



Business Continuity Management and The Extended Enterprise

Continuous Availability in a Real-Time Economy

Business Continuity is receiving a great deal of attention in the aftermath of recent events, including the London Bombings, the devastating hurricanes of 2005, as well as numerous software failures and cyber-attacks. Business Continuity Management (BCM) and Continuity of Operations (COOP) is a multi-dimensional practice requiring a balance of investment against risk to the enterprise. Verizon Business's experience managing a large global network infrastructure through some of the most disruptive events of the past few years has provided it with a number of proven BCM and incident management capabilities. This paper discusses the major themes within Business Continuity Management, namely the shift from event driven IT-focused disaster recovery to a more broad-based integrated risk management approach that deals with emerging issues like the extended enterprise and workforce continuity. The discussion begins with a review of the potential threats to continuity of operations and the requirements of recent regulatory actions.

By Jonathan Nguyen-Duy

Continuous Availability

The real-time, widely distributed enterprise has become a standard global business model. Driven by market forces for greater efficiency, productivity, and profitability; enterprise businesses are leveraging new processes and technologies to compete in a highly dynamic global market place. Real-time transactions and integrated supply chains, linking the buyer and seller, mean businesses are vulnerable to even the shortest interruptions. For many enterprises, an hour of down time can cost millions of dollars in lost revenue, productivity, and market capitalization.

Historically, businesses focused on IT recovery—creating a plan to recover from an unforeseen event, such as a power outage, hurricane, earthquake or fire. Traditional approaches featured redundant data centers, telecommunications capabilities, and IT resources. Disaster recovery plans often involved an off-site facility where a set of the minimum business critical systems were available to receive a copy of the latest back-up tapes. The systems would be reloaded and brought online, typically within 24 to 48 hours and sometimes as long as 72 hours, depending on the complexity and criticality of the environment. In today's business environment, the need for real-time access to data and applications makes this model no longer tenable. Businesses simply cannot afford to stop for a few minutes, let alone a couple of days while critical systems are brought back online.

While maintaining data and communications resilience is an important component of any business continuity plan, enterprises must also consider how to protect the most critical component of their business—the workforce. Workforce continuity has emerged as an important BCM consideration as enterprise perimeters expand to support new partnerships, global customers and mobile or remote workers. BCM initiatives need to consider continuity of operations for an extended enterprise through events such as pandemic influenza, infrastructure disruptions and a wide array of other events that may prevent employees from reaching their primary work sites. For some businesses, administrative recovery can be just as critical as IT recovery.

This factor drives requirements to go beyond redundant facilities and resources—to address the need for continuous interactive communications and secure remote access.

Key Components of Successful BCM Programs

BCM initiatives typically focus on the continuous assessment of business needs, acceptable levels of risk and responding with a set of processes and infrastructure designed to optimize operational availability. Effective BCM initiatives must enable the continuation of all critical business processes through a wide range of events—from power outages to pandemic influenza. Therefore, successful business continuity programs are multifaceted, drawing from a broad range of alternatives, and striking a balance between the risks and expense that are appropriate for each enterprise. BCM is more process than product and one size does not fit all. However, successful business continuity management solutions usually incorporate generally accepted best practices and include the following key components:

- Executive sponsorship—Senior leadership must champion BC
- Multi-disciplined team—BC cannot be done by IT alone
- Risk Assessment—Understand the potential exposure and tolerance for uncertainty
- Business Impact Assessment—Quantified analysis of all critical processes and systems
 - Recovery Time Objective—the maximum amount of time within which a function must be restored in order to avoid unacceptable damage
 - Recovery Point Objective—the maximum amount of acceptable data loss after an incident as measured in time
 - Network and Security Assessments for critical applications and processes
- Strategy Development—Recovery strategies based on the corresponding recovery objectives
- Automated plan development and implementation—Investment in planning tools; regular plan review, test and refresh; update plans at least once per year

Compliance: Setting the Agenda—Business Continuity Can No Longer Be Ignored

One needs to look no further than the headlines in today’s business publications to know that compliance is setting the agenda for many executive management teams in boardrooms around the world. More and more often business continuity is being linked to regulatory compliance.

