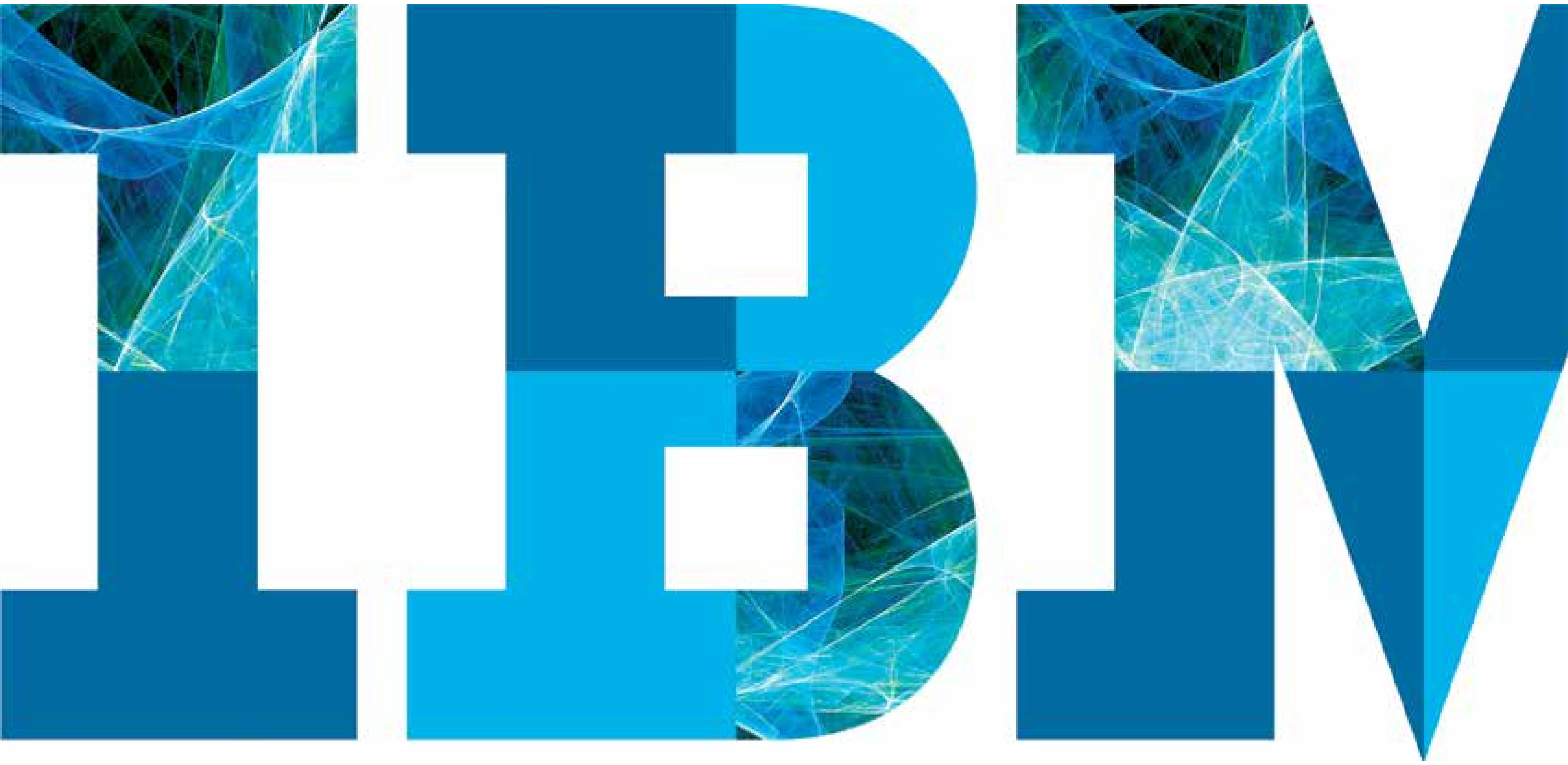
IBM Global Technology Services
White Paper

IBM Business Continuity and Resiliency Services

Aligning IT risk management with strategic business goals

New metrics and technologies help meet the challenges of an always-on business world



A better approach to IT risk management

Information technology is no longer a secondary or tertiary business function. Now, IT's support of business goals includes tasks like using mobility to open new revenue streams and improve employee productivity, deploying cloud technology to more efficiently and economically run production workloads, and analyzing big data for true business insight. In short, business success now hinges in large part on the constant availability of IT services.

Despite the critical role played by IT, many business leaders lack confidence in their organization's ability to effectively identify and manage IT risk. For example, only 17 percent of the 2,316 IT professionals surveyed in the IBM Global Study on the Economic Impact of IT Risk said their organization has a comprehensive IT risk strategy that is consistently applied.[1] In fact, 31 percent said their organizations had no IT risk strategy at all. This is happening at a time when a thoughtful, holistic IT risk management plan has never been more important.

Because of the increasing reliance on IT, the time is now to develop and implement holistic risk management programs—ones that examine IT risk in light of an IT failure's potential to affect overall business operations and strategic goals. This approach differs from the traditional development of risk management plans: identifying threats and prioritizing programs to combat them based on the likelihood of the threat's occurrence.

