Supporting information technology risk management

It takes an entire organization
Introduction
As information technology (IT) has evolved into a central component of business operations, the business has become increasingly vulnerable to IT risk. IT events can no longer be contained without impacting overall business functions. Today, data loss, corruption and inaccessibility, as well as system and infrastructure failures, can severely impact an organization’s productivity. This white paper is designed for organizations to learn more about the wide-scale effect that information technology risks have on overall business functions. It explains the various types of risk to consider and why managing these risks efficiently requires balancing risk mitigation with the value that a particular business process provides for the organization.

Confronting the challenges
Faced with more challenges than ever before, organizations must make a greater commitment to managing IT risk to the business. Nevertheless, a 2010 survey of IT professionals showed that 34 percent of respondents rated their organization’s overall approach to mitigating IT risk as average or poor.¹

# ISACA®, a 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.”

Most organizations have just a handful of business processes that contribute to the majority of their business revenue or reputation. Although eliminating IT risk entirely may not be realistic, it does make sense to balance the risk mitigation selection based on the value that a particular process brings to the business.
Senior business leaders and officers, need to recognize that business processes and technology are interdependent, irreplaceable components of a comprehensive risk management solution. With this understanding, they are better positioned to work with IT risk managers, business process leaders and other risk stakeholders to efficiently and cost effectively plan, implement and manage technologies that address enterprise IT risks. Organizations that lack this basic understanding are more likely to face potential consequences, including:

- **Overlooking significant risks.** Although C-suite officers may be able to delegate oversight of operational risks to line-of-business (LOB) managers closest to the risks, ultimately they are still responsible for ensuring that risks are identified, mitigated and optimized at an enterprise level.
- **Inadequately meeting fiduciary obligations.** Officers are expected to sustain and protect their firm’s core businesses.
- **Leaving business processes vulnerable.** Reliable business operations depend on the protection of business processes against operational risks consistent with the loss potential from the risk.
- **Reducing profits.** Even non-catastrophic “operational” disruptions can have a huge cumulative financial impact on an organization’s business.
- **Creating negative publicity.** When issues arise, media exposure can have a lasting impact on an organization’s brand and good will.

**Types of risks**

IT risk can involve a range of threats, from the everyday to the unthinkable, with varying levels of likelihood and impact. These threats can be grouped into three categories: Data-driven risks, business-driven risks and event-driven risks.
Supporting information technology risk management

Data-driven risks: From an IT perspective, data-driven risks often receive the most attention. Generally, they occur more frequently than other types of risks, but the financial loss from any one occurrence is relatively low. 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.

Business-driven risks: Business-driven risks directly impact business continuity and business operations. An organization’s board members would typically be most concerned about these risks because they are generally more strategic in nature than data-driven risks and have businesswide ramifications.

Event-driven risks: Any event that disrupts an organization’s workforce, processes, applications, data or infrastructure can be classified as an event-driven risk. These risks affect business continuity and viability.

Developing an effective IT risk management solution
The importance of managing IT risks increases as businesses seek to leverage existing technologies and produce better compliance results in order to stretch and improve their bottom line.
Effectively managing IT risk requires:

- Evaluating how a disruption or corruption of IT services could threaten and impact critical business services
- Effectively identifying and measuring IT risk to the business
- Defining strategies for managing those risks judiciously
- Defining and implementing an ongoing IT risk management and governance program
- Monitoring IT risks on a continuous basis and taking appropriate, timely actions to mitigate the risk to business services

A successful IT risk mitigation program consists of five phases: Management and governance, assessment, planning and design, implementation and testing, and monitoring.

Management and governance: Both business conditions and IT capabilities and costs change over time. IT risk management and governance is the process by which an appropriate IT risk posture is maintained long term. Key elements include:

- Creating policies with clear roles and responsibilities to establish the context of “risk” as related to the company’s enterprise risk management program
- Defining key risk indicators (KRIs) for IT risk (indicators that can be measured and monitored to give an early warning to changes in the company’s risk profile)
- Embedding IT risk management considerations into the operational processes of the enterprise
- Evaluating, reporting and communicating on the IT risk profile
- Re-evaluating IT risks and updating mitigation strategies as appropriate

Assessment: The first step of this phase is to clearly identify and evaluate the types of IT risk an organization might face and to gauge its ability to rapidly respond to risk events. Assessment is an ongoing process that involves:

