



# BUSINESS CONTINUITY AND DISASTER RECOVERY: A STRAIGHTFORWARD APPROACH *by Wes Gorham*

“Don’t put all your eggs in one basket.” This old chestnut is particularly appropriate when it comes to managing risk. Risk represents different things depending on your audience. We often hear of the importance of managing the risks associated with making personal investments. Until we understand investing well enough to weigh equity against the level of tolerable risk, we risk making uninformed decisions that could have devastating results.

The same principle holds true for organizations seeking to manage their own risk while striving to achieve the goals and priorities set by their management. The business continuity and disaster recovery (BC/DR) plan is a key tool in any organization’s risk management toolbox. This article is intended to serve as a primer for creating a BC/DR plan, providing you with the essential knowledge, expertise, and practical decision-making skills you need to be successful.

## **AN ENTERPRISE-CENTRIC, HOLISTIC FRAMEWORK**

Business requirements drive the criteria for quality. These requirements and their corresponding processes are the “customer-driven” nervous system of the organization. The continuity requirements of these processes drive the level of risk mitigation investment the organization includes in its business strategy. These business processes, in turn, enable service delivery. The result is a BC/DR program that provides for the needs of the business and reflects the business’s commitments to its customers.

IT provides specific technical services to various lines of business throughout an organization. These business operations have an inside-out view of the organization, while the executive-level looks from the outside in. The diagram on the following page illustrates the holistic nature of a typical BC/DR program with this bidirectional view. Lower-level operational activities are the key to linking specific customer-driven requirements for risk tolerance with criteria for quality. The high-level activities set the framework for strategy, policy, and constraints on corporate requirements.

## BUSINESS CONTINUITY RESILIENCE AND DISASTER RECOVERY CONTINUUM



Let's take a closer look at the continuum model section by section to better understand the key activities and deliverables, and the role the service desk plays in the overall delivery.

### SENIOR EXECUTIVE DIRECTION AND COMMITMENT

Leadership is an essential element in setting the strategic vision. In today's fast-paced business world, most executives are concerned with developing a strategy that helps the organization achieve and sustain strength and profitability. With this in mind, it is still possible to build a sustainable BC/DR program and secure solid commitment at the executive level. The priorities established during strategic planning become the goals, objectives, values, and guiding principles that support the risk management program and protect the organization's investment.

From a risk management perspective, senior leadership typically takes the following into consideration:

- Regulatory, financial, and legal issues;
- Customer obligations;
- Insurance coverage (requirements and protection);
- Risk mitigation requirements (as a means of protecting some business functions); and
- Image and reputation.

### BC/DR STRATEGY AND POLICY

Before continuing, it is important to understand the differences between BC/DR *programs* and BC/DR *plans*. The BC/DR program is the business continuity management lifecycle that supports the risk management process and protects the organization's investment and assets. The BC/DR plan falls under the control of the BC/DR program and serves as the instruction manual for the continuity and recovery of business operations and technology services. Holistic in nature, it is a road map for seamless recovery, enough to sustain an acceptable level of service delivery.

The strategy and policy phase sets the policies and standards required to achieve the desired results. The key components of this phase are:

- Policies and standards (for ensuring the continuity of business operations);
- Maximum allowable downtime (MADT) and recovery time objectives (RTOs);
- Resilience;
- Methodology and tools;
- Processes; and
- Deliverables and results.

