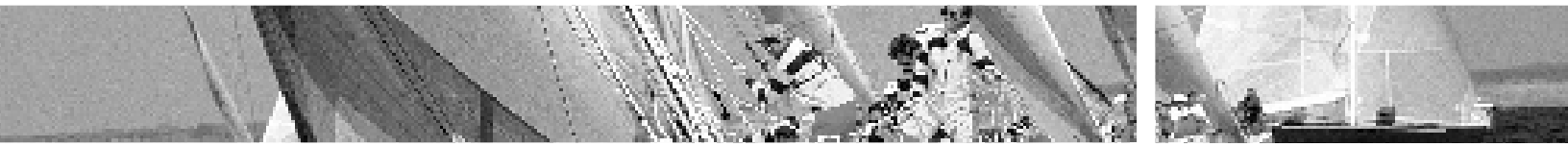
IBM Global Technology Services
February 2010

Examining business resiliency management best practices

How to prepare today for future trends in business resiliency management



by Linda B. Laun, CBCP
IBM Managing Consultant/Global Methods and Tools Development Manager
Business Continuity and Resiliency Services (BCRS)

Contents

Executive summary

Maintaining the continuity of a business was once viewed in the context of ensuring a disaster recovery plan was safely kept in the trunk of our car. Today, however, organizations must address the entire range and level of their exposures, including:

- IT disruptions
- Sudden competitive moves
- Consumer demands
- Security threats
- Market fluctuations
- Compliance with numerous government and industry regulations

To fully address these exposures, risk management, business continuity, crisis management and security professionals need to achieve business resilience to adapt and respond rapidly to threats and opportunities. Business resiliency management (BRM) has evolved to describe the holistic management of these diverse activities. The main drivers for BRM growth and maturity—around-the-clock service delivery, globalization and increasing operational risk—are expanding the scope of BRM beyond its roots in the IT department.[1] Organizations are forming cross-business, cross-functional programs and showing growing interest in finding a standardized way to manage them. Through standardization and potentially certification, businesses open the possibility of using BRM as a market differentiator, which only a rare few are able to do today.

To manage the similar, yet diverse techniques of continuity, recovery, availability and crisis management under one management umbrella, many BRM managers are following best practices formed over the past 30 years and are looking to the latest trends for answers about future best practices. In this paper, we'll explore IBM's proven, methodical and risk-centric approach to prepare, manage, and execute business resilience and continuity risk mitigation techniques across six defined layers of resilience. In particular, we'll look at recent trends to help you take your BRM programs to the next level and mitigate the ever-changing risks inherent in every environment.

Introduction to business resiliency management

Constantly changing business requirements have driven the evolution from early technology recovery solutions with timeframes of days to weeks, to today's environment of continuous business and IT operations. Where disaster recovery once gave way to business continuity in the mid 1990s, business continuity is now giving way to business resilience. Availability, recovery, security and compliance techniques have converged and must be managed concurrently to create an infrastructure that can sustain true business resiliency. It is the convergence of these techniques within a highly secure environment that requires business resiliency managers to administer more complex elements at the same time and in proportion to the level of service that the business demands.

To accomplish this goal, many companies are developing all encompassing, cross-functional programs to maintain continuous business operations and access to critical business data, while managing and predicting costs to achieve and maintain a highly ready state. The ability to blend solutions to accommodate the most critical business processes and applications with the highest level of protection—and still enable less critical applications with less stringent solutions—is a trademark of a resilient company.

Business resilience management is the holistic management of the processes to identify potential risks based on impacts that threaten an organization. One of the most critical aspects of achieving business resilience, a strong BRM program, can help enable organizations to rapidly adapt and respond to risks, as well as opportunities, in order to maintain continuous business operations, be a more trusted partner and enable growth.

BRM best practices

What will future business resiliency management best practices look like? Before anticipating and possibly predicting tomorrow's most effective or efficient methods, we should first examine today's best practices across six key facets of resiliency. The IBM Business Resiliency Framework parses an organization into unique, but interdependent layers consisting of strategy, organization, processes, applications and data, technology and facilities, and security. Examining an organization through these layers can help reduce complexity and improve BRM visibility into potential risks and exposures.

