



**Protect critical information with
a smart information-based-risk
management strategy.**

Contents

- 2 *Executive overview***
- 3 *Finding and using information that drives business success***
- 5 *Managing the dynamic nature of information***
- 7 *Overcoming the challenges associated with managing information-based risk***
- 8 *The keys to successful information-based-risk management***
- 12 *Conclusion***

Executive overview

As the business world becomes more global and interconnected, information-based risk grows. Having larger, more remote workforces results in a greater number of access points—at multiple facilities, at home offices and through mobile devices such as laptops and personal digital assistants. An expanding volume of data is available online for partners, suppliers, customers and the general public. The systems and processes that support information storage and flow are becoming more complex. These modern variables make it even more critical for organizations to protect their information, to a greater degree than ever before. Any event that disrupts the flow of information can put an organization at risk, whether the disruption originates with the organization’s systems, processes, human resources or facilities, or external sources such as partners, suppliers, vendors or industry utilities. Compromised data can expose organizations to regulatory fines or legal actions. Unauthorized access to intellectual capital can cut into a company’s competitive advantage. Security breaches can undermine customer confidence. System downtime that limits access to data can stifle productivity.

In this business climate, organizations that want to thrive must implement a focused strategy to control information-based risk. Every organization must be able to protect its information assets, as well as the systems, processes and human resources that support and use the information.

This white paper outlines four components—continuity, recovery, availability and security—that should play a part in any strategy for managing information-based risk. It recommends a systematic approach to helping you protect your critical information assets while providing a more flexible and strategic foundation for addressing business challenges.

Highlights

Information is the linchpin in every business decision and every transaction.

Organizations must identify the data that yields useful information and must understand why it is important to the business.

Finding and using information that drives business success

Never before has information played a more important role in organizations' success. Information is the linchpin in every business decision and every transaction. Businesses rely on timely, accurate information to make major decisions – and to recognize and take advantage of business opportunities when they appear. They need it to communicate with customers and to enable collaboration both internally and externally. Information provides the inspiration and the justification for high-impact innovation. There are, in fact, entire business models built on the creation, exchange, distribution, storage and management of information. It is clear that information, and its protection, should not be treated lightly in any organization.

To use information effectively in their operations, organizations must identify the data that yields useful information and must understand why it is important to the business. Furthermore, the organization must know how to transform different types of business-critical data into information, and then into shared institutional knowledge.

Consider the different forms that information can take. Information at its most basic level is in the form of raw data – ones and zeros in a computer; documents in file cabinets; fax transmissions. Data can come from a variety of sources and can exist in a wide range of formats, such as an employee's handwritten notes, an e-mail message, a customer relationship management (CRM) database, and photographs or drawings that have been scanned into electronic files. This disparate, raw data remains relatively useless and insignificant until it is compiled, interpreted and transformed into relevant information.

Highlights

If handled correctly, an organization's knowledge base can be used systematically for decision-making activities that directly influence business performance.

Information must be managed proactively—with heightened awareness of the associated risks.

Coherent, ordered groups of information can contribute to the organization's collective knowledge base. If handled correctly, the knowledge base can be used systematically for decision-making activities that directly influence business performance. Many of these activities are performed by employees, but it is not only the organization's human resources that interpret data and put it to use: Computerized decision-support systems can facilitate advanced decision making by using a combination of explicit, programmed knowledge and heuristics. These systems can often account for a larger number of variables than humans do—from environmental concerns and market conditions to interpersonal dynamics and collective past experience.

Whether it is a human element or an advanced business intelligence engine that employs the data, the resulting information must be managed proactively—with heightened awareness of the associated risks. Organizations must put strict controls in place to manage and protect this vital corporate asset. Information-based-risk management must take into account not only the data itself, but also the ancillary components that support and make use of the information for decision making. These components include the systems, processes and resources needed to create, capture, store, integrate, access, analyze and distribute information. Only after all these areas are addressed can an organization actively enable an uninterrupted flow of information across the business.

