

# A MODEL FOR BUSINESS RESILIENCY

Thomas E. Martin, Eagle Rock Alliance, Ltd.

**T**HE TERMS *BUSINESS CONTINUITY* (BC) AND *DISASTER RECOVERY* (DR) HAVE BEEN USED FOR years to describe the planning process for business interruptions. Experts may disagree on the exact definition of each, but in general, BC focuses on people and processes as they relate to business operations, while DR relates to the infrastructure and IT components. Both disciplines are reactive in nature—they are initiated in response to an event that has disabled some portion of the business entity.

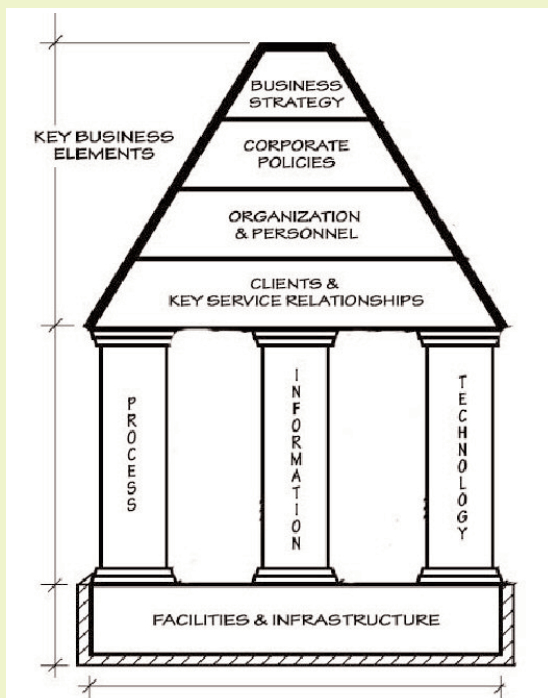
As BC/DR industry has matured, the reactive focus is being replaced quickly by more proactive measures that minimize the need for acute reactions to unplanned events. Investments in *high-availability* solutions for continuous processing are becoming commonplace. Additionally, renewed focus on people and process has placed similar priorities on succession planning and business process redundancy. These factors have led to a new industry term—*business resiliency*.

## Business Resiliency

The concept of business resiliency is broader than the combined scopes of BC and DR, because it establishes a framework for businesses to inspect or evaluate every aspect of an enterprise. A resilient enterprise has the ability to stretch and bend, avoiding a breakdown while implementing the recovery plans in the event of the unexpected or unavoidable. This broad scope allows a business to respond to unplanned events or disasters, as well as to normal business activities such as acquisitions, downsizing, or market shifts.

Business resiliency reaches beyond protection to provide a proactive, comprehensive, and robust strategy to achieve and maintain a competitive advantage. To support the needs of today's businesses effectively, the underlying operational infrastructure must be flexible and adaptive,

FIGURE 1



while simultaneously protected against unknown or unexpected threats.

Understanding the required elements of resiliency planning and how they relate to the organization's business model are essential in building a sustainable resiliency strategy. Following is a description of these elements.

## Business Model

Figure 1 (page 30) depicts a traditional business model that can be applied to most businesses today. The top four layers of the model represent the cultural, or apparent, elements of a business, where the business defines its identity, culture, and product or service direction. These layers represent the strategic and guiding elements of the business—elements that govern and establish policies, priorities, investments, partnerships, and client-facing commitments.

The three *pillars* and the foundation in the model represent the underlying capital and operational investment made in the business. This investment must support the strategy and goals of the business. Tradeoffs between in-house support and outsourcing various functions represented by these components can be made, but service levels must meet minimum necessary criteria to sustain the business. True *resiliency* means coordinating these minimums while building a solid prevention strategy and an effective crisis response.