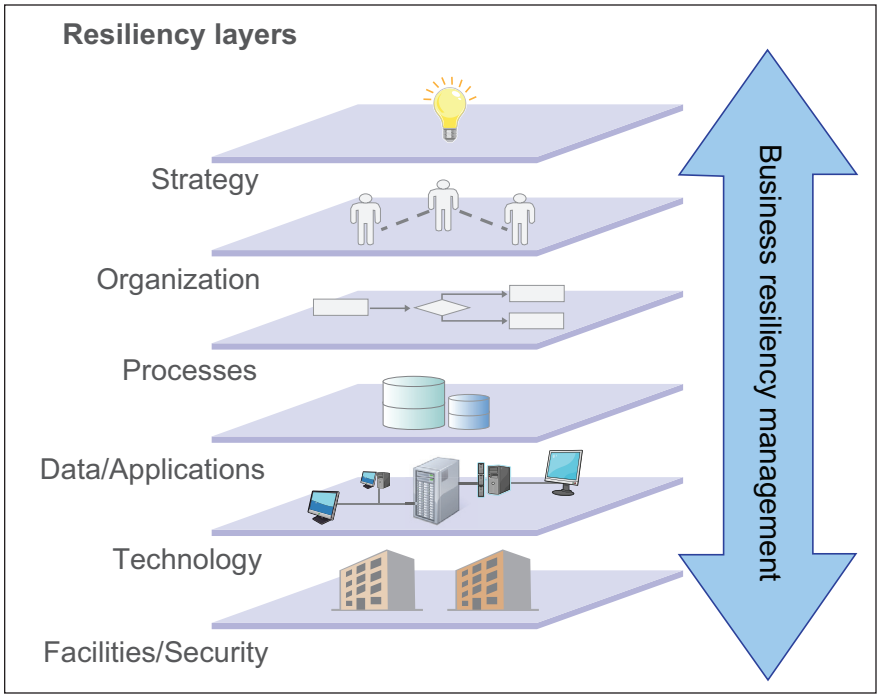


Figure 1: IBM Business Resiliency Framework

Furthermore, viewing a business in this manner also helps enable the identification of crucial interdependencies between business processes and the information technology that enables them. Understanding these interdependencies can give management the required context to prioritize business resilience initiatives and manage the program more efficiently.

Strategy

Resiliency begins with strategy. Since the business strategy is the roadmap for achieving business goals, a resilience strategy that is in harmony with business goals is imperative. The target is to enter a state of preparedness such that the action is thought out and pragmatic rather than impulsive and frantic. The motivation to capture these actions is established and defined at the strategy level and reviewed, monitored and enforced by a centralized, governing body.

Governance and program management strategy

Management support is essential to the success of the BRM program. BRM is an enterprisewide matter and should include all lines of business and be centrally managed by a cross-function, cross line-of-business governance committee. A governance and program management strategy should be selected and customized from one of the numerous standards, guidelines or frameworks published around the world today. Using a framework enables the disperse agents across the organization to work in a disciplined way through a well-defined governance and management structure. The governance policy should be linked to the corporate mission, culture and values, and should provide ways to quantify, track and communicate the value of the program to the organization using business language rather than operational metrics.

Risk- and impact-driven mitigation strategy

Fundamental to a solid BRM program is the need to investigate what could impact the function of the critical processes and resources needed to proactively reduce the risk of an outage. The characteristics of a best practices risk mitigation strategy are the prioritization of mitigation actions based on the impact to critical business resources. This is facilitated by a thorough risk and impact analysis process that identifies potential threats, such as events that cannot be

prevented, for example a hurricane, fire or strike, and their associated risks—the result of the threat occurring, for example, curfews, mandatory closings and building damage.

