



Reduce risk in business acquisitions and consolidation by better managing IT and infrastructure dependencies.



Brian G. Barnier
IBM Business Resilience — Governance, Risk and Compliance Leader
203-486-4263

March 2008

Contents

- 2 Overview**
- 3 Deal with “planned” business change from all quarters**
 - 4 *Overcoming the challenges of business change for IT and infrastructure risk management***
- 5 Be proactive in leveraging best practices**
 - 6 *Key success factors in reducing acquisition risk through IT and infrastructure***
 - 7 *Fuse IT and business objectives for greater effectiveness***
- 8 Benefit from IBM insight and a broad range of resilience solutions**
- 10 Conclusion**
- 10 For more information**
- 11 About IBM Service Management**

Overview

While some business change is unplanned (that is, dramatic changes in market condition or natural disasters), other change is planned. Some of the riskiest “planned” changes include acquisition, expansion, consolidation or new product launches. These changes have a far-reaching impact on an organization – including its IT and infrastructure. And, inevitably, this impact commands attention at the top of the business, as CFOs and other senior executives make commitments to “the street” and customers about what their IT and infrastructure will be able to achieve – and how quickly.

Such commitments can be intimidating to even the savviest IT organization – yet they also represent a great opportunity. The IT and infrastructure team plays a dual role in such business change situations, acting to both reduce risk in IT, as well as a way to use IT to reduce operational risk in other areas of the organization.

Managing risk through resilience requires a new, more expansive way of thinking and acting in order to address a wide range of threats to multiple business assets and resources. The good news for IT professionals is that by proactively managing IT and infrastructure risk in the context of specific business initiatives, they can help build a more resilient enterprise that can spring into action to take advantage of market opportunities.

Deal with “planned” business change from all quarters

While much discussion of risk management and resilience has focused on external, “event-driven” risks, “planned” business changes are typically more common and can have equally serious financial consequences if not managed well. This type of change includes:

- **Acquisition, consolidation, globalization and expansion**
 - Drive significant IT platform change.
 - Place stress on IT and the infrastructure.
 - Execute under fast timelines, creating pressure (thus raising the potential for error and loss).
 - Are often highly visible to external parties of interest, such as financial investors.

- **Changes in board policy or senior management** drive new priorities, including:
 - New governance processes.
 - More emphasis on effective risk management.
 - New requirements to demonstrate compliance.

- **Major new customers and supply chain requirements** can impose new contractual requirements to reduce risk (especially relating to time-sensitive and quality issues), so that risks don't ripple through tightly coupled supply chains.

Highlights

Risk management failures can hurt share price, market value, revenue, expense, differentiation and customer satisfaction

- **Technology changes** can introduce risk from the project as well as from the change in management approach or actual platform. Such technology changes can encompass:
 - Technology management such as shared services and data center consolidation.
 - Conversion from manual to more automated methods.
 - Virtualization efforts.
 - The increasingly mission-critical role of mobile devices and Web tools.
 - Green initiatives.

Dealing effectively with change from all these quarters is critical, because risk management failures can hurt share price, market value, revenue, expense, differentiation and customer satisfaction. In addition, the success (or failure) of a resilience strategy is very visible to senior business leaders, as well as the CIO and staff, IT relationship managers and IT functional leaders.

Overcoming the challenges of business change for IT and infrastructure risk management

The challenges for IT and infrastructure teams posed by business change include:

- Dealing with business issues from above (what we might call formal dependencies).
- IT's own change dynamics resulting from efforts to rationalize and streamline (for example, data center consolidation, shared services, virtualization, grid).
- The introduction of new technologies to address business issues (such as mobility, collaboration, SOA and green initiatives).

Highlights

In addition, the human side of maintaining resilience after change such as an acquisition occurs must be considered. This is often overlooked, but what's the point of recovering data if no one can physically or virtually get to it? When a facility is selected for closure, how much consideration is given to accessibility in the event of various threats? Obviously, capabilities such as work area recovery must be a key component of a resilience strategy.

In working through these challenges, the IT leader must recognize that he or she is in a key leadership position. The dependencies of a business activity, process or application are often not visible to the business owner or the general risk manager. It is the IT person who has the business service management tools, IT service models and other tools – and who is aware of the extent to which the business depends on resilience in IT and infrastructure.

Risk can be managed more effectively through the creation of a common risk assessment vision for IT leaders, business owners and risk managers

Risk can be managed more effectively through the creation of a common risk assessment vision for IT leaders, business owners and risk managers. With this risk-based view in hand, the IT and business risk partners can recommend an action plan that analyzes risk in financial terms meaningful to the CFO, other senior executives and investors. This view will both protect value against loss and create value through improved resilience.

Be proactive in leveraging best practices

Building a unified approach to risk assessment requires, first of all, a view of all the threats to IT and infrastructure that can undermine a given business activity. Sometimes, the “little things” are less noticeable at first, but turn into huge losses. Operational stability problems are prime examples. Availability, release, configuration and capacity can all cause significant losses. Secondly, a unified approach requires a common language for risk management. Both of

Highlights

these objectives can be met through a reliance on open standards. As a bonus, you gain the collective wisdom of others who have created and used these standards and practices.

From a cross-industry perspective, the leading IT and infrastructure risk standards are provided by the IT Governance Institute:

- Control Objectives for Information and related Technology (COBIT®) focuses on the control of technology and supporting infrastructure.
- Val IT™ deals with the value creation aspect of IT to meet business needs.
- A useful supporting standard is IT Infrastructure Library® (ITIL®), which specifies process flows for activities such as change, release and problem management.