A number of industry regulations and guidelines now include requirements related to business continuity, such as disaster recovery plans, data backup/retention and secondary sites for IT operations. Enterprises are increasingly being asked to provide details about their BCM programs in order to maintain existing business or to compete for new contracts. Enterprises understand that they’re only as resilient as their supply chain and now set high BCP standards for partners, vendors and other stakeholders. Below are just a few of the compliance/regulatory items frequently identified on a CEO’s agenda:

	Industries Affected	Primary Focus	Business Continuity Implications
Sarbanes-Oxley	All public companies traded on U.S. stock exchanges	Corporate governance	Long-term data storage/archiving
Gramm-Leach-Bliley (GLB)	Financial Services	Information retention and security	Data Replication—long-term storage/archiving
HIPAA	Healthcare	Standardization of healthcare transactions and privacy of patient records	Requires disaster recovery plan, crisis operations plan, and data backup
FISMA	U.S. Government	Information security	Requires government to be open and operational through a crisis
Basel II Accord	Financial/Banking	Created by the Basel Committee on Banking Supervision, Sound Practices for Management and Supervision, 2003	Requires business continuity plan and loss limitations
FERC RM01-12-00 (Appendix G)	Energy/Utility	Regulation focused on larger metro utilities. Rural Utility Services are exempt.	Requires disaster recovery plan

Table 1. Sampling of Industry Regulations Affecting Business Continuity



Hazards

To frame the discussion of business continuity planning, it is useful to begin with an assessment of the types of events that can disrupt business. One can then begin to assess the impact and formulate a strategy for mitigating the effects of each potential threat. Hazards come in many forms but can be broken down into three basic categories: Facilities Infrastructure, Workforce Continuity, and IT Infrastructure.

Facilities Infrastructure Hazards

- Natural Hazards (floods, blizzards, hurricanes, forest fires, earthquakes, etc.)
- Human caused (chemical spills, train derailments, terrorist attack, civil unrest, power outages, fuel disruptions, etc.)
- Geographic (transport infrastructure, amenities, staffing resources)

Events that affect the facilities, whether of natural origin or man-made, have been the focus of the disaster recovery discussions. The hazards that typically impact an entire facility are large in scale and often come with little warning. Within the context of Business Continuity Planning, interruptions of this magnitude may be the central driver of the solution, but they should not be the sole focus of planning.

Workforce Continuity Hazards

- Flu pandemic
- Employee loss (work stoppage, death, layoff, resignation, or illness)

Events that affect the personnel of a business, rather than its infrastructure, are a relatively recent BCM issue. However, when one examines the information flows within an enterprise, the people and their ability to access data and applications are clearly a critical element. Personnel-related disruptions can be broad, as in the case of a significant pandemic flu outbreak or weather-related event. However, even the loss of a single key employee can be devastating, if the person in question is the only one who possesses critical knowledge or skills. Effective Business Continuity Planning must also address somewhat unpleasant topics, such as, how would an enterprise sustain operations if a significant percentage of employees were unable to perform their duties for several days, weeks, months or permanently. Can the business rapidly implement staggered work shifts or remote working strategies? The first step to ensuring workforce continuity is to assess which skills are needed to sustain critical processes, where they are located and how readily they can be re-directed to ensure continuity.

IT Infrastructure Hazards

- Hardware failure
- Software errors
- Security event (virus, worm, denial of service attacks or break-ins)
- Network transmission degradation or failure
- Change management error
- Human error

IT infrastructure has long been at the center of disaster recovery. It is an area where technology creates both exposures and the solutions needed to support the real-time, extended enterprise. The threats to IT infrastructure include physical impacts, such as hardware failures and circuit cuts, as well as less visible but very real threats from software bugs, security events, and simple human error. BCM initiatives need to address the complete business information flow and the entire critical infrastructure that supports it.