In large or more mature companies, this risk analysis is a component of the larger enterprise risk management (ERM) program. ERM, as a formal practice, is growing in visibility and importance. An ERM program may follow different frameworks based on industry, but most typically will include the common themes of identification, prioritization, response and monitoring.

Business resilience is a crucial design point for ERM programs and may cover a wide range of risk types[2] such as: business driven with an emphasis on strategic, compliance and financial risks; event-driven risk that focus on operational and hazard types; and data-driven risks that affect reliable and effective processing, reporting and dissemination of information.

Exercise strategy

All technical and business mitigation solutions must be validated. This is typically accomplished through exercising or testing the steps captured in a plan to ensure the documented procedures are executable and accurate, the solution can be completed in the time frame required, and personnel are trained in their roles. The exercise strategy helps protect the organization's investment, since without periodic exercising, the effectiveness of the plan can quickly erode.

Plans should be exercised regularly, commensurate with their importance to the company, and at least annually. Different types of exercises can be employed to ensure all facets of the plan and the solution are validated. These can include tabletop or walkthrough discussions for plan execution, simulation through active participation to enable the process or technology external to the production

environment, or full failover by switching from the production environment and operating from an alternate site. The use of virtual testing can help you emulate your recovery actions without interrupting production, while logging actions to create an auditable report trail.

Awareness and education strategy

Education and training of personnel in special, critical and multiple roles plays a significant role in the success of the plan execution and may influence the time required to execute tasks. An awareness and education strategy helps ensure all employees are aware of the plan, not just those who participate regularly. Pandemic preparedness is a good example of using awareness programs to educate personnel on simple techniques to maintain their health and the health of their family members to mitigate the risk of high employee absenteeism predicted during a major flu outbreak.

Crisis management and communication strategy

Crisis management is the process of managing multiple responses to an event with a consistent approach to respond quickly and appropriately, thus minimizing damage to the organization's reputation and business operations. A proper strategy in this area calls for clear command decisions, documented actions, defined roles and responsibilities, and the ability to communicate effectively and efficiently across the entire organization. Communicating during a crisis is probably the single most import aspect of preventing a small incident from becoming a disaster. The key is maintaining current, accurate communication lists for both internal and external contacts, written scripts for internal and external communications, company fact sheets, and ensuring employees are versed in public relations, legal response and insurance. The communication plan should include contingencies for the loss or major degradation of standard access for both voice and data networks. Reliance on the Internet and intranets can be affected, so contingencies that include out of region service providers still prevail.

Organization

Organizational considerations play an important role in achieving business resiliency. Many of the essentials of organizational change are required to build a successful resiliency plan, such as a visible, committed executive sponsor; documented roles, responsibilities and accountabilities; defined cross-line-of-business linkages; and identified skills that are critical to the organization.

Resilience organization design

The resilience organization consists of two main bodies: those who make the program run on a daily basis and those on the governing committee who define, manage and enforce polices defined in the strategy layer. While disaster recovery and even business continuity may have at one time been the responsibility of the IT department, the trend is to move this function out of the IT department and higher in the corporation reporting to or even managed by a C-level person. In the most mature industries and larger companies, the role of chief resilience officer is starting to emerge or the BRM staff aligns with the chief risk officer.

A centralized BRM committee's main responsibility is to set policy that guides the BRM program to:

- Provide clarity, definition and guidance to the participants and stakeholders.
- Encourage or mandate participation from the critical participants.
- Heighten communications to ensure awareness up and down the management chain as well as to all internal and external stakeholders.
- Enact and report regular and pertinent business measurements that show the success of the overall BRM program.
- Ensure accountability with responsibilities tied to job descriptions and adequate rewards for participation and success.

Processes

A resiliency plan should concentrate on both the business and IT processes that are most vital to the enterprise. Creating and sustaining processes that support resilient business operations and infrastructures requires identification of the minimum required process functionality during disruptive events, alternate processes and procedures that will allow operations to continue during times of stress, and redefinition of processes to achieve better workload balance.