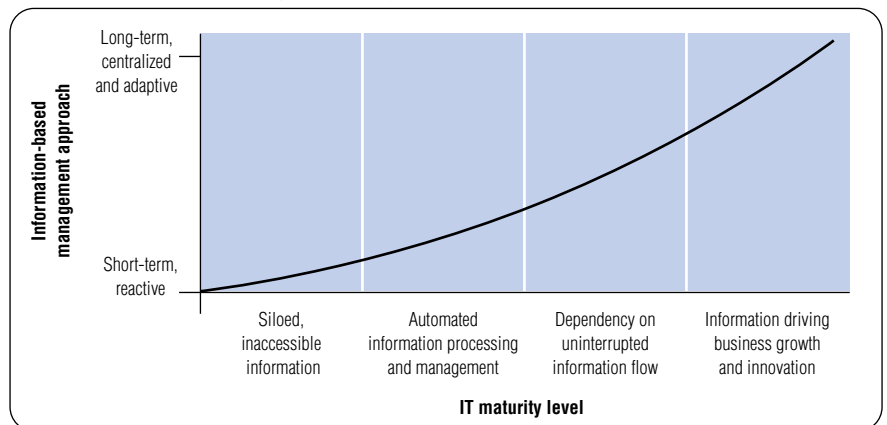
Highlights

Real-time, integrated, Web-based systems provide virtually immediate, worldwide access to critical information.

Managing the dynamic nature of information

Information can no longer be considered a static element of the business. Organizations are using real-time, integrated, Web-based systems that draw data directly from a variety of sources to gain virtually immediate, worldwide access to the information that is critical to the task at hand. With the introduction of remote access and myriad mobile devices, employees now have 24x7 access to the data they need. Organizations can also share data more easily with external entities, such as partners, suppliers and customers. Furthermore, automation, data warehouses and business intelligence systems make it easier and faster to access and interpret the vast stores of data that today's organizations now maintain.

Greater IT capabilities require higher levels of risk-management



As information becomes more dynamic and pervasive, organizations need to adopt increasingly proactive approaches to managing information-based risk.

The evolution of information-risk-management strategies in relation to IT capabilities As organizations employ increasingly sophisticated methods for accessing and leveraging information, they typically find themselves requiring more holistic, proactive approaches to mitigating information-based risk. At a low maturity level, organizations may not yet use their stores of information effectively.

Highlights

Automation can enable real-time, online access to data, but it can also introduce a new level of complexity in the IT environment.

Data is sometimes stored in separate silos, and can be difficult to access and synthesize. If organizations decide to adopt information-based-risk-management capabilities at this stage, they typically target one area at a time, and focus on simplifying processes and increasing productivity.

This early approach to protecting the IT infrastructure is characteristically reactive, consisting of limited-scope technology solutions that address targeted problem areas, such as accounting or payroll. While the solution may mitigate information-based risks temporarily, it inevitably becomes obsolete as a result of changes in business conditions and in the IT infrastructure. At this level of maturity, an organization lacks a holistic, long-term view of information-based-risk management – and will eventually have to revise its approach.

At the second level of maturity, organizations begin to automate information processing and management. Automation can enable real-time, online access to critical data, but it can also introduce a new level of complexity in the IT environment. Organizations often find it critical to centralize data, integrate systems enterprisewide and introduce point-in-time recovery capabilities to reduce business disruption in the event of an outage. In this stage, the emphasis shifts from point problems to long-term organizational productivity and continuity.

Farther along on the maturity scale, organizations are facing stringent business demands for greater accessibility and availability. At this point, every aspect of their operations depends on the continuous flow of information – and they can't afford disruptions. Organizations at this level of maturity quickly learn that it's necessary to take a pragmatic approach to business-continuity planning.

Highlights

Organizations should strive for a future state in which centralized, adaptive systems monitor information flow around the clock.

An information-based-risk management strategy must be compatible with the business strategy and with corporate governance and crisis-management programs.

Striving to protect both the IT infrastructure and the interests of the business, they develop continuity and recovery plans that can minimize downtime in a wide range of situations, whether they are related to natural disasters, power outages, system failures or human resources churn.

The final stage of the maturity curve represents a future state in which centralized, adaptive systems monitor information flow around the clock to ensure strict alignment with business requirements. Organizations in this stage need detailed knowledge of every essential piece of the organization, from business functions and processes to applications, technology platforms and supporting resources. Critical components must be identified, documented and monitored to give organizations a full understanding of the potential impact of an event. Aggregating business and IT requirements in this way can enable transparent operations that make it easier to deliver products and services smoothly—to both end users and external parties.