Although the act of quantifying and qualifying risk factors provides useful information for risk analysis, it does not accommodate management's need to align risk decision-making priorities with business objectives. This is a significant limitation of the traditional approach to risk management, and is inconsistent with the International Organization for Standardization's (ISO) 31000 standard emphasizing risk management as a strategic discipline. Because the traditional risk management approach does not establish a link between IT services and strategic business objectives, it cannot demonstrate the potential effect of risk on an organization's ability to achieve those objectives. In order to appropriately identify business risks associated with the use of IT, organizations need to develop a risk management approach that can:

- **Protect brand reputation and revenue** by improving availability and resiliency—the keys to providing the near constant access to data, systems and applications demanded by today's "always on" business environment
- **Improve competitive advantage** by deploying analytics to help organizations examine data so as to make calculated responses to risk that competitors cannot
- **Reduce financial and reputational exposure** by helping to protect the business from negative disclosures, business losses and fines or penalties associated with downtime or data loss
- **Improve alignment of IT with business needs** such as the need to improve business agility, allowing organizations to more quickly respond to both threats and opportunities

Developing the right metrics

In the past, organizations have used key performance indicators (KPIs) as metrics to track and manage their performance in the implementation and achievement of risk management initiatives. However, IBM believes that KPIs are insufficient to appropriately measure IT threats, their potential impact and an organization's ability to respond to them. Key risk indicators (KRIs) are often preferable metrics. Why? While KPIs are based on historical performance data, KRIs developed by the organization can act as early warning indicators to alert organizations to the presence of emerging risks, helping them better evaluate, mitigate and even avoid IT threats.

Examining the way IT supports business operations in four key categories can help organizations develop key risk indicators. Those categories are:

Availability and resiliency: Business and IT executives must jointly establish availability and resiliency goals and strategies for systems, applications and data, deploying advanced methods, tools and technologies to speed their recovery after an outage.

Data security, archiving and analysis: Data needs to be protected, archived and analyzed in a way that helps the organization both meet governmental and industry regulations and obtain true business insight.

Agility, scalability and performance: The IT organization must be able to respond to fluctuating business needs by adapting IT capacity and performance to changing requirements.

Accuracy and timeliness: Accurate and timely information flow across business and operational processes is crucial for business performance. Data quality, including the source of the data (whether internal or external), must meet criteria for reliability in order to support business goals.

An organization should develop KRIs by examining IT service delivery for each category to determine how an interruption in delivery is likely to affect business operations. Take data security and archiving as one example. If a retailer insufficiently protects data and customer credit card information is stolen, that retailer risks damage to its brand, business losses brought about by consumers' fear of using credit cards while shopping, and non-compliance with Payment Card Industry data protection standards. If a healthcare company stores data for an insufficient period of time, it risks monetary penalties for failing to meet the data retention regulations of the Health Insurance Portability and Accountability Act. Risks to data protection and retention have therefore become risks to the business itself. Anything that threatens data protection or retention, therefore, should be considered a key risk indicator.

In addition to their examinations of IT, organizations should also review critical components of the core business to determine their linkage to IT risks and identify metrics to monitor. IBM suggests "deconstructing" the company into six domains necessary to business operations, assessing the risks to those operations if IT is impacted, then determining ways to improve the availability and resiliency of those domains. The domains are:

People: The human resources who compose the company, and how to keep them working and communicating in the event of disruption

Processes: The company's core business processes and the technologies required to keep them operating

Technology: The equipment, tools, data, applications and systems that support core business processes, including new and emerging technologies such as cloud computing, mobility and social business

Suppliers: The businesses and other organizations that provide the critical materials, services and information necessary for the company to conduct business

Infrastructure: Components—such as physical security, electrical systems and cooling—necessary for business operations and under the control of the company

Exostructure: Critical components of the ecosystem—including power supply, water supply, roads, transportation, food supply and communications—typically outside of the organization's control. However, it is important to note that many elements of the exostructure can be re-created by the business for use in times of emergency. For example, third-party business resilience centers can provide fully operational work sites to which a business can relocate during times of emergency.

The IBM method of IT risk management

IBM has established a risk management method based on ISO 31000 that can help IT organizations better identify, assess and respond to business threats in alignment with overall business goals. The method consists of three steps: ascertain, assess and act (see Figure 1).

Ascertain

The first step in the IBM method is to establish goals for the IT risk management program. Setting goals early in the process helps clarify the work to be done and also helps to engender corporate buy-in to risk management programs. To help establish goals, the organization must determine strategic business initiatives, define IT risk-management tasks, and identify internal and external stressors. The IT threats and stressors that are likely to have the greatest impact on IT's ability to support business operations are key risk indicators. Next, the organization should define clear roles and responsibilities for risk management tasks, working to include required stakeholders throughout the organization. Broad engagement of people from across various departments should be encouraged. Defining roles in this way helps to establish IT risk responsibilities.