## Resiliency Model

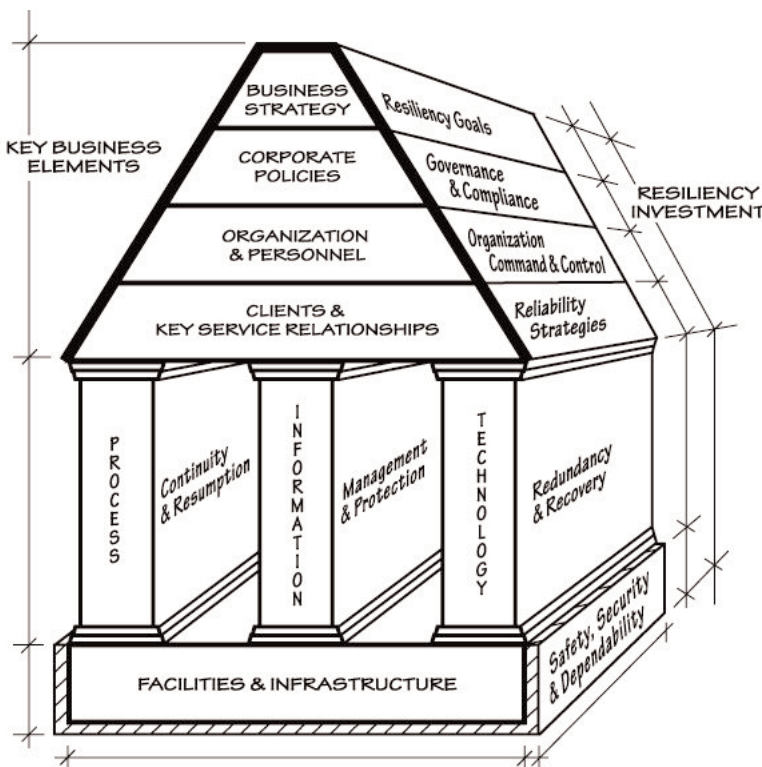
When the model is rotated slightly, as in Figure 2, business resiliency components can be incorporated into the traditional business model. This view outlines the investment categories, which constitute the level of resiliency commitment made by an organization. As in a traditional business model, the top layers determine the commitment level, or the magnitude of the investment that an organization will make to meet stated resiliency goals.

Let's take a closer look at each of these resiliency elements as they relate to the enterprise business model depicted on the front face of the model.

## Business Strategy—Resiliency Goals

Goal setting for resiliency of the business itself is a cornerstone in business strategy implementation. Executive management must define these goals to establish the service criteria for an organization's functional availability. For example, an organization must decide whether to be operational around the clock, with full process and personnel redundancy, or to be available Monday through Friday with 99 percent availability. The resiliency goals must be in step with the business and investment strategy. Likewise, the elements of the resiliency model must be aligned with the implementation and execution at all levels of the business strategy throughout the enterprise.

FIGURE 2



## Corporate Policies—Governance and Compliance

The success and long-term viability of enterprise resiliency relies on a well-managed system of checks and balances within a *program*—not through isolated *projects*—focused on business resiliency. Resiliency goals must be implemented in a structured and controlled environment. The organization must be able to plan and measure progress and investments against stated objectives. These objectives must be defined as specific metrics for service delivery, response, and availability commitments of the business.

These objectives must mesh with the established overall resiliency goals and budgets, and must also meet any compliance requirements for a specific industry. In addition, a governance model must be established to define the organizational elements and quantify the objectives and measurement criteria, as well as set up operational program elements. Program management sets the parameters, manages the work to be performed, tracks the progress, audits the results, and generates status reports on a regular basis.

## | Business Resiliency |

### Organization and Personnel—Organizational Command and Control

The ability to provide leadership during a crisis is vital to the enterprise's resilience. An emergency communication capability, as well as a documented crisis response plan and emergency response plan, are top priorities to assure the safety of personnel and the viability of the enterprise during and after an emergency.

Breakdowns in communication can result in lost lives, lost business, and the avoidable consequences of a poor response to an unplanned event. Communication with critical information sources (e.g., first responders, civil authorities, facilities personnel and utility providers) sets the stage for properly assessing an incident and its impact. Communication with employees allows the flow of vital information to ensure safety, security, and proper response to the crisis. Communication with clients, business partners, and stakeholders is key to preserving the enterprise's reputation and marketability. Communication with key vendors, outside service providers, and other third parties is critical to establishing smooth continuation of business activities.

### Clients and Key Service Relationships—Reliability Strategies

Business resiliency objectives cannot be effective without individual strategies to direct how objective will be achieved. The management teams that will be accountable for meeting the objectives need viable, documented strategies in place to achieve each of the objectives. Partners and key service providers must participate in the process to be capable of providing an appropriate response in the event of an emergency.

Reliability strategies may call for a high level of operational redundancy, or may simply identify an alternate location from which to rebuild. In either case, it is critical that strategies, detailed plans, and measures be in place to assure that systems, data and personnel will be available to meet the objectives. Failing to develop and fund effective strategies, as well as failing to empower personnel to carry out the plans, can expose the business to potentially excessive downtime costs and loss of opportunity.