Overcoming the challenges associated with managing information-based risk

Developing a strategy for managing information-based risk can be a difficult task. The risk-management strategy not only must address the data, IT systems, processes and human resources involved, it must be compatible with the company's overarching business strategy, corporate governance framework and crisis-management procedures. The strategy should help facilitate the following:

- *Managing regulatory compliance requirements*
- *Integration with security policies*
- *Data synchronization among systems*
- *Integration across the supply chain, including with vendors, distributors, partners, suppliers and customers*

Highlights

- *Flexibility to adapt to changing business conditions and emerging threats*
- *Reporting capabilities to enable ongoing adjustments in risk-management priorities*
- *A system of checks and balances among business units*

IT complexity can make it difficult to manage and control information flow across the enterprise.

Technology plays a key role, as well. Given the relentless pace of technological advancement, organizations are facing expanding, multiplatform IT environments. Though continuing advances can deliver significant improvements in information access and system performance, they can also increase complexity and drive up management requirements. This complexity can make it difficult to synchronize data, facilitate physical security, efficiently utilize capacity and live up to service level agreements. The challenge of managing and controlling information flow can increase exponentially as the ability to access and distribute information extends farther across and beyond the organization.

The keys to successful information-based-risk management

An effective program for managing information-based risk should be multifaceted, covering four basic areas: continuity, availability, recovery and security.

With so many factors contributing to the flow of information across the organization, it is important to take a comprehensive and systematic approach to managing risk. An effective program for managing information-based risk should be multifaceted, covering four basic areas: continuity, availability, recovery and security. When combined with a consistent focus on addressing and managing information-based risk, efforts in these four areas can help enable greater availability of information and access to critical business processes – while enhancing the resilience of the IT environment across the enterprise.

Highlights

A detailed analysis of the organization can help identify complex relationships and interdependencies that support information flow.

Organizations should link availability plans to business continuity efforts—and prioritize them using the same set of principles and assumptions.

Continuity

Creating a continuity plan requires an identification of the processes and information that are most important in sustaining business operations. Organizations should start by performing a detailed analysis of business functions, mapping business-critical activities and their supporting systems, processes, data and resources to get a comprehensive view of the enterprise. Doing so can help enable the organization to identify not only key elements, but also complex relationships and interdependencies woven throughout the infrastructure and the human resources hierarchy. During analysis and planning sessions, organizations should assign levels of importance to applications and information, based on the business impact of losing them. These components should then be linked to business functions, so basic IT activities can be oriented toward supporting business continuity. After assessing the IT environment, organizations may find it useful to strive for improvements in incident management, technology upgrades, application development cycles or the ability to accomplish mergers or acquisitions quickly.

Availability

Without an IT infrastructure that provides the required levels of availability, business continuity plans will likely have limited effectiveness. That is why it is so important to link availability plans to business continuity efforts—and prioritize them using the same set of principles and assumptions about the relative criticality of processes and information. This parallel approach for continuity and availability plans can help organizations protect high-priority business functions by adding redundancy and resiliency to the network and systems where needed.

A detailed high-availability strategy provides the actual delivery mechanism for helping enable critical information to be accessible on a 24x7x365 basis. This strategy must provide that the business priorities are well understood,

Highlights

An availability plan should be developed based on business priorities, not on the underlying technology requirements.

Recovery programs should be designed as a complement to both continuity and availability plans.

Organizations should minimize single points of failure and store critical information outside of the primary data center to prevent data loss or exposure.

and that they're interlocked with an IT infrastructure that will enable smooth operations and support the needs of the business. An availability plan should be developed based on business priorities, not on the underlying technology requirements. Availability solutions are often built from a technology perspective to minimize cost and complexity. Such a bottom-up approach increases the chances of failing to meet business requirements, since effective availability solutions typically require multiple platforms and resources for proper execution.

Recovery

A properly designed recovery program should define complex business interdependencies and map out the supporting delivery infrastructure. These elements should be integrated with overall business objectives as well as associated continuity and recovery strategies. This level of capability requires detailed design, implementation, operation and management to address various facets of disaster recovery – such as crisis management, incident management and vital-records management. These facets are linked closely to the continuity requirements discussed above.