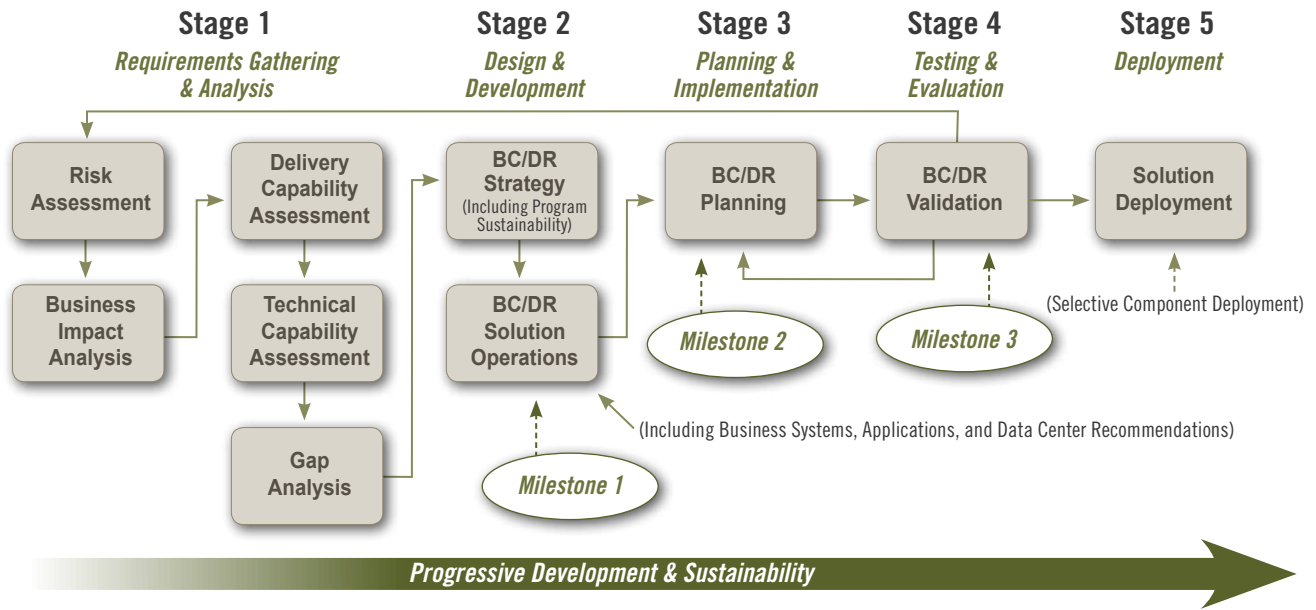
Typically, a business continuity (BC) manager is responsible for driving the program by providing the oversight and direction that opens the doors of communication and cooperation from upper management down through to the lower levels of the organization. The BC manager is ultimately responsible for the program's success; however, he or she will require the assistance of key individuals. A disaster recovery (DR) manager, for example, may be chosen to lead the DR portion of the program.

Each business unit within the organization also plays a key role. The service desk, for example, is typically a mission-critical business unit. The services it provides before, during, and after a service disruption are vital. Therefore, the service desk should be proactive and develop and maintain its own viable BC/DR plan. Such a plan would include things like workaround procedures to mitigate the adverse impacts of a service disruption and keep key business processes operating at an acceptable level. It would also include provisions for handling the increased call volumes the service desk is likely to experience during a service disruption.

The planning stage is critical, and for best results, you should follow your tactical delivery road map. The essential goal is to

# BUSINESS CONTINUITY AND DISASTER RECOVERY

## THE RESILIENCY AND RECOVERY ROAD MAP



design, develop, and implement the BC/DR program in a controlled manner, using the iterative process illustrated in the diagram above. Remember, to ensure seamless implementation, a well-established delivery model and execution plans is critical.

### BC/DR BUSINESS PROCESSES

The planning, solution development, and delivery activities that take place in this phase are continuously improved over time, as business requirements evolve. For example, the service desk contributes to the BC/DR program by actively participating in planning activities, and by building, training, testing, and continuously improving its own BC/DR plan. It also collaborates with other service units, when necessary, to ensure that the BC/DR Plan is consistent and provides seamless, end-to-end continuity.

The service desk is also responsible for provisioning the back-up facility, to be used when the primary facility is rendered unusable. Any tools and systems lost during the disaster, such as the incident logging tool, must be recovered. Following its BC/DR plan, the service desk would simply mobilize its staff and any other required resources to the alternate facility and resume operations in an effort to maintain service continuity. It may not be feasible to deploy the whole solution all at once, but pieces of the solution can be compartmentalized and deployed selectively over time.

These are the typical elements of an established BC/DR program and plan:

- Business requirements;
- Methodology, policies, and guidelines;
- Processes and procedures;
- Tools and templates;
- Risk assessment and business impact analysis (BIA);
- Delivery and technical capability;
- BC/DR strategy and solution;

- Emergency response (includes disaster declaration, escalation and notification, call trees, etc.);
- Technical recovery plan (i.e., recover the IT infrastructure);
- Resumption plan;
- Repatriation plan (i.e., return process activity and/or IT back to steady-state); and
- Ongoing testing, maintenance, audit governance, and continuous improvement.

### BUILDING, MAINTAINING, AND TESTING PLANS

Once the BC/DR program and plan are in place, they must be maintained. Having invested large amounts of time, energy, and money deploying the program and plan, they must be continuously improved, particularly as business requirements change and evolve. This helps ensure that their accuracy and integrity are in line with the business's needs.

