Aligning IT with strategic business goals

*An proactive approach to managing IT risk to your business*
Contents

2 Executive summary
3 The evolving business challenge of IT risk management
3 The traditional approach to managing IT risk
4 Embracing a holistic approach
6 The IT Risk Spectrum
8 The IBM method of managing IT risk to the business
10 Summary
10 Why IBM?
12 For more information

Executive summary

For virtually every business operation today, information technology (IT) is an essential and indispensable component. Although this reliance on IT provides obvious benefits, it also presents significant business challenges. The complexities of IT and its interconnectedness to so many areas of the business leave organizations more vulnerable than ever to inherent risks. Events that impact IT, which previously could be contained within the IT department, can now affect the entire business. Data loss, corruption and inaccessibility—as well as security breaches and infrastructure failures—quickly become public events that can severely impact an organization’s productivity, its reputation and its ability to achieve strategic goals.

Despite the widespread business impact that IT threats can have, most organizations do not consider aligning their IT risk management plan with their strategic business initiatives. Instead, they continue to implement a more traditional approach to risk management that focuses on performing a cost-based analysis of what might go wrong in an uncertain world and on implementing metrics derived from variables that cannot be satisfactorily documented. Such an approach can be unreliable and may not adequately help identify and manage IT risk.

ISACA, the nonprofit, global membership association for IT and information systems professionals, defines IT risk as “the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.”¹

A more effective means of managing the impact that IT risk can have on the business involves taking a holistic approach. Using this method, IT service delivery capabilities can be more directly linked to what the organization needs in order to improve reliability, flexibility and agility in meeting business goals and objectives. Such an approach helps provide more accurate and timely information about the risk that the current state of IT service delivery poses to a company’s business goals and thus, helps prioritize appropriate mitigation efforts.

This white paper examines the business challenges and risks that IT dependence can present and why traditional approaches to IT risk management have become inadequate. It then introduces a structured approach that ties risk management back to the organization’s overall strategic business initiatives. By improving the alignment of IT with business needs, the IT organization
can help the business to operate more cost effectively and enhance its ability to respond to change with more informed, measured decisions.

The evolving business challenge of IT risk management

In the early days of information technology’s evolution, IT primarily referred to an organization’s hardware and networks, which simply provided a means for processing information and safely storing and backing up data. Over time, the need for improved business efficiency, the greater reliance on technology for executing critical business transactions and the thirst for more information and more complex analytical reporting have made the role IT plays in the success of the business inexorably intertwined with the operation of the business itself. IT’s support of business goals has grown to include tasks like accommodating an increasing amount of data and applications, organizing it so that it is useful and storing it in a way that keeps it accessible. Additionally, IT management is responsible for employing a wide range of processes, people, facilities and strategies to deliver the expected results to the business. It must manage these responsibilities—while also meeting the growing demand for flexibility and around-the-clock availability—with a smaller IT budget and fewer people.

This evolving dependence on IT has also increased the impact that IT risks can have on an organization’s entire business. The higher priority given to business resilience, along with the standardization and broadening of risk management to encompass business units and their processes, has certainly helped to reduce these risks. Nevertheless, many business leaders still lack confidence in their organization’s ability to effectively identify and manage IT risk. Consider, for example, the following findings from three different IBM studies:

- Chief information officers (CIOs) who expressed concerns about risk management and compliance: 58 percent
- CIOs who rated their company’s overall approach to mitigating IT risk as “average” or “poor”: 34 percent
- Senior executives who said they do not have a formal risk-management function in place: 30 percent

The traditional approach to managing IT risk

Why have we developed such a lack of confidence in IT risk management? Threats to IT services present risk to the business when vulnerabilities are exploited across a wide spectrum. Many companies continue to analyze risk through a very narrow lens that focuses on the financial impact of IT service delivery. This “traditional” approach begins by identifying conventional threats—such as fires, floods, power failures, vandalism, terrorism and security failures—based on the potential impact that these threats could have on business availability, recoverability and security. However, threats that fall outside of the conventional realm are easily overlooked. If an organization cannot identify threats or accurately determine their likelihood, it cannot assess its true vulnerability to them.

