IBM Business Continuity and Resiliency Services
January 2009

Business resilience: The best defense is a good offense

Develop a best practices strategy using a tiered approach

Contents

Introduction

In the world we live, disaster recovery is not an option, it's a must. But is just thinking about disaster recovery limiting your view point? Should you consider a broader approach that is systematic and proactive, instead of reactive? At a time when you need it most, a strong business resilience strategy can save you time, effort and money. Instead of typical strategies and execution for recovery, with business resilience strategies in place, your business can be ready—right from the start.

Perhaps you have heard of business resilience concepts, or maybe you have even considered implementing resiliency strategies in your organization but need guidance about what steps you need to take to optimize your investment and protection. This paper will provide you with a better understanding of the value of business resilience and how your IT architecture and management teams can use a tiered resilience approach to balance and align your technology capabilities and investments with your business requirements.

Highlights

Business resilience is the ability to rapidly adapt and respond to risks.

What is business resilience?

Business resilience is the ability to rapidly adapt and respond to business disruptions and to maintain continuous business operations, be a more trusted partner, and enable growth. True business resilience starts with understanding exactly what your business needs in order to survive unexpected events and plan ahead for challenges that could come at any time. Whether an event is IT related, business related, or a natural disaster, there will always be challenges to overcome. Think of business resilience as your ticket to continued business service and operational continuity—proper planning, readiness, and the ability to respond quickly to any threat or opportunity.

Focusing only on disasters lead organizations to work defensively, but a proactive approach to business resilience helps enable your organization to respond to an unexpected event more quickly and more cost-effectively. In addition to disaster situations, a strong business resilience program can help your organization prepare for audits and demonstrate compliance with regulatory requirements.

Perhaps you already have a disaster recovery plan in place. Isn't that good enough? When it comes to data privacy and system outages, and your business is on the line, there is no such thing as "good enough." Business resilience is important because effective resilience strategies enable you to avoid costly downtime, avert many security attacks, and lessen the impact of other catastrophic events.

With the constant-changing landscapes of today's business environments, are you ready?

In our constantly changing business environments, organizations face increasing risk exposures due to greater global and regional dependencies, in addition to complications with supply chains and global demands. In tight, competitive markets and uncertain economic times, brand vulnerabilities and data integrity risks also top the priority list. However, perhaps the most common vulnerability is business disruption or downtime. When day-to-day business is disrupted, for any reason, the financial impact can ruin your business. The indirect impacts of downtime such as lost market share, decreased productivity, regulatory non-compliance and damaged reputation are equally damaging. To get an idea as to if your business is ready for the next threat, interruption or challenge, ask yourself the following questions:

- *Have you recently experienced a disruption? What impact did it have on your operations?*
- *What risks pose the greatest threat to your continuous business operations?*
- *Are your business operations sufficiently scalable to accommodate a major increase in workload, in response to a spike in demand for your services?*
- *How does your current recovery capacity match your peak business processing volumes?*
- *Have you considered the resilience capabilities of your key business partners and third-party service providers?*

Highlights

Business risks can be event driven, data driven or even business driven.

What are business risks exactly?

Your business is exposed to risks that can come from all directions and in many scenarios. Business risks can be event driven, data driven, or even business driven. These risks are more prevalent during events that are triggered by regional power failures or natural disasters. However, your business is also at risk from relatively minor incidents. In fact, most disasters are the result of a collection of relatively small events happening at the same time in response to a common trigger.

During data-driven events such as virus attacks, data corruption, disk failure, application outages, and network problems, you can minimize your exposure if you fully understand and prepare for, or even prevent a disastrous event. The same can be said for business-driven risks such as audits, new product roll-outs, future marketing promotions, or even failure to meet industry standards. If you are prepared for these events, you are in a better position to react faster, meet requirements and often exceed expectations.

Event-driven risks such as natural disasters, regional power outages, acts of war, or even economic downturns can be minimized if you identify your vulnerabilities and plan accordingly. If your resilience strategy plans for these events, the actual impact to your business can be reduced.

The following illustration provides an overview of specific data, business and event-driven risks as well as estimated monetary consequences:

The curve on this chart follows an approximate $100,000,000 cost of outage. Consider that small cost outages that happen frequently have been reasonably well addressed by technology solutions such as antivirus software and firewalls, etc. Disk failure and data corruption problems have also been reduced or eliminated by technology-related solutions. Organizations now need to address business and event disruptions that are lower in probability, but of much greater impact should they occur.

