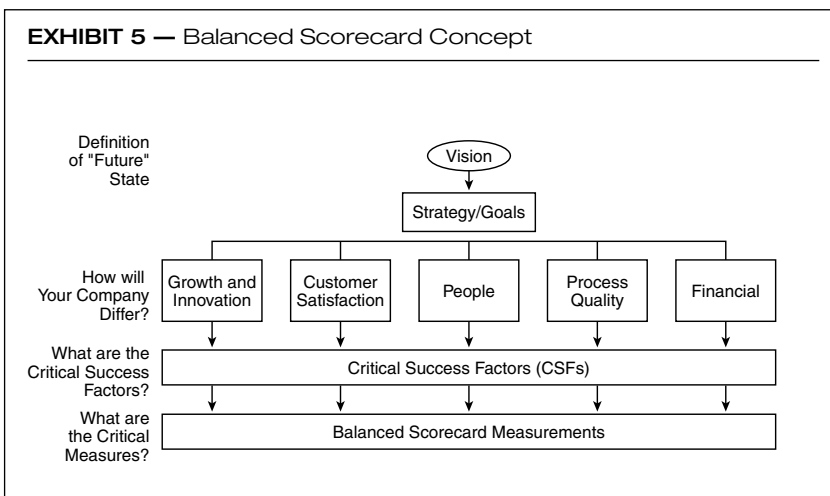
- How much money is spent on hotsites?
- How many people are devoted to CP activities?
- Was the hotsite test a success?

Instead, the focus should be on measuring the CP process contribution to achieving the overall goals of the organization. This focus helps to:

- Identify agreed-upon CP development milestones
- Establish a baseline for execution
- Validate CP process delivery
- Establish a foundation for management satisfaction to successfully manage expectations

The CP balanced scorecard includes a definition of the:

- Value statement



- Value proposition
- Metrics/assumptions on reduction of CP risk
- Implementation protocols
- Validation methods

Exhibits 5 and 6 illustrate the balanced scorecard concept and show examples of the types of metrics that can be developed to measure the success of the implemented CP process. Included in this balanced scorecard approach are the new metrics upon which the CP process will be measured.

Following this balanced scorecard approach, the organization should define what the future state of the CP process should look like (see the preceding CP value journey discussion). This future state definition should be co-developed by the organization's top management and those responsible for development of the CP process infrastructure.

**EXHIBIT 6 — Continuity Process Scorecard**

**Question:** How should the organization benefit from implementation of the following continuity process components in terms of people, processes, technologies, and mission/profits?

<b>Continuity Planning Process Components</b>	<b>People</b>	<b>Processes</b>	<b>Technologies</b>	<b>Mission/Profits</b>
Process methodology				
Documented DRPs				
Documented BRPs				
Documented crisis management plans				
Documented emergency response procedures				
Documented network recovery plan				
Contingency organization walk-throughs				
Employee awareness program				
Recovery alternative costs				
Continuous availability infrastructure				
Ongoing testing programs				
etc.				

---

**Exhibit 4** illustrates the current state/future state visioning overview, a technique that can also be used for developing expectations for the balanced scorecard. Once the future state is defined, the CP process development group can outline the CP process implementation critical success factors in the areas of:

- Growth and innovation
- Customer satisfaction
- People
- Process quality
- Financial state

These measures must be uniquely developed based on the specific organization's culture and environment.

#### **WHAT ABOUT CONTINUITY PLANNING FOR WEB-BASED APPLICATIONS?**

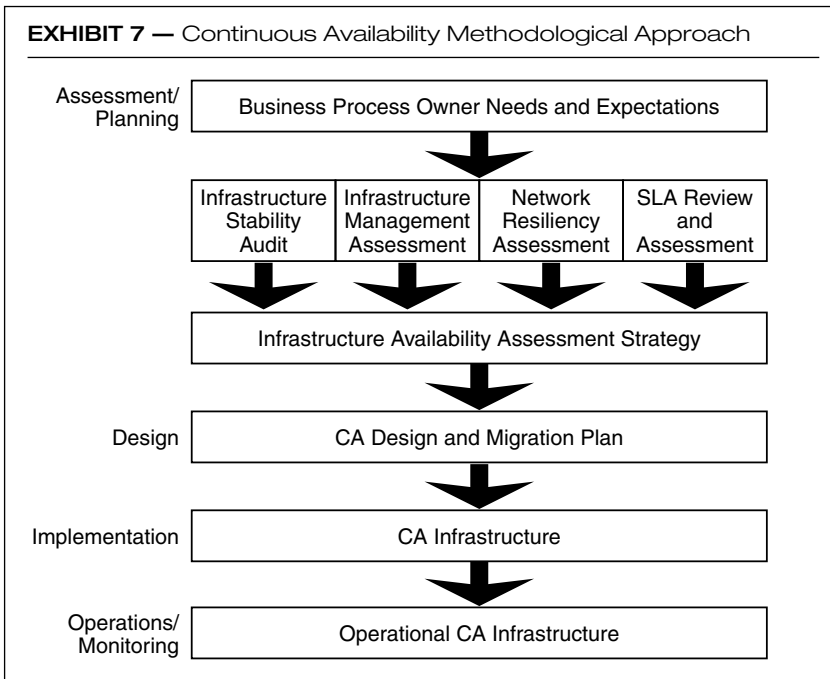
Evolving with the birth of the Web and Web-based businesses is the requirement for 24x7 uptime. Traditional recovery time objectives have disappeared for certain business processes and support resources that support the organizations' Web-based infrastructure. Unfortunately, simply preparing Web-based applications for sustained 24x7 uptime is not the only answer. There is no question that application availability issues must be addressed, but it is also important that the reliability and availability of other Web-based infrastructure components (such as computer hardware, Web-based networks, database file systems, Web servers, file and print servers, as well as preparing for the physical, environmental, and information security concerns relative to each of these [see RMR above]) also be undertaken. The terminology for preparing the entirety of this infrastructure to remain available through major and minor disruptions is usually referred to as continuous or high availability.

