



Resilient infrastructure: Improving your business resilience.

*Gregg Goble, Vice President,
Resilient Business & Infrastructure Solutions*

*Howard Fields, Managing Principal,
Resilient Business & Infrastructure Solutions*

*Richard Cocchiara, National Principal,
Resilient Business & Infrastructure Solutions*



Contents

2 Introduction
3 Framework for resiliency
9 Building blocks of resiliency
12 Seven steps to achieving resiliency
17 IBM capabilities
19 Conclusion
19 For more information

Introduction

Today, business functions are virtually inseparable from the information technology (IT) that supports them. e-business has changed the way organizations operate and interact with their customers, employees and business partners. To sustain profits and capture market opportunities, organizations have increasingly embraced e-business, customer relationship management (CRM), supply chain management (SCM), and online trading applications. As daily business operations, and continued survival, become increasingly dependent on IT, organizations are planning and implementing resilient infrastructures—infrastructures that are capable of proactively responding to both anticipated and unexpected stresses and strains. These stresses and strains can be both positive and negative in that they may reflect fluctuating market demands, man-made events, component failures and natural disasters.

In today's marketplace, business disruptions are no longer merely embarrassing or inconvenient. They can be potentially fatal to an enterprise. At the very least, they can lead to lost market opportunities, degraded brand and reputation, lost customers, and declines in shareholder value. At the very worst, they can result in circumstances that lead to the demise of the enterprise. To limit the potential financial impact of stresses to the infrastructure, an enterprise must improve its ability to respond accurately and rapidly to both disturbances and opportunities.

While not every business risk can be eliminated, many can be mitigated and managed. To contain business risk within acceptable levels, an enterprise and its value chain partners must ensure that their combined infrastructure is resilient—fortified, recoverable and adaptable. From a business perspective, a resilient infrastructure can protect the ability of the value chain to “deliver the goods” regardless of unexpected events. This manifests itself in security-rich, agile, available and recoverable business processes, technologies and organizational constructs.



Highlights

Viewing a business and its value chain in terms of various solution layers can help improve insight into potential risks and exposures.

This paper defines the concept of resiliency within the context of today's increased uncertainty. It offers a new approach to improving resiliency and explores some of the options available to an organization striving to better position itself for unimpeded growth and success.