Critical business process identification and prioritization

Critical business process identification is facilitated by a business impact analysis (BIA) that helps to prioritize the business processes and establish the required business case to defend the mitigation responses needed to protect them. Businesses increasingly require a more granular, or services view of their anticipated losses. In this type of approach, the analysis looks at the business silos, such as departments or functions, as well as across each silo, tracing a business service as it touches each department. The business processes are prioritized by analyzing the impact to the business due to the loss of that process and estimating the financial and non-financial risks to the company. This analysis produces a more realistic reporting of the potential overall loss due to the interruption of any one of the pieces required to produce the service.

Mapping business processes to their application and data, technology, and facilities layers ensure all dependent physical requirements, system, network and data storage needs are identified. This mapping should include analysis of upstream and downstream dependencies to determine input and output data streams for data synchronization. Technology dependencies should also be reconciled to ensure the correct recovery order or availability techniques are applied to the entire critical process and systems, not just applications. The same dependencies between the business units themselves should be reviewed to ensure the correct recovery order among processes, departments and even divisions.

Applications and data

Today, the ability to constantly provide reliable information to people both inside and outside the enterprise from multiple, disparate data and application sources is a requirement. Rather than being aligned only with technology, applications and data are now tightly linked with business processes and organizations.

Managed information protection

The goal of the BRM program is to ensure data is managed in a way to protect the business from losing its most valuable commodity—its data. The timely and accurate backup of data has to be considered, executed and validated by proving the ability to recover or access data operationally, such as to retrieve a user's deleted file, as well as for entire data pools (for example, from an alternate site). To reduce human error and increase the likelihood of capturing required data, companies are seeking out services and tools that provide higher levels of data automation to back up data from servers, desktops and laptops, wherever they are located, with minimal human intervention.

E-mail, a highly convenient form of communication, has become a necessity that businesses rely on not only for internal messages but also for around-the-clock access to external parties in and out of a recovery effort. Thus, access to e-mail has become a priority for communication during an event, making it critical for data protection solutions and availability.

Technology

Since a significant portion of most business budgets is used for building the IT infrastructure, it is prudent to align these investments with the enterprise's resiliency objectives. All important technology components must be considered when planning for resiliency, including hardware architectures, system software, middleware and networks. Each component must be examined to ensure that its level of availability—through reliability, redundancy or failover—is in line with the enterprise's resiliency objectives.

Risk- and impact-based solution design

Based on the substantiated selection of critical business processes and the risk tolerance of the company, the business resiliency manager can more confidently match risk mitigation solutions to the organization's need. One way to select an appropriate solution design is by using resilience tiers. Resilience tiers provide an objective scale to classify business resilience requirements into a set of consistent metrics and criteria across an organization. They also provide a set of definitions to establish business resilience requirements in terms of technical resilience capabilities on a continuum of service level requirements. Consequently the business requirements are linked to technical resilience requirements and capabilities.

Through standardization and disciplined implementation, the architect can design solutions that fit each tier based on the characteristics of that tier. Resilience tiers also provide the criteria and metrics to measure, manage and report on achieving business resilience goals often missing in most programs to gain management recognition. Figure 2 shows sample service resilience metrics and targets for possible tiers. While the names are immaterial, the example resilience tiers illustrate different targets for each of the three service continuity goals listed down the first column. Targets should be appropriate and customized based upon results of the impact and risk analyses.

Resilience Tiers	Platinum	Gold	Silver	Bronze
Service level objectives	Business functions that, if unavailable, will result in either financial or legal penalties based on regulatory restrictions *Typically assigned to the top 5 to 10 percent of applications that drive revenue and profits, and that highly impact brand reputation*	Business functions that present a potentially broad impact across the internal organization *Cannot afford to be without these functions during critical processing windows*	Business functions that support back-office functions such as analysis and reporting *Processes where the functionality can wait or must wait for large amounts of data to be restored*	Non-critical, back-end, offline business functions *Typically alternate, but less desirable, methods are available to achieve same business function to support extended outages*
Service level availability requirements	• Continuous availability • 99.999 percent • Zero planned outages	• Near continuous • 99.99 percent • Up to four-hour planned outages (maintenance)	• High availability • 99.9 percent • Up to four-hour planned outages (maintenance)	• Moderate availability • 99.5 percent
Service level recoverability requirements	Return to service in less than five minutes (all events)	Local: Return to service in less than five minutes. Data Center: Return to service in less than two hours	Return to service in less than two hours (all events)	Local: Return to service in less than eight hours Data Center: Return to service in less than specified timeframe (days to weeks)

