Risk mitigation for business resilience
White paper

A comprehensive, best-practices approach to business resilience and risk mitigation.

September 2007

IBM Governance and Risk Management
Business alignment, visibility and control

Contents

Overview: Why traditional risk mitigation plans fail

A successful governance and risk mitigation strategy must operate at multiple levels with broad coverage. Risk mitigation plans at many organizations fall short simply because they are not comprehensive and fail to take into account the reach and range of all the risks that they actually face. Often this occurs when organizations only focus on specific areas of risk categories, only plan for certain types of risk or don't understand all the different areas in their organization that particular risks will impact. For example, in the area of disaster recovery, most plans fail to account for the following areas of concern:

- **Human issues** — Plans are often inadequate for ensuring communication with, support for and mobilization of employees, decision makers, suppliers and customers, as well as providing the means to protect families.
- **Infrastructure issues** — How will the organization deal with prolonged power failures, travel and transportation restrictions and logistics disruptions? Are there adequate fuel supplies? Are resources such as generators staged in safe locations?
- **Business issues** — The traditional view of disaster recovery has primarily been focused on data and the IT infrastructure, but many of the impacts of a disaster are business-related issues that affect people, business processes, facilities, transportation, communications and regulatory compliance.
- **Community issues** — Organizations must not neglect their responsibility to help employees and their local communities and regions recover from major disasters.

This white paper discusses common types of risk, the considerations for each and the steps organizations must take to develop an effective risk mitigation strategy.

Highlights

Organizations need to take a comprehensive and methodical approach to risk mitigation to ensure their business continuity and livelihood

Build a comprehensive strategy for risk mitigation

Whether it's to mitigate risks associated with a major disaster, or more common risks in the areas of business operations or data availability, organizations need to take a comprehensive and methodical approach to risk mitigation to ensure their business continuity and livelihood. Such an approach needs to evaluate and address the priorities and capabilities of the business along three risk mitigation dimensions:

- **Risk reach and range** — Understanding the risks that an organization has and the impacts, or reach and range, of those risks both inside and outside the company.
- **Resilience framework** — What is the resilience of the current environment to mitigate the identified risks? What are the organization's specific areas of vulnerability and what capabilities does it currently have to predict, prevent and recover from risks?
- **Resilience strategy** — What is the appropriate strategy to respond to the organization's risks? What is necessary to improve the resilience of the current environment and achieve the desired state of resilience?

Identifying types of risk

The first step in developing a comprehensive risk mitigation plan is to identify the types of risk an organization might have that impact business resilience. They include:

- Business-driven risks.
- Data-driven risks.
- Event-driven risks.

Business-driven risk

Business-driven risks impact business continuity and business operations. They are generally more strategic in nature, with business-wide ramifications that an organization's board members would typically be most concerned about: the compliance, governance, availability, security, performance and integrity of critical business services. Business-driven risk includes the ability to protect the business and keep it accessible whenever and from wherever in support of continuous business operations as well as compliance with industry and government regulations.

Data-driven risk

At an IT level, data-driven risks often receive the most attention. These risks have some crossover with business-driven risk in terms of business continuity and business availability, but their focus is at the system or data level. What infrastructure, processes, people and systems does an organization need in order to keep data and information accessible for business operations, compliance audits and legal requests? How does it back up and quickly retrieve critical data and information whenever and wherever it is needed? How does it protect that data against viruses, worms, theft and loss? How can the organization make sure data is reliable, authentic and continuously available? Even though data-driven risks are often a primary concern of IT organizations, they are not exclusive to IT data. Data-driven risks deal with the availability of data and information in all of its different forms as used by the organization, including paper-based data.

"According to the U.S. National Archives and Records Administration, 25% of the companies that experienced an IT outage of two to six days went bankrupt immediately."

— The Economist Intelligence Unit 2007, ***Business resilience: Ensuring continuity in a volatile environment***

Event-driven risk

Any event that disrupts an organization's workforce, processes, applications, data or infrastructure can be classified as an event-driven risk. This category focuses on actual events that create risk to business continuity and viability, such as natural disasters, pandemics, fires, thefts and even IT attacks.
To mitigate these risks, organizations create disaster recovery and crisis management plans to ensure that they have the people, networks, IT services, facilities and whatever else is needed to meet the recovery objectives of the business. The ability to mitigate event-driven risks is often contingent on the ability to distribute operations beyond the area of immediate impact of the identified risk.

Risk reach and range: understanding risk and its impacts

Reach and range describe the different ways a risk can potentially affect the enterprise, such as information accessibility, communication flow, ongoing operations and workflow interactions. By defining the reach and range of a risk, an organization can better determine where it should place its attention with regard to that risk. This involves analyzing how far a risk potentially extends within and beyond the enterprise. It requires an accurate understanding of how much of the enterprise's business operations and value chain will be impacted by a given event.