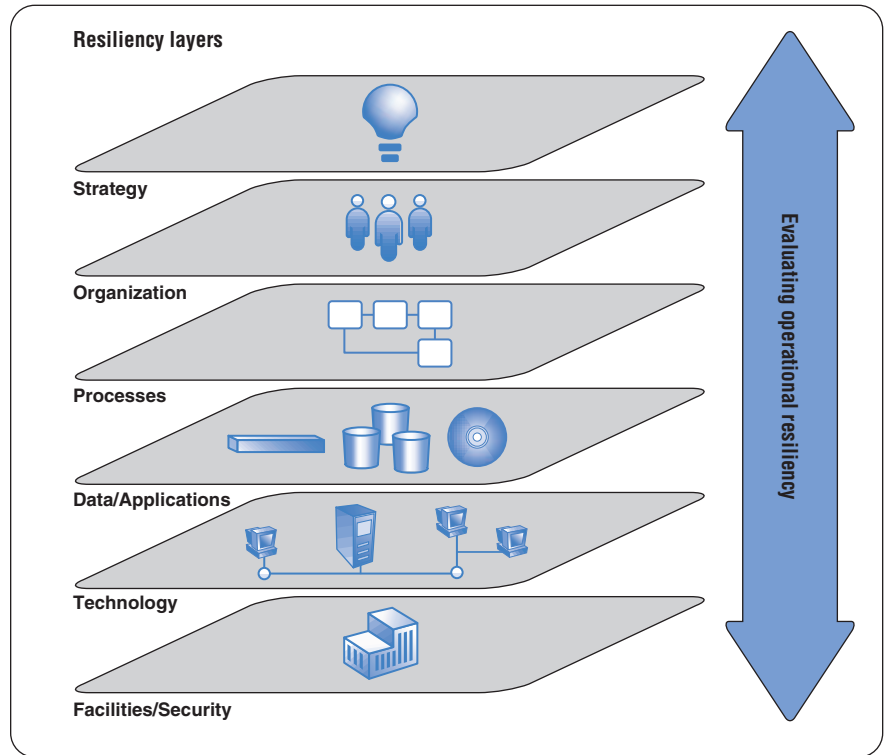
Framework for resiliency

An organization's infrastructure can be quite complex. It consists of many components that sustain the delivery mechanisms necessary for the business to achieve its goals and objectives. In many cases, this infrastructure extends beyond the enterprise walls through a dynamic value chain of suppliers, distributors, partners, and even customers. To reduce complexity and improve management insight into potential risks and exposures, a business and its value chain can be viewed through the lens of six unique "solution layers." These layers are strategy, organization, business and IT processes, data and applications, technology, and facilities and security. Viewing a business or value chain in this manner enables the identification of crucial interdependencies between business processes and the information technology that enables them. Understanding these interdependencies gives management the required context to prioritize business enhancement proposals.



Highlights

Planning operational resiliency



An effective operational resilience strategy begins with a comprehensive assessment of the risks faced by an enterprise, including those that derive from its position in the industry, as well as from IT and organizational factors.

Strategy

Resiliency begins with strategy. Since business strategy is the roadmap for achieving business goals and objectives, and since resiliency protects your ability to reach those goals and objectives regardless of anticipated and unexpected events, logic dictates that resiliency must become a component of strategy. This is best accomplished through a holistic resilience assessment that examines and scores three sets of factors that affect business success. The first set examines unique vulnerabilities and risks specific to an enterprise given its industry and its competitive position within that industry. The second set examines an enterprise's strategies that address well-known IT issues including continuity, availability, performance, support, capacity, security, governance, etc. A third set of factors examines the baseline organizational culture and the degree to which it enables employees to successfully handle the anticipated and the unexpected stresses and strains that they face every day.



Highlights

As a company's business model evolves in response to changes in the marketplace, so too must its strategy for sustaining a resilient business environment.

Since an overall strategy reflects a comprehensive analysis of a business in relation to its marketplace, industry and value chain, resiliency planning must be viewed as a continuous process. As market demands change, business vulnerability points change with them. Therefore, a resiliency plan must be viewed as a continuum within an overall business strategy.

Ensuring the success of a resiliency plan requires making a determination of how it will be integrated and managed in light of the governance model. In addition, the near-term evolution of the business model must be evaluated, business requirements prioritized and the current business risks and acceptable tolerance levels identified.

Funding for resiliency, and measures for determining the return on resiliency investment, must be defined and agreed to. Once implemented, a resiliency plan should yield a measurable return consistent with business goals.

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 communication protocols; defined cross-line-of-business linkages; and identified skills that are critical to the organization.



Highlights

Identifying the minimum process functionality an enterprise requires to sustain operations in times of stress is key to increasing the company's preparedness for unanticipated events.

Achieving organizational resilience should go beyond typical organizational issues and may include the creation of virtual, flexible and distributed workplaces to enable collaboration among employees, suppliers and customers anywhere, anytime. The degree of workplace flexibility required is dependent on an organization's current capabilities and critical business processes, and is influenced by its culture. In effective workforce transitions, organizational change management is a critical component in increasing the speed of change and ensuring the durability of the change while minimizing disruption to the organization.

Business and IT 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. Alternate processes and contingency plans should be clear to stakeholders at all levels in the organization while still adhering to a corporate governance model that safeguards against improper use of business processes or assets. By creating and/or modifying business processes and organizational environments that mutually support virtual, flexible and distributed workplaces, a business can increase its preparedness to respond to and recover from unanticipated events.