By identifying potential vulnerabilities, you can design resilience solutions so that you are ready to respond and minimize impact of disruptive events.

Highlights

Key challenges

- ***Viewing resilience as a strategic enabler***
- ***Defining the value of business resilience***
- ***Working with advanced technologies***
- ***Maintaining continuous availability for your business services***

Key challenges

Implementing any resilience plan comes with challenges. One of the key challenges is assessing risk versus cost—how vulnerable are you and how much will it cost to protect you? A second challenge is moving executives away from an insurance mentality and toward viewing resilience as a strategic enabler. In today's tight economic climate, there is intense internal competition for resources. Rationalizing the return on investment of resilience strategies can be difficult.

From an IT perspective, many companies face complex challenges when dealing with advanced technologies. For example, many organizations use security technologies such as firewalls and encryption. If your organization is faced with a disruptive event or outage, will you be able to provide continuous availability for business service? If, in fact, you use these technologies, implementing alternative resources during disruptive events for high availability is the key to proper preparation. Effective business resilience strategies can help you identify alternative solutions and plan for those times when you need it most.

A major challenge for many organizations is determining which solution is best and provides the optimum amount of protection. Once this decision is made, procuring funding is often the next challenge. A key to successful business resilience is fully understanding the level of protection your business needs and then creating a strategic plan accordingly. This will help protect you from wasting money on unnecessary technologies, while still providing effective business resilience. Getting executive support for funding is more easily facilitated when a sound plan can demonstrate the value of business resilience across the organization accounting for business, workforce and technology requirements.

Perhaps the most overlooked challenge with resilience planning is the human factor. During times of distress and chaos, organizations focus available resources on responding to difficult situations. Often, individuals work around the clock until the situation is resolved. Sustaining overworked personnel may not be an effective business strategy, especially when a crisis is at hand. In times of crisis, you need your employees at peak performance. An effective business resilience approach can help you take a look at potential risks and plan your workloads accordingly. When making a mistake is not an option,

Highlights

this type of strategy reduces stress on your employees and cuts down on potential human errors due to overworked personnel. You can also develop strategies for times when your workforce may be unavailable, during a natural disaster, for example.

Using resilience tiers as a best practice for defining your architectural approach

The most effective resilience planning comes from understanding your situational and organizational needs before a disastrous event can occur. Resilience tiers help you accomplish this. Resilience tiers help you understand how much resilience you really need throughout your entire enterprise, and also help you identify how to optimize your investment.

Resilience tiers classify business resilience requirements into a set of consistent technology metrics and criteria.

Resilience tiers use a classification system that defines levels of resilience to match your business-driven requirements. Resilience tiers span all business units, services or technologies, and streamline the direction for building a resilient architecture. Resilience tiers provide an objective scale of classification for business resilience requirements—a set of consistent metrics and criteria across your organization that are then linked to technical

resilience requirements and capabilities. Business resilience requires an architectural approach that also spans the breadth of enterprise capabilities. Resilience tiers provide that approach by:

- *Defining a broad continuum of business resilience requirements that apply to all IT-enabled processes and services in an enterprise*
- *Linking those requirements to a set of technology domains that address all capabilities and resources in the IT environment*
- *Providing technical characteristics, criteria and metrics that enable the results to be measured against business resilience expectations and to be monitored and managed for ongoing operations*

For example, consider the different expectations and terminology for availability requirements used by IT executives and business executives. IT architects and executives analyze performance in uptime measurements, typically IT service level agreements that exclude non-operating hours, such as maintenance windows. However, a business executive assesses performance in terms of the tangible availability of business services, regardless of the cause of disruption. From a business perspective, there is no distinction between availability and uptime. A true resilience measure is holistic, viewing the availability of a robust business service and not an availability average of each functional component.

Highlights

Resilience tiers help rationalize the optimum resilience solutions.