After the conventional threats have been identified, the next step in a traditional approach is to prioritize the management of those threats according to the potential business costs, losses and
operational effects. Although the act of quantifying and qualify-
ing these factors may provide useful information for risk analysis, it does not accommodate management's need to align decision-
making priorities with business objectives. This is a significant limitation of the traditional approach and is not consistent with the International Organization for Standardization’s (ISO) 31000 standard emphasizing risk management as a strategic discipline for making risk-adjusted decisions rather than as a compliance-based function. Because the traditional approach does not establish a link with enterprise objectives and strategic business initiatives, it cannot demonstrate the effect of risks on achieving these objectives.

If an organization cannot identify threats or accurately determine their likelihood, it cannot assess its true vulnerability to them.

Embracing a holistic approach

In order to appropriately identify the business risks associated with the use of IT, organizations need a broader view of IT risk that goes beyond traditional standards and that aligns IT with the strategic direction of the business. Specifically, they need an approach that can:

- Improve alignment of IT with business needs to expand business agility by more quickly responding to change with informed, measured decisions
- Protect brand and revenue by helping to assess the threats to the IT infrastructure, their potential business impact or benefit and an organization’s risk tolerance to help plan a realistic strategy
- Improve IT service levels to achieve strategic business initiatives by helping to manage IT risk with more accurate and appropriate information
- Reduce financial and reputational exposure by helping to protect the business from negative disclosures, losses and fines or penalties
- Increase their competitive advantage by helping them to make calculated responses to risk that competitors may lack the insight to make

By tying classic risk techniques directly to strategic business initiatives, organizations can more easily document key performance indicators (KPIs) and key risk indicators (KRIs) and prioritize risks based on their impact on or contribution to strategic goals. Additionally, the business is better able to implement balanced risk management plans, employ clear communication plans and continually monitor risk indicators.

The importance of stronger metrics

More and more companies are defining KPIs as metrics to track and manage their performance at each managerial level involved in the implementation and achievement of strategic business initiatives. KPIs are consolidated in reports to provide board members with a high-level overview of the historical performance of the company and the forward-looking achievement of the strategic business initiatives. Metrics are also required to track and manage risks; however, the KPIs are not suited for this purpose because they are based on historical performance data.

Instead, KRIs are required as early warning indicators to alert the organization about emerging risks well before the risk actually occurs, allowing businesses to capture opportunities or reduce a potential negative impact on the organization's ability to achieve its objectives. These indicators must alert the organization early enough to provide time to react and take appropriate measures to counter the risk.
Although KPI and KRI metrics are different, they are related. KPIs are used to track businesses performance. KRIs are used to warn businesses of impending change. Because business entities are interdependent in terms of services, if a supplying entity is not capable of providing a service, the receiving—or dependent—entity is at risk. These are “capability” risks that could potentially prevent the dependent entity from achieving its performance targets and should be managed through KRIs. Using an illustrative example:

If opening new channels to exchange information with customers is fundamental to providing desired customer experiences, and if it is part of the implementation of a broader strategic initiative of “becoming customer centric,” several of the following business KPIs might be involved:

- Reducing the implementation time of the new channel (ideally, down to three months) to respond more quickly to new market opportunities and achieve a faster return on investment
- Increasing the rate of acquiring new customers through the new channel
- Increasing the daily scheduled uptime (ideally, to 24 hours a day)

Assuming this new channel is based on a new Internet website accessible by smart phones, the dependency on IT is obvious, and the business could consider IT to be a potential risk if it does not provide the expected service criteria. The channel implementation time—which the business expects to be equal to or less than three months—could be directly affected by the time required to design, develop and implement the new Internet website, currently estimated by IT to be six months.

IT’s next steps are to perform a gap analysis to identify the areas needing improvement and a root-cause analysis to understand why the implementation of new IT services takes so long. If, for example, the outcome of the root cause analysis shows that a) the application development time is too long due to limited availability of the development systems, and b) the time to procure the new hardware for the new application is prolonged due to complicated purchasing processes, then there are now two KRIs that can be used as leading indicators of the IT service’s “agility” factor to produce a timely response to new service.