Highlights

Various measures can help ensure that data and applications can withstand unanticipated events.

Investment in IT infrastructure must be aligned with an enterprise's overall resiliency objectives.

Data and applications

In today's marketplace, 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, data and applications are now tightly linked with business processes and organization. Specific measures, such as determining the tolerance level of key applications to infrastructure failures and possibly diversifying data and applications, must be done to help ensure a resilient enterprise. This diversification of applications and data will allow for greater workload balancing as well as protection against organizational impacts due to the loss of key personnel. Opportunities for streamlining applications and simplifying data and application architectures through standardization should also be explored. Finally, end-to-end tests of application suites supporting critical business functions should be performed on an ongoing basis to ensure that performance, availability and scalability continue to support changing business resilience goals.

Technology

Technology plays an essential role in building a resilient, flexible business. 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.



Highlights

Overall resilience depends on the reliability and redundancy of nearly all of a company's technology components.

Both physical and logical security must be taken into consideration when planning for business resilience.

Important technology components to consider when planning for resiliency include 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. Specifically, defined architectures must be in place for critical hardware functions; single points of failure should be known and addressed in support of overall resilience goals; actual availability measurements should be taken and compared to the enterprise's availability requirements; and the ability for infrastructure to recognize and repair itself with little or no human interaction should be examined.

Enterprises that require short recovery times may need to focus specific attention on hardware, software and network architectures in their business resiliency plans. This might include continuous replication from a primary processing site to an alternate site, which can then be used in the event that the primary site becomes unavailable. In addition, specific requirements for supporting critical hardware and software need to be examined to help ensure rapid response in the event of component failures.

Facilities and security

When examining the resiliency level of an enterprise's facilities, one should include environmental considerations, geographical locations and dispersion, levels of security access to the facilities (physical and logical security), and power protection plans. A resiliency plan should encompass all enterprise locations and address the unique features of each location to achieve the desired resiliency level for the entire enterprise. Facilities and security considerations range from the obvious, such as ensuring adequate power, heating and cooling, to the often-overlooked questions of providing and testing physical and logical security mechanisms, the ability to accommodate a virtual workplace when needs dictate, and how well facilities are really distributed and able to handle changing demands.



Highlights

In addition to taking obvious security measures for protecting their facilities, enterprises must not overlook less-obvious measures for protecting vital corporate information.

Recovery, hardening and redundancy are widely recognized as vital ingredients of a successful business continuity plan.

While obvious precautions must be implemented to protect a company's buildings and data processing facilities, less obvious measures are also needed to ensure the security of the vital corporate information that could be susceptible to attack from internal and external snooping, sabotage or theft.

Building blocks of resiliency

If the framework for resiliency provides us with the architecture to begin creating a resilient infrastructure, the building blocks of resiliency provide the foundation. The building blocks for implementing a resilient infrastructure include recovery, hardening, redundancy, accessibility, diversification and autonomic computing. The first three building blocks are widely recognized today as vital ingredients of successful business continuity plans.

Recovery—The provision for safe, rapid, offsite data recovery in the event of a disaster.

Hardening—The fortification of all or part of an infrastructure to make it less susceptible to natural disaster, employee error or malicious actions.

Redundancy—The duplication of all or part of the infrastructure to supply hot, active backup service in the event of an unanticipated event.

These building blocks are primarily defensive in nature. They are necessary for protection, but by themselves, do little to help improve your competitive posture. Using these tools alone can lead to a “bomb shelter” mentality: You create a bomb shelter miles away, stock it, and forget about it. It doesn't get updated because it's viewed as “insurance”—a static initiative. You feel more secure and protected with it, but it doesn't help the bottom line.



Highlights

Resiliency is more than taking defensive steps to protect an enterprise; it must also include proactive measures for improving competitive position.