Continuous availability (CA) is not simply bought; it is planned for and implemented in phases. The key to a reliable and available Web-based infrastructure is to ensure that each of the components of the infrastructure have a high-degree of resiliency and robustness. To substantiate this statement, *Gartner Research* reports "Replication of databases, hardware servers, Web servers, application servers, and integration brokers/suites helps increase availability of the application services. The best results, however, are achieved when, in addition to the reliance on the system's infrastructure, the design of the application itself incorporates considerations for continuous availability. Users looking to achieve continuous availability for their Web applications should not rely on any one tool but should include the availability considerations systematically at every step of their application projects."<sup>7</sup>

Implementing a continuous availability methodological approach is the key to an organized and methodical way to achieve 24x7 or near 24x7 availability. Begin this process by understanding business process needs and expectations, and the vulnerabilities and risks of the network infrastructure (e.g., Internet, intranet, extranet, etc.), including undertaking single-points-of-failure analysis. As part of considering implementation of continuous availability, the organization should examine the resiliency of its network infrastructure and the components thereof, including the capability of its infrastructure management systems to handle network faults, network configuration and change, the ability to monitor network availability, and the ability of individual network components to handle capacity requirements. See [Exhibit 7](#) for a sample pictorial representation of this methodology.

The CA methodological approach is a systematic way to consider and move forward in achieving a Web-based environment. A very high-level overview of this methodology is as follows.

- *Assessment/planning.* During this phase, the enterprise should endeavor to understand the current state of business process owner expectations/requirements and the components of the technological infrastructure that support Web-based business processes. Utilizing both interview techniques (people to people) and existing system



---

and network automated diagnoses tools will assist in understanding availability status and concerns.

- *Design.* Given the results of the current state assessment, design the continuous availability strategy and implementation/migration plans. This will include developing a Web-based infrastructure classification system to be used to classify the governance processes used for granting access to and use of support for Web-based resources.
- *Implementation.* Migrate existing infrastructures to the Web-based environment according to design specifications as determined during the design phase.
- *Operations/monitoring.* Establish operational monitoring techniques and processes for the ongoing administration of the Web-based infrastructure.

Along these lines, in their book *Blueprints for High Availability: Designing Resilient Distributed Systems*,<sup>8</sup> Marcus and Stern recommend several fundamental rules for maximizing system availability (paraphrased):

- *Spend money...but not blindly.* Because quality costs money, investing in an appropriate degree of resiliency is necessary.
- *Assume nothing.* Nothing comes bundled when it comes to continuous availability. End-to-end system availability requires up-front planning and cannot simply be bought and dropped in place.
- *Remove single-points-of-failure.* If a single link in the chain breaks, regardless of how strong the other links are, the system is down. Identify and mitigate single-points-of-failure.
- *Maintain tight security.* Provide for the physical, environmental, and information security of Web-based infrastructure components.
- *Consolidate servers.* Consolidate many small servers' functionality onto larger servers and less numerous servers to facilitate operations and reduce complexity.
- *Automate common tasks.* Automate the commonly performed systems tasks. Anything that can be done to reduce operational complexity will assist in maintaining high availability.
- *Document everything.* Do not discount the importance of system documentation. Documentation provides audit trails and instructions to present and future systems operators on the fundamental operational intricacies of the systems in question.
- *Establish service level agreements (SLAs).* It is most appropriate to define enterprise and service provider expectations ahead of time. SLAs should address system availability levels, hours of service, locations, priorities, and escalation policies.
- *Plan ahead.* Plan for emergencies and crises, including multiple failures, in advance of actual events.