Recovery programs should be designed as a complement to both continuity and availability plans – providing alternative processing capabilities in the event of an outage or other disruption that could compromise local processing. Organizations should implement and maintain a separate recovery center with a stand-alone configuration to minimize single points of failure. All critical information should be stored outside of the primary data center facilities to help prevent data loss or exposure, and must be synchronized at the time of recovery to ensure accurate information for the resumption of business processes. Organizations should also perform robust, regular testing to confirm end-to-end information validation and compliance with end users' requirements as well as those of external partners that contribute to overall business outcomes.

Highlights

Security represents an integral component in every enterprise information-based-risk program.

Organizations need the ability to detect threats, intrusions and unauthorized access—and to act quickly to mitigate the damage.

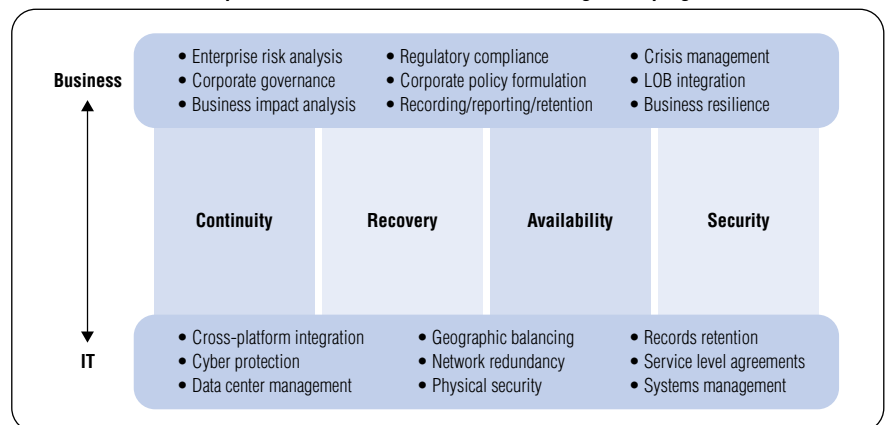
A program that incorporates continuity, recovery, availability and security can help overcome the challenges associated with increasingly sophisticated information-management techniques.

Security

Security represents an integral component in every enterprise information-based-risk program, and should be a common consideration in continuity, availability and recovery plans. Regardless of where the information resides—at the business process level in the production environment, at the redundant operations level supporting availability, or in the remote data backup facility that supports recovery—organizations should develop and follow strict guidelines for managing, transferring and restoring data to protect it from damage or exposure.

Organizations need to start by assessing their current capabilities as they relate to both physical and logical security, and identifying potential exposures and single points of failure. It is important to develop policies that govern infrastructure, management processes, access rights and other factors. Organizations need the ability to detect threats, intrusions and unauthorized access—and to act quickly to mitigate the damage. Security plans should focus on the protection of not only intellectual capital and confidential information but the physical infrastructure and employees, as well.

A comprehensive information-based-risk-management program





When addressed as part of a balanced approach, these four areas should help organizations overcome the challenges associated with increasingly sophisticated information-management techniques, and can form the basis for a comprehensive program for managing information-based risk.

Conclusion

The challenges that companies face in managing and protecting information are changing dramatically. Continually evolving technology affords greater opportunities to extend the enterprise, often on a global basis. The resulting global availability of information is critical in realizing successful business outcomes. At the same time, threats to the enterprise's information are increasing, as are cost pressures to deliver more effective solutions with less funding.

In this changing business climate, a focused strategy must be implemented to control information-based risk. A combination of four areas – continuity, recovery, availability and security – can provide a systematic approach to helping protect organizations' critical information assets and enable a more flexible and strategic foundation for addressing challenges in the future.

For more information

To learn more about continuity and recovery, contact:

Joseph E. Starzyk, PMP
Senior Business Development Executive
IBM Business Continuity and Recovery Services
E-mail: jestarz@us.ibm.com
Phone: 1 407 849-9364

© Copyright IBM Corporation 2007

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

Produced in the United States of America
02-07
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.

IBM assumes no responsibility regarding the accuracy of the information provided herein, and use of such information is at the recipient's own risk. Information herein may be changed or updated without notice. IBM may also make improvements and/or changes in the products and/or the programs described herein at any time without notice.

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.