Resiliency is not simply an “insurance” measure, but a comprehensive and robust strategy to gain competitive advantage. There are three additional building blocks that can help you move from a defensive stance to a proactive and competitive position within the marketplace: accessibility, diversification and autonomic computing.

Accessibility—The ability for enterprise personnel, partners and customers to easily access the infrastructure from anywhere, in the event that the primary work site is inaccessible. It includes the deployment of diverse communication technologies (e.g., wireless, fax, e-mail, instant messaging).

Diversification—The physical distribution of resources (hard assets and people) and implementation of diverse communication pathways to decrease the probability that a single disaster will incapacitate the enterprise. The goal is to create an operational infrastructure that is physically distributed but capable of being managed as if it were a single consolidated entity. Thirty years ago, when developing what eventually became the Internet, the U.S. military postulated that the chief tenet of resiliency was diversity. The idea behind diversification was to “not put all the eggs in one basket.”

Autonomic computing—The inclusion of self-managed hardware and software components in the infrastructure. These products self-regulate, making decisions without human intervention or, at a minimum, bypassing a problem and alerting the human attendant to initiate appropriate action. Many of these products are available today, and more will be introduced into the market in the near future. As technology progresses, resilient infrastructures will contain more autonomic components with self-configuring, self-healing, self-protecting and self-optimizing capabilities.



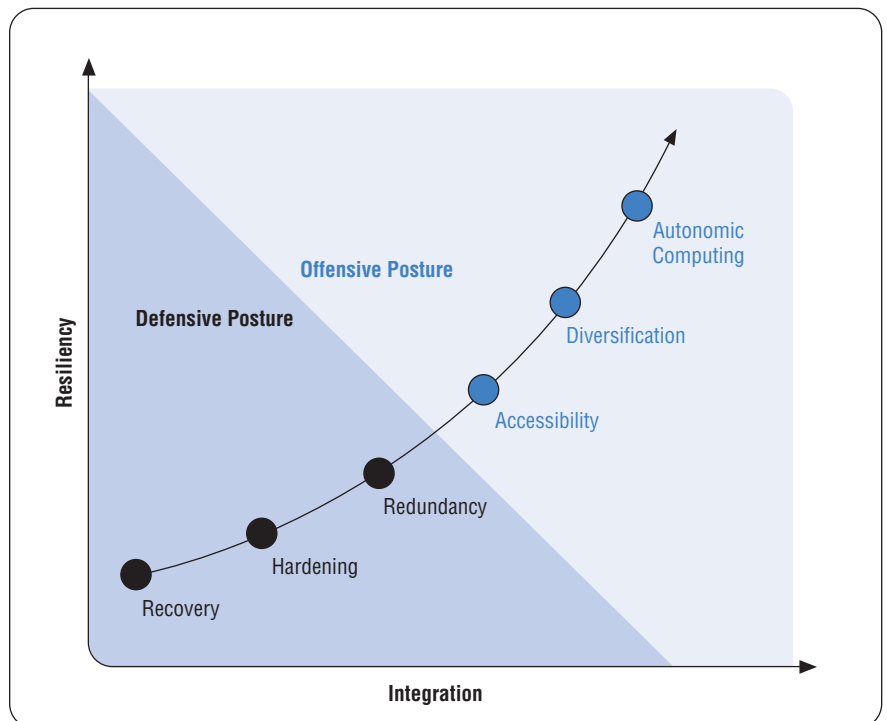
Highlights

An enterprise may implement the building blocks of a resilient architecture across the board, or may apply them selectively, depending on particular needs.

Autonomic computing products not only help protect an enterprise's IT infrastructure, but can lower the total cost of ownership and provide a powerful competitive advantage. The idea behind autonomic computing is to provide a resiliency solution that is integrated into daily business operations and not a separate contingency tower that's ignored. It is a solution that provides a platform that is highly agile and helps lower response time.

These building blocks can be utilized in a homogeneous fashion or in various combinations depending upon your needs. In most cases, companies will adopt a hybrid approach, such as "diversifying" operations and only "hardening" certain sites and links where critical applications or data reside.

