

Business resilience: Providing targeted resilience solutions for the enterprise

Develop a best-practices resilience strategy using a tiered approach matched to the needs of your business



Contents

- 2 Executive summary
- 2 What is business resilience?
- 3 Are you prepared?
- 3 Key challenges in risk assessment
- 4 Using resilience tiers to define your architectural approach
- 5 Benefits of resilience tiers
- 5 Four levels of resilience
- 7 Providing a more granular, resilience-level analysis of business impact
- 8 Applying resilience tiers to business services
- 9 Summary

Executive summary

Enterprises of all sizes are continually introducing ever more complex technologies into their businesses, not only to drive more growth but also to help manage it soundly. Although new technological solutions, appropriately applied, can be a vehicle to business success, they place a great deal of stress on the mission-critical systems that keep your business working toward its defined objectives. As the number of critical applications—and the technology required to support them—increases, there is a broader set of risks to mitigate, a wider range of exposures through the web and the risk of higher losses in shorter periods of time.

To remain competitive, you cannot afford to be without your mission-critical systems for hours—and sometimes even for minutes. Leaving systems at risk of disruption without being certain of recovery time is therefore not an option. Yet a one-size-fits-all business resiliency solution that provides superfluous availability on noncritical systems can be unnecessarily costly. So how do you provide for the spectrum of business resilience needs across your technology solutions? And further, how do you fulfill those needs in the most cost-effective manner? The answer is to achieve business resilience relative to the needs of your business, matching each business service and its related assets to the appropriate level of resilience that is required to lessen the impact of a disruption to your business. This white paper describes a tiered approach to business resilience and discusses best practices you can utilize in identifying critical resources and developing such a strategy.

What is business resilience?

Business resilience is the ability to rapidly adapt and respond to business disruptions and to maintain continuous business operations, which in turn helps you to build trusted relationships and enable growth. True business resilience starts with understanding exactly what your business needs in order to survive unexpected events and plan ahead for sudden changes that could come at any time. Think of business resilience as your ticket to continued business service and operational continuity with proper planning, readiness and the ability to respond quickly to any threat or opportunity.

Whether an IT- or business-related event or a natural disaster, the challenges you must prepare for are multitudinous. Focusing only on disasters leads organizations to work defensively, but a proactive approach to business resilience helps enable your organization to respond to an unexpected event more quickly and cost-effectively. In addition to outlining responses to

disaster situations, a strong business resilience program can help your organization prepare for audits and manage compliance with regulatory requirements, thus reducing business risk.

Perhaps you already have a disaster recovery plan in place. Is that sufficient? When it comes to data privacy and system outages and your business is on the line, you probably do not want to run the risk of finding out that your disaster recovery plan was not as effective as perceived. 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.

Are you prepared?

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 direct financial impact can ruin your business. The indirect impacts of downtime, such as lost market share, decreased productivity, regulatory noncompliance and loss of reputation are equally damaging. To get an idea as to whether 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 relationships and third-party service providers?
- What are the critical business services and assets that must be protected to reduce or eliminate irrevocable damage?

By identifying potential threats and vulnerabilities, you can design resilience solutions that can prepare you to respond and minimize the impact of disruptive events.

Key challenges in risk assessment

Implementing any resilience program 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 identifying the correct business services and related assets to ensure the right level of protection for all of your critical business assets. In today's cost-constrained economic climate, there is intense internal competition for resources.

Creating the proper investment case is crucial to realizing success.

A major challenge for many organizations is determining which solution is best at providing the optimum amount of protection for the level of investment. 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, and the business stakeholders are involved in the process.

Perhaps the most overlooked challenge in resilience planning is the human factor. Executing projects with teams who are already stretched for time and who may lack skills and methods to identify, categorize and then implement a resilience solution can negatively affect timely execution. Identifying risk and its related impact must become part of daily operations rather than a marathon effort at specified intervals. Embedding risk identification and measurement within the enterprise's processes, and especially in the earliest design cycles, is optimum to ensure resilience solutions are applied for every process, system and asset that demonstrates need.

Key challenges:

- Providing effective, cost-efficient solutions tied to the business need
 - Ensuring the business has the right level of protection based on impact
 - Building proper investment case at a granular level
 - Ensuring resilience across the organization
 - Executing timely and effective analysis, design and implementation with existing work force
 - Ensuring business services and related assets have the right amount of protection
-

Using resilience tiers to define your architectural approach

The most effective resilience planning comes from understanding your situational and organizational needs before a disastrous event occurs. Enabling a standardized approach to business service prioritization and solution selection can greatly speed decision making. New applications are easily placed within the defined resilience tiers. A services impact view of your business, tied to solution selection using resilience tiers, can 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 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
- Presenting technical solutions in business terms

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 nonoperating 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 total availability of a business service, not an availability average of each functional component.

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

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 enterprisewide business resilience
- Consistent criteria when choosing solutions to help ensure new development accounts for resilience requirements in its design and cost case

Traditionally, disaster recovery managers are responsible for the disaster recovery budget, while operation managers have the need to design resiliency into their technical solutions. Resilience tiers help bridge the communications and planning gaps for business continuity resilience and planning. In addition, resilience tiers can help you pursue resilience requirements as an integrated, enterprisewide approach that achieves greater affordability for your organization.

Resilience tiers help rationalize the optimum resilience solutions.

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 nonessential business applications. More important than the labels is that each resilience tier translates into defined metrics categories, such as availability targeted 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				
Service description	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, the business cannot afford to be without this function	Business functions that support back-office functions such as analysis and reporting	Noncritical, back-end, offline 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	Nearly 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 time frame (days to weeks)

Understanding the delivery requirements of specific levels of resilience helps ensure your strategy can provide the optimum amount of resilience.