Benefits of resilience tiers

Defining, developing and maintaining resilience tiers and associated resilience capabilities have a number of benefits to an enterprise, such as:

- *Business-to-IT alignment*
- *Rationalization of investments in resilience capabilities*
- *Improvements to enterprise risk planning, strategy and architecture*
- *More prescriptive management of the IT environment to achieve enterprise-wide business resilience*

Resilience tiers can also help with gap analysis across the business, service and technology domain levels, as well as with the reuse and integration of resilience solutions aligned to resilience tiers with solution architectures.

Another benefit is that traditionally, disaster recovery managers own the budget for disaster recovery and IT development, while operation managers have the need to design resiliency into their technical solutions. Resilience tiers help bridge the communications and planning gap for business continuity resilience and planning. In addition, resilience tiers can help you pursue resilience requirements as an integrated, enterprise-wide approach that achieves greater affordability for your organization.

How you can use resilience tiers

There are multiple scenarios in which you can use tiers to strategize and align with your business resilience needs. For example, for new application development and deployment, resilience tiers provide the comprehensive set of definitions, technical characteristics, criteria, and metrics that you need to design to specific service levels of service. Using this objective and quantitative approach as part of the non-functional requirements definition and prioritization will ensure that the resilience objectives and acceptable costs, will be integral to the overall service quality. In addition, the cost and time to design into new applications is much cheaper as opposed to retrofitting into a production environment that is experiencing operational outages.

An organization can also use resilience tiers for guidance to mitigate the potential chaos caused by situations such as mergers and acquisitions. The merger of two IT organizations can result in differing, and sometimes even incompatible processes for managing day-to-day operations—as well as lengthy debates and delays in prioritizing new development and deploying new technologies. Resilience tiers provide a framework for selecting best practices from each, enabling two IT organizations to align to a single, target architecture. Resilience tiers can help to reconcile business resilience requirements and to guide the infrastructure requirements, architectural design decisions and major initiatives that will be implemented to achieve the future state resilient IT environment.

Highlights

Resilience tiers help define a framework that addresses all infrastructure components.

Lastly, resilience tiers are a critical element in cloud computing initiatives. A tiered resilience approach enables you to define a replicable and measurable framework that can address all infrastructure components including storage, networking and load balancing, and that can scale to address a range of client resilience requirements. In addition, the tiered resilience approach applies to a wide range of architectural patterns and resilience solutions such as redundancy, clustering, grid, virtualization and replication.

Who should define and maintain resilience tiers?

In general, definition of resilience tiers is a team responsibility. The primary teams are service level management team (IT) and business representatives; they should take responsibility for the definition, documentation, maintenance and communication of the resilience tiers. Secondary teams should include enterprise, business, information system (IS) and IT architecture teams as well as the requirements management team; they should contribute and support the primary team effort.

Four levels of resilience

IBM has a four-tier approach to resilience tiers. Each tier serves as a set of design guidelines that specify the characteristics of industry best practices for each of eight technology domains: facilities, network, storage, server, database management system (DBMS), middleware, application architecture, and systems management.

These domains span the four resilience tiers defined by IBM as Platinum, Gold, Silver and Bronze; while IBM categorizes these tiers as such, some technology professionals may refer to resilience tiers as Tier 1, 2, 3, and 4, or Priority I, II, III, and IV, or even as critical, essential, routine, and non-essential business applications. More important than the labels is each

Highlights

Four levels of resilience:

- *Platinum*
- *Gold*
- *Silver*
- *Bronze*

resilience tier translates into defined metrics categories, such as availability targeted typically defined as 99.999 percent, 99.99 percent, 99.9 percent and 99.5 percent for Platinum, Gold, Silver and Bronze, respectively as provided in the following table:

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. During critical processing windows cannot afford to be without this function.	Business functions that support back-off functions such as analysis and reporting.	Non-critical, back-end, off-line business functions. Typically alternate, but less desirable, methods are available to achieve same business function to support tolerance for 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 in specified timeframe (days to weeks).

As an example, let's analyze the four resilience tiers for defining data storage availability. The Platinum resilience tier defines this as access to data that is always available; whereas the Bronze resilience tier classifies this as a best effort to provide access to data in a defined availability window. Depending on what your business resilience requirements are, either level might provide adequate data storage availability; however, the Platinum resilience tier provides a constant level of availability. The recoverability strategy for the Platinum resilience tier reduces return to service to less than five minutes for all events, where as the Bronze resilience tier classifies return to service in less than eight hours for local recovery only, and up to two weeks for the data center. Again, depending on what your business requirements are, either level could provide adequate recoverability; however, the Platinum resilience tier provides the fastest recoverability for your most mission-critical business functions.