There is an obvious IT capability gap in terms of responding in a timely manner with the correct new or modified IT service in support of changes in business requirements; therefore, the business is at risk of failing to achieve its strategic goal. To monitor that risk, the business has to define a specific KRI and IT has to define a KPI to track the improvement in the area of “time required to implement a new service.”
The IT Risk Spectrum
To answer the need for a more structured and holistic approach, IBM has built the IT Risk Spectrum™, which consolidates a variety of IT risks into five logical categories. These risk categories help determine the impact that the current state of IT service delivery and mitigation prioritization can have on business goals. By using the IT Risk Spectrum, companies can improve the alignment of IT to their business needs and thus use IT to help make the business more agile. As depicted in Figure 2, the IT Risk Spectrum consists of five IT risk groupings that can be associated with specific business goals: agility and appropriateness, scalability and performance, security and data protection, accuracy and timeliness, and availability and recoverability.

Agility and appropriateness: IT services must have the capability to adapt and transform rapidly, effectively and cost efficiently to achieve targeted business outcomes.

Scalability and performance: The IT organization must be able to respond to changing business needs by adapting IT capacity and performance as needs fluctuate. In addition, it must be able to track applications and data performance, as well as throughput metrics, among all services and components. An ability to align itself with the performance and capacity needs of business users and customers is also necessary.

Security and data protection: Using system management, archiving and formal reporting and investigation help maintain a high level of security. Infrastructure and physical security are also required to help provide adequate data protection.

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 certain criteria in order to support business goals.

Availability and recoverability: Keep systems running and, if necessary, recover from interruptions in line with business expectations.

<table>
<thead>
<tr>
<th>IT Risk Spectrum</th>
<th>Real-life risk example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agility and appropriateness: Adapt and continuously transform more rapidly, effectively and cost efficiently to achieve targeted business outcomes.</td>
<td>A European bank can’t satisfy varying maintenance requirements for its customers until it deploys a multiplatform performance management solution to help expand the reach of its IT services to new internal customers. The result: increased service agility and flexibility, improved internal customer satisfaction and reduced management cost.</td>
</tr>
<tr>
<td>Scalability and performance: Maintain more acceptable performance based on business needs and appropriately accommodate changes in business service volume.</td>
<td>A US retailer experiences an unprecedented surge in online shoppers, which disables its web store. The company’s inability to scale to demand causes a loss of sales, negative publicity and loss of customer confidence to purchase online.</td>
</tr>
<tr>
<td>Security and data protection: Provide the appropriate access controls while helping to protect the business’ information and resources.</td>
<td>An industrial manufacturer in Tokyo fails to upgrade firewalls and antivirus software. Hackers access customer data, leading to cancelled contracts and a loss of customer confidence.</td>
</tr>
<tr>
<td>Accuracy and timeliness: Provide more accurate data to the right people, at the right time to enable more informed decision making.</td>
<td>A European bank applies application updates that corrupt client data, causing a computer outage for multiple days unacceptable delays to account updates and widespread media coverage and calls for investigation.</td>
</tr>
<tr>
<td>Availability and recoverability: Keep systems running and, if necessary, recover from interruptions in line with business expectations.</td>
<td>A Turkish telecommunications provider’s data center is flooded as a result of unprecedented rainfall. Without a documented and tested recovery or continuity strategy, customer service is disrupted, and the provider experiences lost processing time, cancelled contracts and damaged brand reputation.</td>
</tr>
</tbody>
</table>

Figure 2: The IT Risk Spectrum consists of five categories based on business goals.
Availability and recoverability: Business and IT executives must jointly establish availability and recovery strategies by using a repeatable, sound process and by spending accordingly to help meet these business requirements. The organization should be able to use advanced methods and tools for a more timely response to incidents, problems and outages—and a continuing improvement process should be in place.

IT risks are constantly applying pressure to an organization's core business. By providing a prescriptive view of the company and an understanding of how IT risks affect specific business goals, the IT Risk Spectrum helps the organization determine how much these risks might impact the core business.