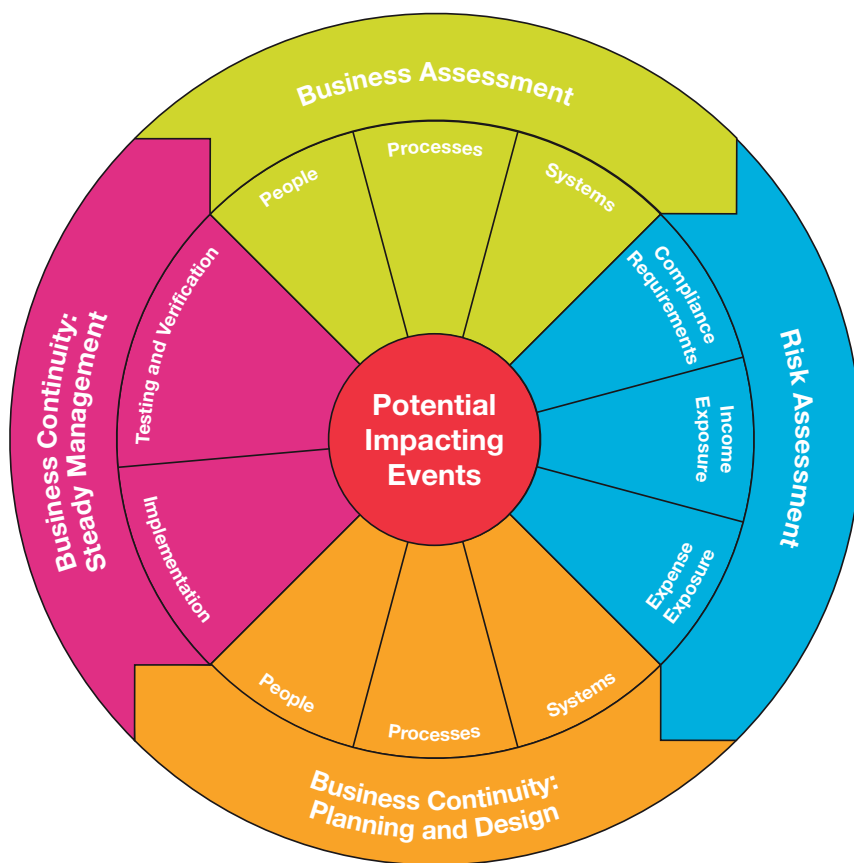
Each hazard, large or small, carries with it a unique set of challenges that a business must address as its BCM strategy evolves. Of course, a number of the BCM components will not be within the scope of IT. For example, to avoid the impact of a significant flu outbreak, many businesses offer free flu shots to employees, thereby mitigating the risk of significant employee absenteeism resulting from seasonal illness.



Business Continuity Management

Business Continuity Management is a continuous process driven by the critical business needs of an enterprise. A complete assessment of the information flows must take into consideration the people, processes and systems (including communications infrastructure) involved in each business information flow. All information flows internal to the company or external to suppliers or customers must be examined. The business assessment is then reviewed in the context of the Risk Assessment. The Risk Assessment helps identify the business continuity requirements, top and bottom line income exposures and potential expenses should an impacting event occur.

Figure 1 below illustrates the Business Continuity Life Cycle. By adopting a life cycle approach to BCM, enterprises should be able to maintain the needed operational resiliency as their environment changes. New applications, mergers and acquisitions, changing regulatory landscapes, and technological advancements can alter the business environment overnight. It is critical that BCM is integrated into all significant business decisions to help enable the enterprise to continue operations while maintaining an acceptable level of risk for its critical information flows.



Verizon Business: Business Continuity Solutions

Verizon Business provides a broad array of business continuity solution components from traditional resilient voice and data services to high-availability, network-embedded applications that enable customers to take advantage of a highly resilient platform at a fraction of the cost of building the platform in-house.