The BC manager will work with key representatives from across the organization, including the service desk, to provide oversight and direction, and to conduct testing exercises. Customers and third-party service providers should also be included in these exercises. Testing provides a mechanism for identification and correcting any deficiencies and nonconformities, and for keeping management and customers happy. The depth and breadth of testing depends on the program's key requirements. In general, the program should be tested annually, though specific testing can be conducted in isolated settings when and where it is necessary.

As noted above, the service desk must participate in the organization's test exercises. These exercises must test employee competency and the functionality of processes, facilities, and technology to verify that the BC/DR plan is sufficient. In addition, a test simulation setting at the alternate facility is absolutely necessary.

A typical test plan should consist of the following:

- An executive summary;
- Scope and scenario;
- Dates, locations, participants, and timescales;
- Assumptions and limitations;
- Objectives;
- Results of the objectives;
- Key strengths;
- Areas requiring improvement, lessons learned, and noteworthy items;
- Risk and change control;
- Test preparations;
- Notification, procedural systems, and participants check;
- Postrecovery check;
- Test cases;
- Technical infrastructure tier testing; and
- An activity log, issues log, and action items log.

### **THE EMERGENCY RESPONSE PLAN: BC/DR INTEGRATION**

To work effectively, the design of the technology and delivery model must uphold the business's requirements and it must be seamless. These requirements are typically quantified by three metrics: maximum allowable downtime (MADT), recovery time objective (RTO), and recovery point objective (RPO). The RPO specifies the point in the operating cycle at which recovery must occur for the business to resume normal operating activities. The BC manager will provide the necessary oversight to ensure that the BC/DR plan integrates the business and its technology, and will make adjustments where necessary.

When a disaster is declared, the service desk may provide extended and even additional services to assist with the recovery. However, the service desk will also be busy recovering assets and resuming operations specific to its own services.

### **APPLICATION ANALYSIS AND ASSET, INCIDENT, AND CHANGE MANAGEMENT**

To ensure that the required assets are included in the BC/DR plan, a reliable method for maintaining critical assets is crucial. All assets must be tracked and managed when changes are being made. At this stage, a configuration management database (CMDB) or other compatible tool for tracking assets will prove beneficial, as will integration with the change management process, which will ensure that the BC/DR plan stays in sync as changes are implemented.

Incident management is also a key process, as a disaster situation is an incident and it must follow the path to resolution set forth in the incident management process. The service desk is responsible for logging and tracking all of the calls it receives that pertain to the service disruption, as well as logging, tracking, and managing all first-pass resolution attempts. Likewise, the service desk is responsible for maintaining asset information and making sure that information is available to assist with handling service disruptions.



Again, as other business and service units invoke their notification and escalation plans, the service desk may be called upon to assist where necessary.

Business systems and applications are interdependent. Establishing a recovery capability that synchronizes application interdependencies will reduce the recovery time window, thus lowering recovery costs and mitigating any adverse effects on service.

### **DRP/DATA STORAGE INTEGRATION**

Finally, selecting the most appropriate data storage solution architecture and recovery/restoration method, based on the DR solution, is essential to any BC/DR plan. The way data is backed up and stored off site, whether your organization uses a simple tape-based method or a sophisticated mass storage design, is crucial if adequate recovery is to be achieved. Synchronization between the primary data center and the DR management hot-site must be engineered to facilitate the simplest and most effective recovery possible in the shortest amount of time. Many organizations fail to realize the importance of this step and find that their data storage and recovery solutions are insufficient.

Business continuity and disaster recovery management are complex disciplines. I trust the insights I've provided here will help you develop your BC/DR program, produce a well-crafted BC/DR plan, and avoid putting "all your eggs in one basket."

*Thanks to Larry Lall, a senior BC/DR consultant at Integritas Solutions, and Derek Gillard, ITSM practice principal at Integritas Solutions, for providing guidance and insight during the preparation of this article.*



### **About the Author**

Wes Gorham is a senior BC/DR consultant with Integritas Solutions. He has more than twenty-seven years of business and IT experience, including the delivery of complex BC/DR solutions for clients across North America. Wes is also certified in ITIL v3 Foundation.

# The Most Boring Subject in IT? by Craig Baxter

What is the most boring subject in IT? Many topics come to mind, but few would argue that disaster recovery (DR) and business continuity would be high on the list. It is a dry subject. It was dry back in 1999 when everyone was anticipating Y2K, and I don't imagine anyone thinks it's less dry today.