### Process—Continuity and Resumption

Identifying and prioritizing business requirements is one of the first steps in establishing a comprehensive BC capability. Sustaining business operations during an unplanned event may require workarounds, alternate workspace, or other special arrangements. Business processes must be identified, prioritized, and mapped for all supporting functional requirements, including voice communications, fax, workspace requirements, applications technology, etc.

Procedures are also needed to account for operational activity between the time an incident occurs and the time when

all the recovery activities are complete. Where to go, how to get there, and what to do once you get there must be documented to avoid added confusion during an incident. All these requirements and activities should be documented in BC plans, which must be properly maintained and periodically tested.

### Information—Management and Protection

A comprehensive vital records program driven by the needs of the business that complies with all regulatory requirements is a necessity to sustain business operations. Information is the lifeblood of every corporation, and having the information available at all times is critical to remaining competitive. Lost information cannot be recovered, and the older the information is, the more difficult it is to re-create.

Regulatory agencies such as the Department of Health and Human Services, NASD, and the Securities and Exchange Commission impose regulations that affect the retention and availability requirements of data for certain businesses. These regulations, coupled with sound business practices, drive the need to properly safeguard information under normal working conditions, as well as in the event of a disaster. Making data available when and where it is needed is paramount to business resiliency. If the corporate asset known as *data* is not properly protected, the business can lose revenue and be subject to substantial regulatory fines.

### Technology—Redundancy and Recovery

Resiliency efforts require proactive, structured, and integrated efforts to achieve desired commitments. Most IT departments are managed as an internal service to the business. Typically, there are service-level agreements by which users measure these departments. Service must be provided under normal conditions, as well as during emergency/disaster conditions.

Business application priorities driven by *recovery time objectives* (RTO)—the amount of downtime that can be tolerated from the point of disaster to the point of functional recovery—and *recovery point objectives* (RPO)—the amount of data loss that can be tolerated during a system or subsystem recovery—will dictate the level of investment to be made in the technology resiliency architecture.

In a business that is totally dependent on technology, a resiliency goal may be set that requires no single-point-of-failure in the support environment. For less technology-dependent businesses, next-day recovery may be adequate. IT DR plans, then, should combine service continuity (fail-over) with restoration, accounting for all levels of RTO/RPO specified by the business. The first step of the plan involves the people and tools required to maintain or restore the environment. The next step is the granular implementation *playbook*, which details the priority order of steps, anticipated timeframes, and interdependencies. Without these plans, a recovery can experience problems that may negatively affect the ability to recover at all.

To subscribe go to [www.continuityinsights.com](http://www.continuityinsights.com)

## Facilities and Infrastructure—Safety, Security, and Dependability

The truly resilient enterprise will mitigate its risks to reduce the likelihood of an occurrence in the first place. Investments in enhancing, or *hardening*, data center facilities to comply with a percentage/failure probability are typical starting points. Investing in both physical and software security is also an immediate investment requirement. Risk can come in the form of man-made risks, natural risks, or infrastructure risks, from either internal or external sources. It is wise to analyze all the possible risks the business may be exposed to, eliminating risks with no potential impact and mitigating those (where possible) that could have a medium or high impact. For risks that carry no mitigation activities, a well-documented emergency response plan will establish a level of preparedness in advance, should such an event occur.

## Conclusion

The enterprise resiliency model presented here is intended to organize business thought processes beyond traditional BC/DR to include business resiliency. Applying the resiliency model will help ensure that business outcomes are delivered by measuring performance against key goals and metrics, regardless of stresses and influences on the organization. Incorporating a resiliency mindset into a corporate culture is challenging, requiring strong executive sponsorship and enterprise awareness programs. This is not an easy task, but the result of a comprehensive resiliency investment will produce a more confident and proactive business model that will prosper in today's competitive business climate.

CI

Thomas E. Martin is managing director for Eagle Rock Alliance (West Orange, NJ). He can be reached at (973) 325-9900 or via e-mail at [tmartin@eaglerockalliance.com](mailto:tmartin@eaglerockalliance.com).

## The Clear Choice



We're the *Business* in Business Continuity.

Management Conference 2005  
**CONTINUITY**  
*insights*

**SHERATON NEW ORLEANS**  
**MAY 16-18, 2005**

To subscribe go to [www.continuityinsights.com](http://www.continuityinsights.com)