Figure 2: Sample resilience tier table with target metrics

Many organizations cannot afford a one-size-fits-all recovery strategy tied to the requirements of their most critical applications, especially because an increasing number of applications are becoming Tier 1 (most critical). As a result, companies can implement a layered recovery strategy to contain costs and match the quality of service to the criticality of the IT service. Gartner predicts that "By 2013, more than 50% of midsize organizations and more than 75% of large enterprises will implement layered recovery architectures.[3]

Applying business resiliency techniques as part of the early product development cycle in all projects allows for earlier identification of resiliency needs. Thus, organizations can accommodate those needs as part of the early funding cycle rather than "going back to the well" after a new product, service or application is in production.

New technology is opening more opportunities to capitalize on hardware inventories. Virtualization of resources allows for more efficient use of server and data center capacity by provisioning it on demand, wherever and whenever it is needed. With the advent of cloud computing, the possibility of having more flexible recovery resources at your disposal increases. When tightly managed, test or development environments can be brought to bear on the recovery and post restoration work effort. However, these technical solutions mandate a higher degree of automation, training, and new management paradigms and disciplines to manage and execute when needed.

Facilities

Business resiliency management should encompass all enterprise locations and address the unique features of each location to achieve the desired resiliency level for the enterprise. Facilities and security considerations range from ensuring adequate power, heating and cooling, to the often-overlooked situations of providing and testing physical and logical security mechanisms, the ability to accommodate a virtual workplace when needs dictate, and the distribution facilities to handle changing business demands.

Work area solution design

Work area solutions ensure that the employee's working environment is available even if they cannot access the primary environment. Some decision makers who have a workforce recovery strategy use remote access technologies as part of that strategy. When selecting a work-at-home strategy, management should ensure that employees can work from home by ensuring access to vital documentation, secure high speed lines and printing.

When choosing alternate sites for work area relocation, selection of such centers must accommodate the employee's personal needs during a crisis such as child or elder care, living quarters and health care. It is critical to exercise this capability regularly to validate that the network capacity will support the extra work load, critical applications can be accessed securely, and employees remember how to sign in and access their work area remotely.

Due to increasing budgetary pressures, some companies "are looking to wring more from existing assets by using distant corporate buildings for secondary or tertiary recovery sites." [4]

Newer social networking applications can be used to reduce the culture change of moving to dispersed work areas and facilitate collaboration. Developments in information and communication technologies, together with the evolution of Internet-based social computing, can reduce human interaction costs; the cost of linking globally distributed people into coherent, highly interactive communities. How we use these newer technologies to our advantage beginning to be explored, but as this industry grows, the ability to link teams working remotely for more efficient results will greatly enhance the distributed, recovering workforce.

Site restoration and return home

The workforce cannot sustain operating from alternate locations indefinitely. Often left out of most plans are the steps for returning to the restored or rebuilt work location or data center. While it is impossible to complete all details before an event, draft project plans and outlines, checklists and established restoration service contracts are imperative to quick reaction after the event to assist with re-establishing your primary work site.

How IBM can help

Pulling together all of these interrelated and dependent practices and technologies—while remaining competitive, managing costs and protecting your business—can be daunting. Partnering with an experienced global leader in business continuity and resiliency can help you accomplish your goals and achieve a more proactive, rather than reactive, approach.

IBM has developed an extensive portfolio of business continuity and resiliency services that are designed to help you assess your disaster preparedness and manage disasters when they do occur. These services, along with IBM technology and consulting, can be customized for the particular requirements of your organization and allow the flexibility for you to manage as much or as little of your business continuity management program as you would like.