Not adequately understanding the reach and range of particular risks is one of the primary reasons that organizations fail to successfully mitigate risk. Too often a company sees itself as an island, not taking into account the role of its supply chain or value net in its everyday processes. For instance, a company's vulnerability to risk rises in proportion to its partners' vulnerabilities and exposures. Production lines come to a halt when suppliers are unable to fill orders. Business operations that depend on external data feeds and inputs cease if those sources become unavailable.

Highlights

By properly identifying the reach and range of a risk, organizations put themselves in a better position to apply the appropriate level of attention to that risk

Reach and range also apply to the opposite end of the spectrum – organizations shouldn't overemphasize certain risks. It's a waste of resources and effort to plan a massive response to a risk that is localized. For example, a department within an organization might be at risk when it only has one employee that knows how to perform a key process. This is a localized risk that can be mitigated by cross-training another employee. By properly identifying the reach and range of a risk, organizations put themselves in a better position to apply the appropriate level of attention to that risk.

The following represents a practical categorization of the different levels of impact and interaction that organizations should look at when determining the reach and range of a risk:

- **Business systems** — Single business systems or applications
- **Business processes** — Both technology-driven and nontechnology-driven aspects of a business process
- **Business units** — Business processes within a discrete line of business or business unit within the enterprise
- **Enterprise** — Enterprise-wide infrastructure, people and business support operations
- **Extended enterprise** — Entities or services outside the enterprise that must be functioning in order for the business to run, such as supply chain, business partners and external service providers

Relating value to risk: quantifying impact

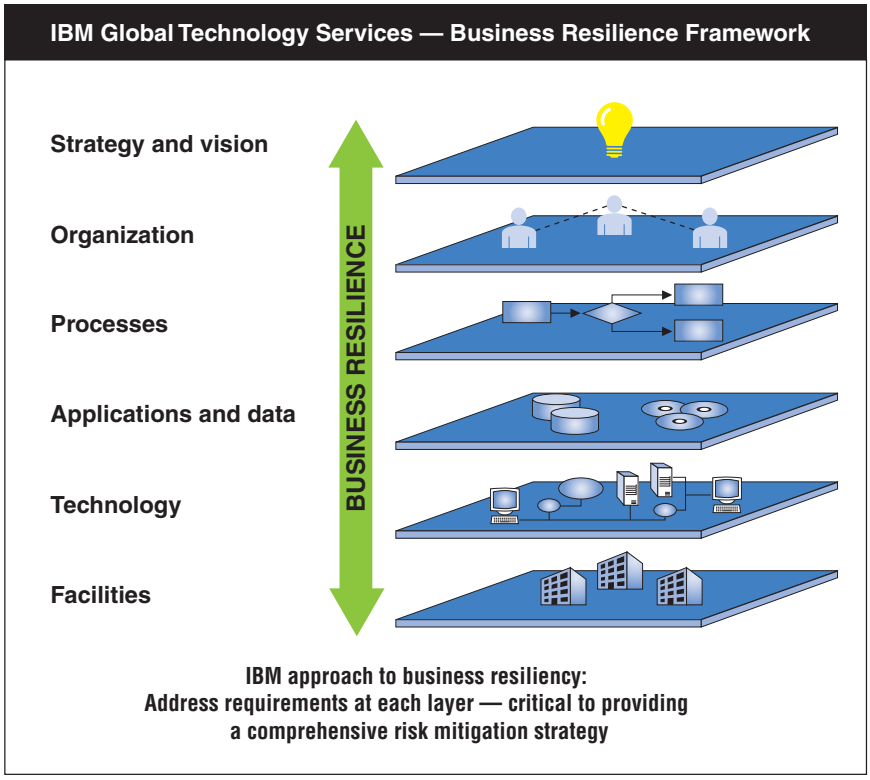
Additionally, to be able to put the most appropriate emphasis on a risk, organizations should establish the value associated with being resilient to that risk by quantifying its impact or opportunity costs. Quantifying risk impact begins with defining what business capability could be affected by that risk and describing the impact to the business or supporting infrastructure. This requires an understanding of the relevant supporting business processes.

The next step involves defining an appropriate metric to objectively measure the impact. Using this metric, the organization can then calculate the

"As they take steps to increase the efficiency of their supply chain, companies have become dependent on a highly complex network of suppliers and partners. Over time, they have also consolidated their supplier base, so that they are more reliant than ever on the ability of those companies to deliver on their promises."

— The Economist Intelligence Unit 2007, ***Business resilience: Ensuring continuity in a volatile environment***

economic benefit or loss derived directly or indirectly from that capability. In addition to the quantifiable economic benefit or loss provided, an organization needs to look at noneconomic factors associated with a capability, such as its strategic value to the enterprise.