Critical components of the core business must also be reviewed to determine their linkage with the IT Risk Spectrum and identify the correct metric to monitor. IBM applies its Core Business Framework to “decompose” the company in such a way as to render the components reviewable and to allow for both dependency and parallel analysis. This framework is comprised of six domains to cover virtually all components—both internal and external—that are necessary to enable business operations:

- **People.** The human resources with assigned roles and responsibilities who compose the company, as well as the processes required to maintain their skills through training and communications
- **Processes.** How the company conducts its core business through business process modeling in an open process framework and maintains its technology through IT strategy and governance, business continuity, backup and recovery, and service management, among others
- **Technology.** Equipment and tools that support the company’s business processes, such as servers, storage systems, networks, databases, applications and telephony
- **Suppliers.** Businesses and government agencies that provide the critical materials, services and information necessary to allow the company to operate and conduct business
- **Infrastructure.** Components under the control of the company that enable operations such as physical security, electrical systems, water and cooling
- **“Exostructure.”** Critical components of the ecosystem, outside the control of the company, such as power supply, water supply, roads, transportation, food supply, communications and governance

---

*Figure 3: IBM’s approach to IT risk management centers on IT risk to the business and its operational components.*
The IBM method of managing IT risk to the business

IBM has established a condensed risk management method based on ISO 31000 that, when applied to the IT domain, can provide a more compliant risk architecture that can more easily interface with virtually any enterprise-wide risk management program. The three phases of this method—ascertain, assess and act—are described below.

Ascertain
The first step in the IBM method is to establish the scope and goals for the IT risk management program. An IT risk program encompasses the activities necessary to continually identify, assess and respond to threats and their relative risks to the business. Without identified goals and clearly defined roles and responsibilities, the subsequent management processes are in jeopardy. Setting both scope and roles early in the process of establishing the program helps to gain buy-in to the process and to subsequent requests for mitigating actions from newly identified IT risk owners.

Establishing the scope can be accomplished by determining the strategic business initiatives, defining the IT risk-management objectives and identifying internal and external stressors. The scope of the program is designed to be very focused at first, expanding later to include the entire enterprise. Other factors determining scope may be the length of time needed for the activity and the locations to be included. It is also during this phase that the risk-assessment method is selected and subsequent measurement systems for the IT risk management process are outlined.

Assess
With the business goals set, the IT risk areas are defined relative to the strategic business initiatives by aligning the IT services directly to their support of business goals. A critical element of establishing holistic risk management for business resilience is the ability to assess a wide range of risks in a balanced way in order to build an overall picture of the threats and opportunities the organization faces. By using a guide like the IT Risk Spectrum and analyzing the IT services that are needed across the entire enterprise to support the business initiatives, the organization can more easily identify which IT service areas it needs most in order to be more agile in responding to change. Clearly understanding the relationship of IT services that support those initiatives is an important aspect of risk assessment.

“IT is a big part of our risk management because nothing can be done without it these days,” says Kris Wiluan, CEO of KS Energy Services Limited.
The next step is to conduct an IT service “all capabilities” analysis to identify measurable IT risks and define performance metrics. This helps determine meaningful KPIs and KRIs and helps to quantify IT risk to the business based on IT performance capabilities. This knowledge improves the organization’s ability to define and prioritize balanced treatment options, place them into a roadmap to implement mitigation solutions with confidence and identify controls to assist with monitoring changes that may impede success.

The assessment must also include the potential impact to business strategic goals should the IT risk materialize, making the IT service unable to provide the expected level of service. This impact analysis can be conducted as both a quantitative (direct financial loss or increase cost of performing a service) or qualitative (impact to reputational risk) assessment. The IBM Operational Risk Quantification (ORQ) method helps analyze broad categories of risk events, including “top-down events,” whose severity is directly measured in financial losses, bypassing process-related detail and “bottom-up events,” which are propagated across a process-resource network to ultimately display a financial impact result.8

It is important that the organization does not lose sight of specialty or compliance risks while it broadens its view of resilience. Rather, it must create an evolving journey toward resilience by including a wider range of risks in the evaluation and prioritization process to help provide a broad-based assessment by the enterprise stakeholders. The assessment phase is designed to provide solid performance and risk indices in the form of KPIs and KRIs, which can enable better visibility into the strategic business goals and the IT services supporting them. A risk-management plan results, which includes responsible and appropriate responses to the identified risk in the form of controls or safeguards.