IBM Resiliency Consulting Services can be engaged to help you assess, design, implement and manage an enterprisewide risk and business resiliency program that includes plans for your workforce. From the initial step of performing a risk and impact analysis, through the final phases of validation and testing, IBM Resiliency Consulting Services can help ensure that in the event of a disaster, your business activities keep running.

IBM Resiliency Consulting Services – resilience program assessment assesses your end-to-end resilience program maturity against industry-leading practices and provides action plans for successful program management, applying regional guidelines and regulations where appropriate.

IBM Managed Resiliency Services are designed to help you avert the need for recovery by maintaining continuity of your critical business processes in case of disruptions and outages. While these services enable you to balance workloads, reduce downtime and limit data loss, they also include tools that specifically address workforce resiliency. IBM can manage and operate your resiliency services for you—either fully or partially. IBM Managed Resiliency Services include:

- Continuous availability, which can help you implement a cloud computing environment.
- Information protection, which can recover email following an outage and provide assistance during an emergency when normal lines of communication fail.
- Emergency notification and collaboration service, which provides an effective method to contact and help large numbers of employees, customers, and other constituents manage through emergencies and disasters.
- IBM Tivoli® Business Continuity Process Manager provides configurable processes to plan, test and execute IT service continuity.

IBM Infrastructure Recovery Services help you respond to and recover from disruptive events, and provide, among other services, crisis management and response and work area recovery. These services directly address the vital human component of your business continuity plan to keep more people productive and help build your reputation for corporate responsibility in the face of a disruption.

IBM provides a wide range of proactive and event-driven managed services, enabling you to select the services that are the most cost-effective and that provide the highest availability for your most critical business data and processes, along with many options for less critical data and processes. By managing and operating these services for you—either fully or partially—IBM can enable you to balance workloads, reduce application and system downtime, and reduce data loss. At the same time, IBM can help you to avoid or reduce capital expense, monitor and manage operational expenses and service levels, and reduce the burden on your IT staff.

Conclusion

The future holds exciting possibilities to increase the effectiveness of business resiliency management. This paper has examined new approaches, including:

- An increased use of enterprise risk management for prioritization of threats and risks.
- A granular, services-level business impact analysis that places business processes and resources in resilience tiers for easier, faster solution design.
- Solution design using resilience tiers and the six resilience layers for IT or business solutions.
- Some important characteristics of the BRM program from IBM across all six resilience layers.

In addition, implementing new emerging technologies and fresh ideas, such as the following, can keep your business in a resilient posture:

- Specialized notification and collaboration tools to increase effective communication across the organization
- Onsite versus remote data protection and specialized e-mail recovery
- Cloud computing for flexible, economic distribution of recovery services
- Virtualization to efficiently use server and system capacity
- Virtual testing and workflow automation to reduce human intervention

The challenges remain in pulling together all of these interrelated and dependent practices and technologies while remaining competitive, managing cost and protecting your business. Businesses today need to be proactive, rather than reactive. Partnering with a global leader in business continuity and resiliency with experience and resources can help you accomplish all of these goals.

For more information

To learn more about the benefits of protecting your information and implementing a world-class Business Continuity Management program through business continuity and resiliency services from IBM, contact your IBM representative, or visit the following Web site: ibm.com/services/continuity

http://www-935.ibm.com/services/us/bcrs/self-assessment/

Notes:

[1] Gartner, Research Roundup: Business Continuity Management and IT Disaster Recovery, February 2009

[2] Adapted from multiple sources, including: Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Enterprise Risk Management—Integrated Framework," 2004; Reuvid, Jonathan, *Managing Business Risk: A Practical Guide to Protecting Your Business*, 2nd edition, Kogan Page: 2005

[3] Gartner, Predicts 2009: Business Continuity Management Juggles Standardization, Cost and Outsourcing Risk, January 2009

[4] Tucci, Linda, "Recession squeezing IT disaster recovery budgets," SearchCIO.com, August 2009

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
February 2010

BUW03016-USEN-03