While many organizations may not need Platinum level resilience, continuous availability is mandatory for some operations, including core banking, space and defense operations and communications industries. Understanding the requirements and solutions that enable delivery of specific levels allows your

strategy to provide the optimum amount of resilience for your organization. Resilience tiers enable you to selectively invest in priority business resilience needs and to prioritize those needs. But how do you know which business resources to assign to which tier?

Providing a more granular, resilience-level analysis of business impact

One of the key challenges companies face today is the ability to accurately assign the right level of protection to each business process and its associated assets. To do this, an organization should leverage the business impact analysis (BIA) to obtain the availability and resilience requirements from the business stakeholders. The problem with traditional BIAs is that the results are compiled for a particular business department or function without consideration of the effect on the service that the organization provides to its customers. The drawback of this functional perspective is that it tends to be centered on the function and often lacks an enterprise view. A resilience BIA identifies the criticality of an organization's services, products and the delivery channels that are used to reach customers. It then assigns these to an associated resilience tier for quicker solution design.

The resilience BIA uses a combination of tangible and intangible analysis techniques to determine and rank impact risks across the organization. Services and products delivered through different channels generate different amounts of revenue and profit to contribute to the financial well-being of an organization.

Therefore, it is important to perform the financial analysis at the services level, touching departments across the organization, to comprehend the impact from outages and interruptions anywhere in the organization and identify the vital resources to protect.

A resilience business impact analysis lets you confidently assign business processes to the right level of protection.

In addition to the financial impact estimation, the business stakeholders should also identify the operational impacts or risks—in other words, the intangible impacts of an outage. Other factors to include are peak periods (worst time to have an outage), existing service level agreements that might indicate the availability or disaster recovery contractual requirements and known legal or regulatory requirements. Considering both tangible and intangible aspects of the company's services provides a more reliable business case to substantiate future investments to protect these critical resources.

The various departments or functional units in an organization use resources to perform work that supports these important services, products and delivery channels. A resilience BIA should also ask department heads or functional owners to estimate impacts. The financial and intangible impacts from the functional units' viewpoint can then be cross checked with the impacts collected from the business stakeholders in order to

confirm and gain consensus on the aggregated financial and intangible risks, and to establish the preliminary recovery priority order. In addition, the availability and disaster recovery requirements from the functional perspective are verified with those from the business stakeholders to ensure the availability and recovery requirements are in synch. This process institutes a cross validation of impact data that increases the accuracy and confidence in the final outcome.

It is important to engage the business stakeholders to obtain the business impact information from the services, products and delivery channels viewpoint. Involving the business stakeholders increases awareness and support of the outcome. It also ensures a broader, enterprisewide view that helps rank the services, products and delivery channels according to criticality and then aligns them with the resilience tiers.

Once the combined impacts are understood, the outage tolerance window is determined based on a solid understanding of the financial and operational risks the organization is willing to accept before sustaining irreparable harm. Regardless of whether the outage was a result of unavailable technology, inability to access facilities, natural disaster or lack of available resources, the resilience BIA seeks the operational outage tolerance information. With this information you can confidently assign service, product and delivery channels to a resilience tier where the initial set of technical availability and recovery characteristics are defined to match the business needs instead of being driven by technology capabilities.

A business-oriented analysis of outage tolerance and impact can help you:

- 1. Enable quicker solution development**
 - 2. Include protection for new development by integrating resilience tiers with development life cycle**
 - 3. Help improve accuracy by instituting cross validation of impact data**
 - 4. Produce a more reliable business case for seeking investments**
 - 5. Increase awareness and business support by involving business stakeholders at all levels**
 - 6. Drive solutions by business need rather than by technological capability**
-

Applying resilience tiers to business services

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 levels of service. Using this objective, quantitative approach as part of the nonfunctional requirements definition and prioritization can help ensure that the resilience objectives

and acceptable costs are integral to the overall service quality. In addition, the cost and time to design resilience into new applications is much cheaper as opposed to retrofitting resilience into a production environment that is experiencing operational outages.

You 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 with a single, target architecture. Resilience tiers can help reconcile business resilience requirements and guide the infrastructure requirements, architectural design decisions and major initiatives that are implemented to achieve the future-state resilient IT environment.

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 addresses all infrastructure components, including storage, networking and load balancing, and that can scale to address a range of business 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.

Summary

The tiered approach to resilience teamed with the resilience BIA can help you prepare for intrusive events proactively. This combined approach helps you increase your return on investment of assets, technology and people at the time when you need it most. Using resilience tiers to develop effective long-term strategies can ensure 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 analysis up front and detailed architectural design to match the tiers will help make sure that your long-term resilience investments preserve value over time.

IBM's resiliency consulting team draws upon the company's global reach with many years of experience as an asset-based business, equipped with specialized tools and methodologies. We can also draw upon experiences with 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 road map to get there. And we can help you prioritize a set of milestones and measurements and a solution designed to improve the resiliency of your business, so you can establish your own best defense using a resilience tiers approach.

For more information

To learn more about IBM Business Continuity and Resiliency Services, please contact your IBM marketing representative or IBM Business Partner, or visit the following website:

ibm.com/services/continuity

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit:

ibm.com/financing



© Copyright IBM Corporation 2011

Produced in the United States of America
May 2011
All Rights Reserved

IBM, the IBM logo and ibm.com, are trademarks of International Business Machines Corporation in the United States, other countries or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

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



Please Recycle