**Act**

Now with the KPIs and KRIs documented and prioritized against business strategic goals, the challenge becomes one of implementing balanced treatment plans, employing clear communication plans and continually monitoring the risk indicators. In this phase, the risk management plan is implemented by assigning the various resources across the organization with the responsibility and accountability to act. The risk owners establish and manage IT risk to help provide alignment with business objectives and to help increase involvement throughout the organization at all levels: C-level management, the business lines, IT professionals, board members and employees.9

Continually monitoring IT risks based on the meaningful metrics devised during the assessment phase helps prepare the business to act responsibly to stressors applied across the organization. These same indicators must be continually reviewed to help provide sustained alignment with changing business objectives. Monitoring can cover many areas of both IT and the business, depending on the outcomes of the risk assessment and KRI definition. Examples may include “percentage of application development and maintenance projects delivered on time or early” or “mean elapsed time to achieve incident resolution.”

Based on the assessment results, the selection of risk mitigation actions must be balanced with the potential impact to the business should the risk occur. Establishing the monitoring processes can be expensive, as each KRI equates to a monitoring cost. Finding this optimal investment point is crucial for businesses that want to enable more successful risk management while maintaining fiscal responsibility.
As the business transitions to this new management system, it needs continued senior-level commitment, as established in the ascertain phase, and adequate resources to develop robust communication, awareness and training programs. These programs are necessary to support integration of IT risk management with broader governance, risk and compliance activities. Additionally, making all stakeholders aware, educated and able to use the IT risk program helps to emphasize that IT risk management is part of everybody’s job. During this transition phase, these training and awareness programs should be aimed at all levels of employees and should help stakeholders to understand their roles and begin regular reporting to the different levels involved with the program.

**Summary**

The proliferation of IT services critical to achieving strategic business goals presents unique risks and opportunities. More than ever, IT must be reliable, predictable, available and security-rich in order to support critical business processes and key initiatives. Identifying the risks to the business associated with the use of IT requires a broad view of IT risks and IT services throughout the organization. This cannot be adequately accomplished with the traditional approach that looks only at the physical and natural threats that may impact IT service delivery. Rather, as this paper has demonstrated, it is time for IT to build on its foundation of threat-based impact assessment and broaden the spectrum of risks it includes to further protect and support the business in meeting its strategic goals.

By implementing a holistic, structured approach, organizations can assign resources across the company, continually monitor IT risk using meaningful metrics and communicate the IT risk management program to all stakeholders. Such a proactive risk culture makes it possible to respond more quickly and appropriately and to find the optimal balance between IT risk and the cost of risk mitigation.

**Why IBM?**

IBM provides IT risk management services to clients who need to more proactively identify, understand, manage and respond to operational risks and business disruptions. We can help you maintain near-continuous business operations, enabling you to better protect your brand and support growth for your bottom line and to remain a trusted provider to your customers and partners. By using industry standards, such as the ISO and ISACA, IBM resiliency specialists become familiar with the environment, help tailor the resilience framework to your unique needs, review the respective collateral to be used for the assessment and provide a roadmap for remediation and improvement. As a global leader in IT solutions, IBM offers a wide range of products and services, which our consultants apply to help meet evolving risk management needs.
For more information
To learn more about the IBM Resiliency Consulting Services, the IBM risk management method or the IT Risk Spectrum, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: ibm.com/services/continuity

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: ibm.com/financing

3 “The evolving role of IT managers and CIOs: Findings from the 2010 IBM global IT risk study,” IBM, September 2010.
4 “Key trends driving global business resilience and risk: Findings from the 2011 IBM global business resilience and risk study,” September 2011.
5 “Key trends driving global business resilience and risk: Findings from the 2011 IBM global business resilience and risk study,” September 2011.
7 “Key trends driving global business resilience and risk: Findings from the 2011 IBM global business resilience and risk study,” September 2011.
8 “Operational risk analytics in the context of information technology (IT) infrastructure,” IBM, March 2012.
10 “Operational risk analytics in the context of information technology (IT) infrastructure,” IBM, March 2012.