Highlights

Understanding the delivery requirements of specific levels of resilience ensures your strategy will provide the optimum amount of resilience.

While many organizations may not need Platinum level resilience, continuous availability is mandatory for some organizations such as core banking operations, space and defense operations, and telecom industries. Understanding the requirements and solutions that enable delivery of specific levels of resilience ensures that your strategy will provide the optimum amount of resilience for your organization. Resilience tiers enable you to selectively invest in priority business resilience needs and to prioritize your needs.

As another example, IBM used resilience tiers to help a major financial services institution redesign their availability architecture. This customer identified the following problems:

- *The application development teams were building and rolling out solutions without structure such as rules, documentation, and evaluation with other teams.*
- *The IT services and support organization lacked an availability and recoverability classification framework for IT service offerings.*
- *The enterprise architecture team did not have a method for defining or assessing the IT architecture domains and service classes.*
- *Across the enterprise, there was no common view of what best practices should guide the development of service classes or resilience tiers.*

Highlights

Using the tiered approach, IBM mapped service level requirements with the existing technology portfolio and identified potential remediation activities.

IBM consultants used the resilience tier approach to help this client establish a common framework to address all of these issues. The consulting team started with an assessment to identify gaps between the installed technology components and the baseline technology characteristics associated with the resilience tiers. IBM consultants conducted interviews to understand the operational environment of these applications, including infrastructure, database, and application components. A representative set of outage scenarios was reviewed and inherent infrastructure pain points were identified. Based on the information received, IBM was able to identify specific gaps in the infrastructure, measured against the baseline technology characteristics, and to assign a relative risk for the availability gaps identified. Using the tiered approach, IBM then mapped service level requirements with the existing technology portfolio. As a result, IBM identified potential remediation activities to close those identified gaps.

The goal of this assessment was to define a set of immediate, tactical actions to improve availability of IT systems. Some of the tactical actions also directly supported the development of a longer term, strategic roadmap of major initiatives that would help the client meet business availability expectations for the in-scope applications; this roadmap included project milestones and high level cost estimates.

As a result of the IBM engagement, the bank's IT organization adopted a framework for classifying and defining resilience tiers for their critical applications. They also initiated a collaborative effort between the Application Development and IT Operations Services leadership (senior executives) to assess the remaining portfolio of critical business applications. This client identified IBM's value propositions as:

- *IBM's resilience tiers were accepted as a best-practice technique for classifying and grouping business applications.*
- *The customer's enterprise architecture team adopted IBM's framework for assessing its portfolio of critical applications.*
- *The customer adopted the resilience tiers for future assessment of availability and recoverability requirements for new business applications. As a result, the resilience tiers became a unification tool for gaining consensus across all IT teams.*

Summary

The tiered approach to resilience can help you plan for intrusive events proactively. This helps you maximize your return on investment from assets, technology and people at the time when you need it most. Using resilience tiers to develop effective long-term strategies ensures that shorter term tactical actions are properly aligned and help your organization progress along the resilience maturity continuum. But keep in mind, you do not need to accomplish this all at once; business resilience is a journey. Investing in proper assessment and design up front will help make sure that your long-term resilience investments preserve value over time.

The IBM Resiliency Consulting team can draw upon our global reach with many years of experience as an asset based business, equipped with specialized tools. We can also draw upon experiences of exposure to companies around the world facing similar issues. So when you need help, IBM is ready to assist. We can help you analyze your organization's requirements, goals, and budget to find out exactly what level of resilience you need. We can help you define a roadmap to get there. We help you prioritize a set of milestones and measurements and a solution designed to improve the resiliency of your business. We help you establish your own best defense using a resilience tiers approach.

For more information

For more information about our business continuity and resiliency consulting services, please contact your IBM representative or visit: **ibm.com**/services/bcrs

Additionally, IBM Global Financing can tailor financing solutions to your specific IT needs. For more information on great rates, flexible payment plans and loans, and asset buyback and disposal, visit: **ibm.com**/financing

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

Produced in the United States of America
January 2009

BUW03008-USEN-00