Building blocks for a resilient infrastructure





Highlights

The first step in creating a vision of a resilient enterprise is identifying what makes your enterprise unique.

Seven steps to achieving resiliency

In order to begin the journey to a more resilient infrastructure, there are seven steps you can take toward achieving resilience.

Step 1: Identify the uniqueness of your business

To include resiliency as an integral component of your overall business strategy, the first step in creating a vision of a resilient and flexible environment is to recognize what it is that makes your business successful. Every industry and every business within an industry is unique, and it is often that uniqueness that creates success. The components that define the uniqueness of your business need to be clearly identified before a resiliency strategy can determine ways you can improve the degree to which your business environment is adaptive and recoverable from disruptions. The components are defined as business processes and functionalities that must operate effectively if a business is to remain viable. These include common processes and certain demands on those processes as dictated by your industry. Each process and functional element should be ranked to allow the prioritization of resources and a structured approach to move toward further analysis of your business environment.

The scope of resilient infrastructure should be evaluated within the context of your business. Every business organization is unique and operates in a different business and cultural environment. An organization should prepare at a level that is appropriate to its unique business and industry requirements, capabilities, future visions, business goals and budget constraints.

Identification of stresses or “scenarios” that could cause impact to your defined processes is critical in assessing your ability to cope with any situation. The scenarios that you define drive the actions you need to take in order to mitigate the risks associated with those stresses.



Highlights

Taking a holistic view of the risks and vulnerabilities that your business faces can help you implement the optimal enterprise-wide protection strategy.

Enterprises are affected by a variety of external factors, from social unrest to economic change to technological innovation.

Step 2: Assess your vulnerabilities

Risks should be identified and assessed in all key business areas by involving both business and IT executives. Recognition and understanding of the vulnerabilities your business faces, and analysis of the impact to your business as a whole, will enable you to survive and stay competitive in challenging and uncertain times. Traditional risk management focuses on individual processes or business entities. The complete enterprise relies on both a complex combination of processes that may change according to conditions, and a network of external interactions and dependencies. A holistic view is required to ensure enterprisewide protection and maximization of the organization's ability to perform under extreme circumstances.

While the catastrophic events of September 11th can serve as a wake-up call, the drivers for resiliency implementation are much broader than terrorism. Examination of how an enterprise is affected by the increasing variety of environmental, social, political, economic and technological issues as well as regulatory challenges must be considered when formulating a solution for infrastructure resilience. Each of these drivers can threaten the viability of your enterprise.

Social unrest—Terrorism, employee error/sabotage and cyber-attacks all seem to be on the rise. Hard assets, information and personnel can be targets.

Natural disasters—IT assets and personnel are often located in high-risk areas.

Political pressures—Government regulation, oversight and monitoring will continue to grow. Governments are also starting to mandate their employees to work from home in order to help ease environmental stresses.



Highlights

Infrastructure resilience must be examined in light of the potential business impact of disruption in each of an enterprise's locations.

Economic change—Mergers, bankruptcies, or even momentary operational failure of a key supply chain partner can cause significant disruption. This driver is exacerbated in a global economy.

Technology—Proliferation of technology, pervasive computing, unpredictable demand fluctuations, and the shortage of skilled IT workers are expected to increase.

Step 3: Determine the level of resilience you need

Risks should be assessed and potential business impacts determined. The understanding of potential loss of business value associated with IT infrastructure readiness is a mandatory element of analysis.

Many organizations operate worldwide. Although a company's headquarters may be located in a very safe country, its manufacturing function may be located in politically tense areas, or its sales offices may be located in volcanic areas. The global corporation must consider resilience from a global perspective. For example, a global organization should have a global business continuity and recovery strategy that includes local needs.



Highlights

It is important to balance cost with risk in establishing a resilient infrastructure.