IBM Resilience Maturity Asset Framework: Identifies areas of vulnerability at each layer of the business.

Resilience frameworks: analyzing current risk environments

Once an organization understands the reach and range of the risks to its enterprise, it needs to evaluate its current ability to mitigate those risks. Due to the inherent complexity of most organizations, such an analysis should

break down the different aspects of the organization into multiple layers that can each be viewed separately to see how they can be used to mitigate certain risks. To help with this analysis, IBM has developed the IBM Resilience Maturity Assessment Framework, which deconstructs a client environment into six layers that include strategy, organization, processes, technology, applications and data, and facilities.

Within each layer is a set of objects with specific attributes that should be analyzed against industry-standard frameworks such as the IT Infrastructure Library® (ITIL®) framework, Control Objectives for Information and related Technology (COBIT), Six Sigma, BS25999, Basel II and the ISO 9000 series. Organizations can utilize the frameworks that are most applicable to the risks that they face to create a comprehensive resilience framework.

Resilience strategy: designing a blueprint for risk mitigation

An analysis of the different risks within each framework layer helps an organization understand the current state of its environment, enabling it to move on to the next step: determining what the future state of its environment needs to look like in order to mitigate its identified risks and creating an appropriate strategy to reach that state. It is important to leverage the risks and capability information to map out a resilience enterprise blueprint of the organization's desired state and how to reach it. This blueprint becomes the strategy for creating a resilient business enterprise.

Just as the framework analysis is based on industry standards, the creation of the risk mitigation strategy – or resilience enterprise blueprint – should also leverage industry-standard best practices in risk mitigation. For example, risk mitigation plans for the strategy and vision layer might require a clearly

Highlights

IBM provides objective, industry-specific analysis of its clients' business resiliency and exposure to risks, including proven tools and methods for developing a comprehensive, dynamic risk mitigation strategy

articulated governance model and security policy for the enterprise. The processes layer might call for the implementation of ITIL and COBIT standards. At the application and data layer, one strategy might be to leverage a service oriented architecture (SOA).

An effective blueprint is actually comprised of multiple layers of resilience strategies, all based on best-practices guidelines and processes. Where appropriate, these different strategies should work together to successfully address the reach and range of the different risks within the framework layers.

Achieve optimum business resilience with IBM

Backed by more than 154 global resiliency centers around the world and its team of 1,300 experienced business continuity professionals, IBM provides objective, industry-specific analysis of its clients' business resiliency and exposure to risks, including proven tools and methods for developing a comprehensive, dynamic risk mitigation strategy, such as:

IBM Resilience Enterprise Blueprint (REB) – a structured methodology for understanding the specific risks a client may face and determining a strategy for mitigating those risks based on the state of the current environment and the desired future state. It provides the linkage between the components or objects that comprise a client environment to comprehensively address risk and create an overall blueprint for achieving resilience.

IBM Resiliency Maturity Assessment Framework (RMAF) – an object-oriented framework used by the REB that defines the components of a business environment and their resilience attributes to promote understanding of potential problems. Layers examined in the RMAF include:

- Strategy and vision.
- Organization.
- Processes.
- Applications and data.
- Technology.
- Facilities.

Resiliency Maturity Index (RMI) – an index developed by IBM researchers to assess the end-to-end organizational resilience and quantitatively compute the resiliency score of the organization. This index helps executives understand how varying the resiliency of different components impacts the overall resiliency of the organization.

IBM Business Continuity and Resiliency Services (BCRS) – IBM BCRS experts can assist in building a robust business continuity solution, from assessment, planning and design through testing, implementation and management. IBM offers an integrated set of service products designed to help organizations identify risks and vulnerabilities; evaluate plans, processes, procedures, roles and responsibilities for the continuity program; map IT to critical business processes; implement and design a business continuity plan and processes; evaluate response capabilities based on specific scenarios; and provide management of the resilience program – including reporting – so organizations can continue operating under virtually any circumstance.

Look to a market leader in business resilience

As a market leader in business resilience, IBM solutions draw from 40 years of business resilience experience to offer a comprehensive, integrated portfolio of solutions that can be tailored to virtually any organization's business continuity, resilience and risk and compliance needs. IBM business resilience solutions enable organizations to respond locally, regionally or globally to opportunities, threats, regulatory pressures and lawsuits – to help protect their brand, defend their business, maintain customer and partner relationships, and position them for growth, while optimizing their use of budget and resources.

For more information

To learn more about IBM business resilience and risk mitigation services and solutions, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/itsolutions/riskmanagement

About IBM solutions for enabling IT governance and risk management

IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards–based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit **ibm.com**/itsolutions/governance

IBM Corporation
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
9-07

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

GMW14000-USEN-00