- 
- *Test everything.* Test all new applications, system software, and hardware modifications in a production-like environment prior to going live.
  - *Maintain separate environments.* Provide for separation of systems, when possible. This separation might include separate environments for the following functions: production, production mirror, quality assurance, development, laboratory, and disaster recovery/business continuity site.
  - *Invest in failure isolation.* Plan — to the degree possible — to isolate problems so that if or when they occur, they cannot boil over and affect other infrastructure components.
  - *Examine the history of the system.* Understanding system history will assist in understanding what actions are necessary to move the system to a higher level of resiliency in the future.
  - *Build for growth.* A given in the modern computer era is that system resource reliability increases over time. As enterprise reliance on system resources grows, the systems must grow. Therefore, adding systems resources to existing reliable system architectures requires preplanning and concern for workload distribution and application leveling.
  - *Choose mature software.* It should go without saying that mature software that supports a Web-based environment is preferred over untested solutions.
  - *Select reliable and serviceable hardware.* As with software, selecting hardware components that have demonstrated high mean times between failures is preferable in a Web-based environment.
  - *Reuse configurations.* If the enterprise has stable system configurations, reuse or replicate them as much as possible throughout the environment. The advantages of this approach include ease of support, pretested configurations, a high degree of confidence for new roll-outs, bulk purchasing possible, spare parts availability, and less to learn for those responsible for implementing and operating the Web-based infrastructure.
  - *Exploit external resources.* Take advantage of other organizations that are implementing and operating Web-based environments. It is possible to learn from others' experiences.
  - *One problem, one solution.* Understand, identify, and utilize the tools necessary to maintain the infrastructure. Tools should fit the job; so obtain them and use them as they were designed to be used.
  - *KISS: keep it simple....* Simplicity is the key to planning, developing, implementing, and operating a Web-based infrastructure. Endeavor to minimize Web-based infrastructure points of control and contention, as well as the introduction of variables.

Marcus and Stern's book<sup>8</sup> is an excellent reference for preparing for and implementing highly available systems.

---

Reengineering the continuity planning process involves not only reinvigorating continuity planning processes, but also ensuring that Web-based enterprise needs and expectations are identified and met through the implementation of continuous availability disciplines.

## SUMMARY

The failure of organizations to measure the success of their CP implementations has led to an endless cycle of plan development and decline. The primary reason for this is that a meaningful set of CP measurements has not been adopted to fit the organization's future-state goals. Because these measurements are lacking, expectations of both top management and those responsible for CP often go unfulfilled. Statistics gathered in the *Contingency Planning & Management/KPMG Continuity Planning Survey* support this assertion. Based on this, a radical change in the manner in which organizations undertake CP implementation is necessary. This change should include adopting and utilizing the business process improvement (BPI) approach for CP. This BPI approach has been implemented successfully at many Fortune 1000 companies over the past 20 years. Defining CP as a process, applying the concepts of the CP value journey, expanding CP measurements utilizing the CP balanced scorecard, and exercising the organizational change management (OCM) concepts will facilitate a radically different approach to CP. Finally, because Web-based business processes require 24x7 uptime, implementation of continuous availability disciplines are necessary to ensure that the CP process is as fully developed as it should be.

## References

1. *Contingency Planning & Management*, January/February 2001. (The survey was conducted in the U.S. in October 2000 and consisted of readers and respondents drawn from *Contingency Planning & Management* magazine's domestic subscription list. Industries represented by respondents include Financial Services; Manufacturing/Industrial, Telecommunications, Education, Utilities, Healthcare, Insurance, Retail/Wholesale, Petroleum/Chemical, Information/Data Processing, Media/Entertainment; and Computer Services/Systems.)
2. Harrington, H.J., Esseling, E.K.C., and Van Nimwegen, H., *Business Process Improvement Workbook*, McGraw-Hill, 1997.
3. Harrington, p. 18.
4. Harrington, p. 19.
5. Robert S. Kaplan and David P. Norton, *Translating Strategy into Action: The Balanced Scorecard*, HBS Press, 1996.
6. Harrington, p. 1-20.
7. Gartner Group RAS Services, COM-12-1325, 29 September 2000.
8. Marcus, E. and Stern, H., *Blueprints for High Availability: Designing Resilient Distributed Systems*, John Wiley & Sons, 2000.

---

Carl B. Jackson, CISSP, CBCP, has more than 25 years of experience in the areas of information security, continuity planning, and information technology internal control reviews and audits. He is vice president—business continuity planning for QinetiQ Trusted Information Management Corporation.

Mr. Jackson can be reached at [cbjackson@QinetQ-TIM.com](mailto:cbjackson@QinetQ-TIM.com).