The foundation of the business continuity portfolio is a suite of consulting services that integrate continuity planning with network architectures—helping you through all stages of Business Continuity Plan Development, from initial planning and assessment through implementation.



By integrating Business Continuity Planning and network planning, Verizon Business can help ensure critical processes and systems are supported by a resilient network architecture delivering advanced communications across one of the world’s largest local to global IP networks. This is a critical vulnerability for many enterprises because BCP and network planning are often segregated functions rather an integrated risk mitigation process. Separate leadership and funding priorities means the network architecture might not be able to deliver performance required in the business continuity disaster recovery (BCDR) plan. With Verizon Business, we work with your enterprise to develop and implement business continuity plans and systems to help you meet these critical business objectives.

BCM solutions are built starting with core components of our Consulting Services, Resilient Voice and Data Services, Security Services, IT Solutions, and then a select set of Network Embedded Applications. Verizon Business can then incorporate Managed Services—enabling your enterprise to focus IT efforts on driving business, rather than supporting your infrastructure. Finally, Verizon Business can provide complete end-to-end responsibility for hosting and managing of key business applications.

Verizon has been building and managing its communication infrastructure to some of the highest standards in the telecommunications industry. Verizon enables millions of businesses and consumers to communicate on a daily basis and through some of the most severe events. With years of experience building and managing reliable communications networks, Verizon Business is able to provide enterprises with the opportunity to establish cost-effective solutions to help maintain non-stop, real-time enterprise operations.



Services available to meet key business continuity requirements include the following:*

Service Focus	Service	Benefit to the Customer
Business Continuity Professional Services	Technology Consulting Services	Assistance in developing or refreshing Business Continuity and regulatory compliance plans
Resilient Voice and Data Networking	Enterprise Mobility—EVDO	Ability to stay connected via notebook PCs via broadband wireless combined with Verizon’s Enterprise Mobility Management Service
	IP VPN Broadband Wireless Back-Up	IP VPN and broadband wireless back-up solution to traditional wire line access
	SIG Broadband Wireless Back-Up	Public access back-up via broadband wireless to tie public locations into private networks
	Private IP—Disaster Recovery Ports	Secondary Private IP port and access value-priced to use as back-up access



	Ethernet Private Line	Provides overall metro area LAN/WAN network flexibility and resiliency
	Custom Redirect Service	Real-time redirect of inbound calls based upon a trigger event to pre-configured alternative numbers
Security Services	Denial of Service—Defense Detection	Increased preventative measures to protect systems from outages caused by DoS attacks
	Managed Firewall Enterprise and Managed Intrusion Protection	Increased preventative measures to protect systems from outages caused by viruses and malicious hacking
IT Solutions	IP Application Hosting	Warm and hot fail-over options to facilitate ongoing operations during outage impact to primary facilities and systems
	Remote Backup and Restore	Data back-up to a remote, secure location managed by Verizon with full restore back to the primary data site when needed
	Managed Storage	Variety of managed and hosted storage solutions to integrate into overall Business Continuity plan
Network-Embedded Applications	Hosted IP Centrex	Flexible VoIP-based calling service with network based IP PBX that enables calling locations to change on demand to any location with Internet access
	Web Center	Flexible hosted multimodal contact center functionality that permits contact center agents to reside anywhere there is Internet access
	Integrated Communications Package	Small business focused unified communication application that provides flexible calling and alternative communications options that does not require a fixed location
Managed Network Services	Managed Network Services	A variety of management options for Verizon services that remove day-to-day operations from an enterprise and move them to Verizon's resilient network operations centers
Customized Business Outcome SLA	Customized Business Outcome SLA	Customized solutions focused on achieving specific business outcomes for an application vs. traditional network and data center SLAs

About Verizon Business
 Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a leading provider of advanced communications and information technology (IT) solutions to large-business and government customers worldwide. Combining unsurpassed global network reach with advanced communications, security, and other professional service capabilities, Verizon Business delivers innovative and seamless business solutions to customers around the world.

*All services may not be available in all areas.