An integral part of a successful business strategy is making resiliency assessment and planning an ongoing process.

Step 4: Balance the associated costs, budget and level of optimum availability you can afford

Once all the key business areas have undergone appropriate risk assessments, the enterprise should determine the types and levels of risk tolerance and identify the types of mitigation measures that are affordable. It is vital to balance costs with business risks. Any design of highly available or resilient networks should incorporate the minimization of downtime associated with anticipated or unanticipated disruptions.

Step 5: Integrate your resiliency plan into your business strategy as an ongoing process

As market demands change, your business vulnerability points change too. Therefore, a resiliency plan must be viewed as a continuum and not a single, static initiative. How an enterprise operates within that continuum, and uses selected tools, products or concepts will differ depending on many factors, such as its industry, competition, location, market, business model, starting infrastructure and budget. A resilient infrastructure is more than a set of products. Investing in hardware and software without mapping to the business requirements and implementing the associated business processes, will not yield an acceptable return. The resiliency of your infrastructure should be assessed periodically, in concert with changes in your business strategy and operations, based on market demands. The key is to match the right strategy and solution to your specific situation as it evolves.

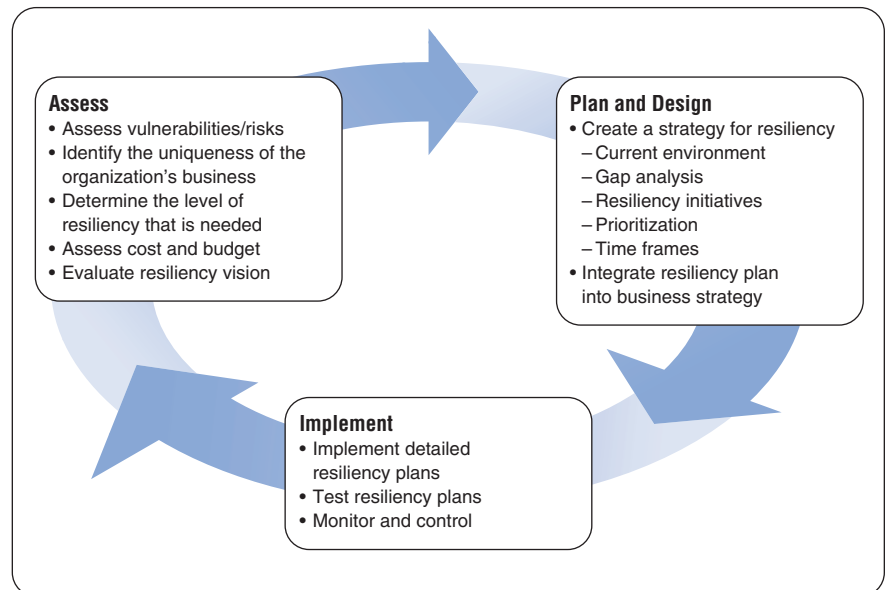


Highlights

Planning for business continuity, risk management and monitoring, as well as controlling availability levels, should be an integral part of the overall business and IT management process. The degree of resiliency that has been achieved to date must be sustained. In addition, you must continuously monitor, control and reevaluate your resiliency plan and environment in order to recognize changes and adapt to them to ensure success in today's fast-paced, changing economic environment. Assessing the resiliency of your infrastructure must be viewed as a continuous process rather than a one-time initiative. Enterprises need to be proactive and incorporate resiliency as part of every new business system and as part of the IT management process. A Gartner Group study indicates that, "to become resilient, virtual organizations, enterprises should make business continuity planning a part of enterprise culture."¹ Building resiliency as an everyday component of your enterprise enables a return on your IT investments.

The process of ensuring the resilience of the business environment is one that continually evolves in response to changing business conditions.

Resiliency process





Highlights

Continuous monitoring and testing of a resiliency plan are vital to ensuring an organization's ability to meeting its objectives.

IBM can assist you in all phases of establishing and sustaining a resilient business environment.