Key success factors in reducing acquisition risk through IT and infrastructure

Adopting a more structured, unified and comprehensive approach to risk management and resilience is critical. However, to attain a higher level of effectiveness in risk management, the organization must also:

- Become more *aware* of the range of potential IT and infrastructure threats to business objectives. Note that this must be a proactive awareness.
- Improve the *ability, effectiveness and efficiency* in identifying, planning for, monitoring, analyzing and responding to these threats.

For successful IT and infrastructure risk management during business change, potential threats to the business need to be more visible and then easier and less costly to respond to

The key to the success of IT and infrastructure risk management during business change is an ability to make potential threats to the business more visible and then make it easier and less costly to respond to them. This can be accomplished by working with the dynamics of three important components of the enterprise: people, organization and automation.

- People: It's important to engender a "risk-aware" culture in which people are aware of the range of potential threat types and are able to respond to such risks.
- Organization: People must be given the structure and tools to be able to respond to risks effectively. This requires strategic integration of a clear governance process. It is necessary to review the various governance styles and select the one that is right for a particular enterprise.
- Automation: The proper automation tools can facilitate the risk management process, as well as monitoring/sensing, responding to system condition and reducing risk in core hardware and software capabilities. These are critical for lowering the cost of the risk management process and making it easier to actually reduce risk.

Fuse IT and business objectives for greater effectiveness

A business change initiative is generally undertaken on a fast-paced, compressed time schedule. To avoid slipups, business process owners and their IT partners must be closely "fused." When IT professionals maintain a focus on business impact and issues, they can effectively position IT as the key player in the resilience solution – and not part of the problem. Enabling a more meaningful business and IT conversation makes it easier for IT professionals to sell their ideas to their business-side colleagues and business funding sources. Through a risk-aware approach, IT leaders can more easily drive alignment with business process owners, through the common language of risk.

Highlights

IBM proactively helps enterprises become more resilient by offering multiple solutions and products related to business resilience and a full life cycle of services

Benefit from IBM insight and a broad range of resilience solutions

As a leading participant in industry open standards, as well as a sponsor and direct participant in standards-writing committees, IBM proactively helps enterprises become more resilient. IBM offers multiple solutions and products related to business resilience, as well as a full life cycle of services that encompass analysis, planning, design, implementation and ongoing management. The company's commitment to identifying the root causes of risks and creating enhanced resilience for its clients has been made unquestionable by its establishment of more than 150 global resilience centers with multivendor environments that support more than 200 hardware and software vendors.

By taking a holistic view of the range of risks to the continuity of business activities, **IBM Resilient Enterprise Blueprint (REB)** provides superior analysis of business process dependencies in IT. REB works in three stages to uncover the root causes of IT risks to business activity and provide specific prescriptive guidance to reduce those risks:

- *Diagnoses* risks to IT against a desired service level for a business activity, based on both process and outcome control evaluation.
- *Prioritizes* actions based on risk likelihood and potential impact on a business activity's service level.
- *Identifies* detailed steps to take to reduce risk.

IBM also provides **advanced software technologies** (for important resilience-related functions such as monitoring, control, mirroring, replication, automated backup and more) that can play a key role in an organization's resilience and continuity efforts. A few examples include:

- **IBM Tivoli® Business Service Manager** helps visualize the health of critical business services and associated service level agreements (SLAs), and enables IT to target resources and actions to the most critical and costly IT resources and issues — ultimately delivering a greater impact to the business.
- **IBM Tivoli Storage Manager family** provides centralized, automated data protection that can help reduce the risks associated with data loss while helping to manage costs, reduce complexity and address compliance with regulatory data retention requirements. Products store backup, archive, manage space and restore bare metal, compliance and disaster-recovery data in a hierarchy of offline storage.
- **IBM Tivoli System Automation family** provides high-availability, enterprise-wide automation across a range of platforms — enabling a single point of control and management for critical applications and IT services that span Linux®, IBM AIX®, Microsoft® Windows®, Sun Solaris and IBM z/OS®.
- **IBM Tivoli Workload Automation family** supports initiatives to help IT respond to change with greater flexibility, optimize availability and service delivery, and help control costs by maximizing resource utilization.

Conclusion

An enterprise's IT leaders are in a key position to help reduce IT and infrastructure risk introduced by such initiatives as acquisition, consolidation, expansion and new products. At the same time, they are in a position to use IT to reduce the business risks themselves. Because of its broad view of the IT operating environment, its approach to resilience and service management, and its involvement in the creation of open standards, IBM has developed unique insights into IT and infrastructure risk. These insights permeate the IBM solutions that help clients both plan for and implement such business change initiatives.

For more information

To learn more about how IBM solutions for business resilience can help organizations effectively absorb unrelenting business change – or to find the right IBM solutions entry point that is right for your organization – contact your IBM representative or IBM Business Partner, or visit ibm.com/itsolutions/businesscontinuity

For more information, please contact Brian Barnier, Global Business Resilience Consulting, at bbarnier@us.ibm.com

About IBM Service Management

IBM Service Management helps organizations deliver quality service that is effectively managed, continuous and secure for users, customers and partners. Organizations of every size can leverage IBM services, software and hardware to plan, execute and manage initiatives for service and asset management, security and business resilience. Flexible, modular offerings span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards-based technology. IBM acts as a strategic partner to help customers implement the right solutions to achieve rapid business results and accelerate business growth.



© Copyright IBM Corporation 2008

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

Produced in the United States of America
March 2008
All Rights Reserved

AIX, IBM, the IBM logo, Tivoli, Visibility. Control. Automation, and z/OS are trademarks of International Business Machines Corporation in the United States, other countries or both.

COBIT and Val IT are trademarks of the IT Governance Institute.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Linux is a trademark of Linus Torvalds in the United States, other countries or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

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.