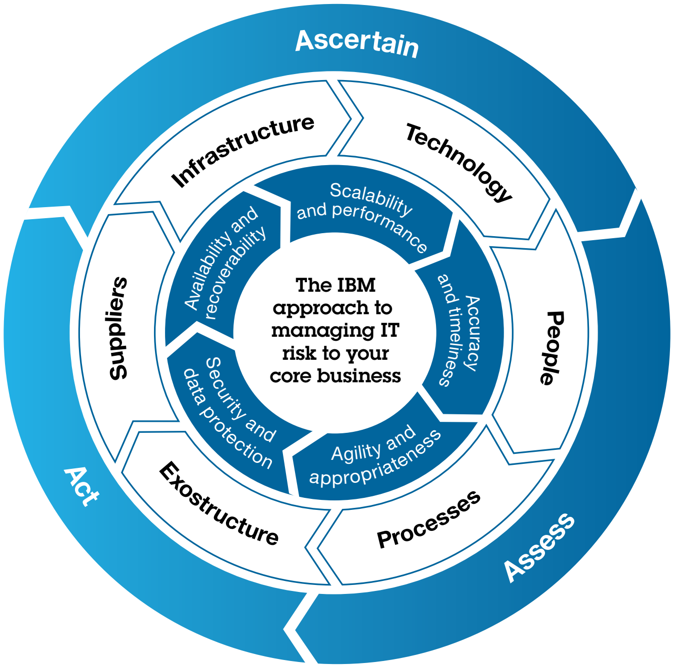

Ascertain
Assess
Act
Infrastructure
Technology
People
Processes
Exostructure
Suppliers
Scalability and performance
Accuracy and timeliness
Agility and appropriateness
Security and data protection
Availability and recoverability
The IBM approach to managing IT risk to your core business

Figure 1: As illustrated here, IBM's approach to IT risk management entails ascertaining, assessing and acting upon IT risk as it applies to IT and business components.

Assess

With risk management goals set, the organization should work to align IT risk management tasks with key business objectives and operations in order to develop key risk indicators. By examining IT operations—including new and emerging technologies such as cloud computing, mobility and social business—against the risk categories discussed earlier in this paper, the organization can more easily identify which IT services it needs in order to rapidly and effectively respond to threats, opportunities or outages. The development of a clear understanding of IT's relationship to key business functions is the most important part of this process. Any assessment should include the potential impact on business operations and goals should the IT risk materialize, rendering IT unable to provide needed service levels. This impact analysis can be conducted as both a quantitative assessment (direct financial loss or increased cost of performing a service) or qualitative assessment (impact on reputational risk). It is important that the organization remain alert to specialty and compliance risks while improving resiliency operations.

Many organizations will find conducting a gap analysis to be helpful in this effort. This type of analysis measures the difference between existing and desired availability and resiliency levels. For example, if an organization determines that to support business resiliency goals, data and applications must be able to be restored within minutes after an outage, and that type of restoration now takes several hours, the organization will need to update its resiliency operations.

Act

At this point, organizations should begin determining how to implement balanced resiliency plans, employing clear communications among stakeholders, continually monitoring key risk indicators, and considering new technologies such as cloud computing to help improve their risk stance. Stakeholders should establish IT risk management activities to help provide alignment with business objectives and to help increase involvement at various organizational levels, including C-level management, lines of business and IT.

Continually monitoring IT risks based on the meaningful metrics devised during the assessment phase helps organizations better prepare for threats of outage or other disruption. Key risk indicators should be continually reviewed to help provide IT services' ongoing alignment with changing business objectives and evolving threats. The monitoring processes can be expensive, since each KRI equates to a monitoring cost. Organizations, therefore, should consider finding the right investment points to both enable more successful risk management programs and stay on budget.

While the business transitions to any new risk management system, it needs adequate resources to develop robust communication, awareness and training programs. These programs are necessary to support integration of IT risk management with broader governance, compliance and availability and resiliency activities. Additionally, making all stakeholders aware of and able to use the IT risk program helps to emphasize that IT risk management is part of everyone's job. During this transition phase, the training and awareness programs should help stakeholders throughout the organization understand their roles in contributing to the new, holistic risk management program.

Why IBM?

IBM Business Continuity and Resiliency Services provides IT risk management services to organizations that need to more proactively identify, understand, manage and respond to operational risks and business disruptions. We have more than 50 years' experience in business continuity and resilience, and our 1,800 resiliency professionals currently serve more than 9,000 organizations worldwide.

IBM Resiliency Consulting Services can help organizations design, implement, test and manage a robust, adaptable and measurable resilience program designed to help you improve risk management by meeting your organization's needs for continuity, availability, security and recovery. We start by taking an objective, broad-range view of the efficacy of your existing risk management environment, examining it against best practices and then, as needed, helping you implement a resiliency solution that better meets today's demands. In doing so, IBM can typically help you better manage risk, improve resilience, prioritize resiliency investments, reduce downtime and defend your organization's data, applications and IT infrastructure—thereby protecting both IT and the critical business processes that depend on it.

For more information

To learn more about the 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

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10504

Produced in the United States of America
August 2014

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

[1] *IBM Global Study on the Economic Impact of IT Risk*, IBM, 2013

♻ Please Recycle