Step 6: Test your resiliency plan

Every component of your resiliency plan should be tested periodically through simulation of various business stress scenarios to ensure that the processes are working together, the people involved are familiar with the processes, and the technology can support your backup plan.

Step 7: Control and monitor your resiliency process against your environment and market demands

The objective of a business resilience plan is to define, document and test an organization and the actions put in place before, during and after a stress condition to ensure acceptable continuity of company operations. Continuous monitoring ensures that the implementation satisfies the targeted objectives. All plans must be rehearsed and reviewed periodically to ensure that all applications and processes work as planned and are still appropriate to the current business environment.

IBM capabilities

IBM understands just how complex the interdependencies of any enterprise's business and IT infrastructure can be. We can assist you in developing a more resilient business environment by identifying and assessing risks, formulating a resiliency strategy, providing end-to-end migration support and implementing the necessary processes, systems and tools to effectively manage your operational resiliency. More importantly, we can accomplish this in a short period of time using time-tested methodologies and tools.



Highlights

We work with you to help ensure that you make the most of your existing IT investments when implementing a business continuity strategy.

We assess the opportunities as well as the vulnerabilities, given our view of the next likely phases in the IT evolution. We examine the many working layers required for an optimal infrastructure implementation: strategy, organization, business and IT processes, applications and data, technology, and facilities and security. Solutions are tailored to your industry-specific business elements and processes, existing infrastructure, current and desired business model, competition, budget constraints and various other factors. We help you incorporate business and IT components into one safe and competitive resiliency strategy.

Resiliency offerings from IBM include assessment, consulting, integration, deployment, testing, outtasking and outsourcing services—as well as a broad spectrum of products, processes and platforms. Understanding that heterogeneous business environments and tight budgets are a reality, our solutions are focused on leveraging existing investments and optimizing the value of your IT investment.

The combination of our experience, industry expertise, world-class research and development capabilities, alliances with leading industry leaders, and global presence offer a powerful partnership to assist you in developing a roadmap that will take you to your desired level of infrastructure resilience.



Highlights

To sustain competitive advantage, an organization must be able to respond quickly to disruptions as well as opportunities.

More than a static insurance policy, implementing a resilient infrastructure is a continuous process for proactively managing risk and capturing market opportunities.

Conclusion

In today's marketplace, an enterprisewide vision for resiliency is imperative for an organization to gain and sustain its competitive advantage. An organization cannot afford to be ill-prepared for unanticipated events and must develop a strategy to respond rapidly to disruptions. Demands, risks and opportunities abound, ranging from market fluctuations to employee error and misconduct to earthquakes and terrorism. Disruptions can be catastrophic and can lead to loss of market opportunities, degraded brand and reputation, loss of customers, and decline in shareholder value.

Building a vision for resiliency begins with the recognition and understanding of the infrastructure vulnerabilities an organization faces, and an analysis of the potential impact of those vulnerabilities on its business. It includes a holistic examination of the various working layers: strategy, organization, processes, applications and data, technology, and facilities and security. A resiliency plan should be tailored to the organization's industry-specific business elements and processes, existing infrastructure, current and desired business models, competition, budget constraints and various other factors. A successful resiliency plan balances the associated costs, budget and optimal level of availability with affordability.

Migration to a resilient infrastructure is no longer viewed as an "insurance" measure, but a continuous, proactive process in gaining or sustaining advantage over the competition. A resilient infrastructure can proactively mitigate and manage key business risks to enable your enterprise to capture market opportunities.

For more information

To learn more about IBM Global Services and IBM Resilient Business and Infrastructure Solutions, contact your IBM sales representative, or visit:

ibm.com/services/its/us/solutions.html



© Copyright IBM Corporation 2002

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

Printed in the United States of America
09-02
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

1 Witty, Roberta. *Building Business Continuity Planning Into Every IT Project*. Gartner Group, December 18, 2001.