Just about every profession has its boring, fundamental practices that no one likes to do, but that must be done. Take basketball, for example. At the college or professional level, you would think players would be experts at shooting free throws and layups. Yet they practice them all the time (and I do mean *all* the time). Those are two of the most basic shots in the game. But how many games are lost on missed free throws? Too many to count. Anyone catch the final game of the NCAA tournament this year? Presumably the best two teams in all of college basketball, yet the losing team missed more layups than a junior high-school team on a bad day. It was painful, even embarrassing, to watch. The result was a blowout the likes of which has never been seen in NCAA tournament history.

The same happens when organizations don't pay attention to DR and BCP, and the infamous Murphy (as in Murphy's Law) comes to collect. As boring as planning and preparing for the unthinkable may be, there are real consequences if a customer can't get through to technical support when a mission-critical application is down and paying customers are dropping like flies. It's not optional.

A few years ago, the multicampus company I was working for in Denver established contingency plans for the unlikely event that one of our buildings lost power or suffered a catastrophe that prevented people from entering the building. We set up alternate workspaces in each of our buildings, with extra PCs and phones that would enable employees to perform critical functions in the event of an emergency at one of our other sites. Then it happened. A spring storm dumped three feet of snow and gridlocked the city for forty-eight hours. No one could get to one of our key operations centers. Not a problem: We had set up alternate sites. But no one could get to any of those buildings either. Our mortgage clients in balmy Florida and sunny southern California had little sympathy for our plight when they couldn't issue financial instruments for closings that day. What we should have done was issue laptops to critical staff and enabled VPN access to our network so they could work remotely from their homes. The technology existed at the time, but few people were taking advantage of it. Our planning was inadequate. We knew it snowed in Denver, but we didn't take the possibility seriously enough and suffered grave consequences as a result.

I have heard it said that DR is the responsibility of the IT organization and BCP is the responsibility of the business units. But DR and BCP go

hand in hand. There is no business continuity without good disaster recovery plans, procedures, and infrastructure, and there can be no disaster recovery without good business continuity planning. I see it as a single discipline: DR-BCP.

Across the organization, leaders must take DR-BCP seriously and implement adequate plans. According to the *2010 HDI Practices & Salary Report*, business continuity sits at the bottom of the list, with 16 percent reporting that they have implemented this ITIL process in their organizations. After financial management, it is the least-followed process. A 2009 study by InformationWeek Analytics reported similar results, with 17 percent of survey respondents indicating that their organizations had no DR-BCP plans, while 20 percent are still working on their strategies.

Nearly fifteen years after participating in my first impact analysis, this is truly alarming. With those statistics, it seems there has not been nearly enough focus on the subject. Where does your organization stand? Are you among the 20 percent still working on a strategy? Is that code for "we'll do something when we get around to it"? At my former company, we thought we had performed good BCP. We were kidding ourselves. Google, Amazon, and Facebook have all made headlines recently over critical system failures that impacted consumers.<sup>2</sup> Will your company be next?

It is not enough to create a plan and assume that you're done. Plans should be reviewed on a regular basis and updated as the business and technology evolves. Have you moved any of your computing infrastructure to the cloud lately? Could that have an impact on the plan your organization created six years ago?

DR-BCP is critical to service desk and technical support groups. After all, isn't the service desk a business function? When something goes wrong, it's going to be right in the middle of dealing with it. And if the service desk doesn't plan for business continuity, it may be subject to the same catastrophic failures as its business counterparts. As the champion of service management, it is imperative that service desk and technical support organizations are directly involved in all aspects of this core discipline and champion the cause. Practice the fundamentals. You can't take shortcuts. There is far too much at stake. Boring? Sure. Optional? Never.



## About the Author

Craig Baxter is HDI's global brand manager, responsible for providing general oversight and management. His background is in software development, IT management, technical support desk, call center solutions, and operations. Prior to joining HDI, he held various positions at First Data Corp., MCI, Softech, and the US Air Force. Craig earned

his BSE in electrical engineering from Northern Arizona University and his MS in computer science from Chapman University.

<sup>1</sup>Eli Khnaser, "Final Frontier: Leveraging Virtualization for BC/DR" (December 18, 2009), *InformationWeek Analytics*, <http://analytics.informationweek.com/abstract/15/1893/Risk-Management/research-bc-dr-and-virtualization.html>

<sup>2</sup>Thomas Claburn, "Cloud Outages Plague Google, Microsoft" (May 13, 2011), *InformationWeek*, <http://www.informationweek.com/news/cloud-computing/software/229500399>