- Defining the key value-producing business services that the organization performs and quantifying their value
- Decomposing the business services into the business components required for their delivery
- Establishing the business impact to the service if a given business component is nonfunctional
- Defining the most significant threats and their relevant risks to the business components by evaluating the probability of each threat’s occurrence and the impact should it occur
- Determining the business services impact based on the effects to the business components
- Establishing and implementing appropriate, cost-effective strategies to mitigate the defined risks based on understanding the organization’s “risk appetite”
- Determining external risk dependencies and how the organization and systems would respond if compromised

Planning and design: During the planning and design phase, the organization develops mitigation strategies for managing IT risks. This phase includes:

- Determining ways to sustain critical operations in the event of a disruption by defining strategic business continuity, disaster recovery and crisis management plans
- Designing a business-requirement-based architecture for the organization’s IT environment
- Optimizing the balance between the organization’s investments in IT risk management and their business value

Implementing and testing: This phase gives the organization an opportunity to validate the effectiveness of its plans, as well as identify weaknesses. Key elements include:

- Creating test plans, executing a successful test, identifying gaps and recommending fixes
- Integrating IT and business needs
- Validating that the IT risk solution is current and actionable
Monitoring: Continuous monitoring of KRI's helps ensure that the organization can identify changing risk levels and take action before the risks materialize and impact a key business service. The keys to successful IT risk monitoring include:

- Mapping IT service components to the business services they support
- Defining KRI thresholds that represent a potentially abnormal condition
- Implementing mechanisms to alert appropriate agents (both people and technology) to take preventive or corrective action

Re-evaluating the IT risk solution

Risks and threats are constantly changing, so organizations need to periodically reassess risks and reconsider the appropriateness and effectiveness of their policies and controls. Questions to address include:

- How does corporate management align IT-related business risk with overall enterprise risk management?
- What challenges does the organization face when balancing the costs and benefits of managing risk?
- What does the organization do to demonstrate that it understands that this is a continuous process and an important part of daily activities?
- Which business functions or processes put the business at the highest risk in case of interruptions or if a security breach occurs? How reliant are these business processes on IT?
- Has the organization sufficiently assessed and mitigated the risk of IT-driven business process interruptions and their financial and reputational consequences?

The IBM offerings

The IBM suite of security and resilience consulting services can identify gaps and areas for improvement in an organization's current IT risk management approach. Leveraging industry standards, such as the International Organization for Standardization (ISO) and Control Objectives for Information and Related Technology (CobiT), IBM resiliency and security specialists become familiar with the environment, help define the security and resilience framework, review the respective collateral to be used for the assessment, and help provide a roadmap for remediation and continuous improvement.

IBM Resiliency Consulting Services can provide flexible solutions tailored to meet an organization's unique IT risk management needs. IBM can help assess, plan, design, architect, implement and test a solution that can be integrated across multiple business functions. Our vendor-neutral approach leverages industry best practices and a structured methodology to help provide a clearer view of IT and infrastructure risks; identify gaps; and define a more comprehensive, cost-effective IT risk management strategy.


IBM Security Services leverages the IBM security methodology to help assess security mechanisms used by an organization's hardware and software systems, networks, databases and personnel. IBM conducts interviews with key managers and staff members to understand the business processes and the effectiveness of existing management controls in the protection and use of data and applications throughout the organization.

Below are examples of how the solutions described above address common business needs:

<table>
<thead>
<tr>
<th>Customer questions…</th>
<th>The IBM answer</th>
</tr>
</thead>
</table>
| How do I know if I have accounted for all of the threats and risks in my environment? | IBM Resiliency Consulting Services:  
- Risk Assessment |
|                      | IBM Security Services:  
- Risk Assessment  
- Security Health Check |
| How do I know which business services pose the greatest financial risk to the stability of my company? | IBM Resiliency Consulting Services:  
- Business Impact Analysis |
| How can I protect my critical data and my business from lost data when the business keeps growing in some areas and cutting back in others? | IBM Resiliency Consulting Services:  
- Business Impact Analysis  
- Managed Backup Cloud  
- Email Management Express |
|                      | IBM Security Services:  
- Data Security Assessment |
| We expect something to get through. How do I reduce the chances of an event critically impacting a crucial business service when the inevitable happens? | IBM Resiliency Consulting Services:  
- Resilient Architecture Design  
- Resilience Plan Development  
- IT and Work Area Recovery |
|                      | IBM Security Services:  
- Security Event and Log Management  
- Firewall Management  
- Intrusion Detection and Prevention System Management  
- Managed Protection Services  
- Identity and Access Management Services |
| I have highly available systems all around, yet they still go down. How can I validate that the technology solution meets the business requirements? | IBM Resiliency Consulting Services:  
- Availability Assessment  
- Validation and Testing  
- Managed Continuity |
|                      | IBM Security Services:  
- Security Event and Log Management  
- Firewall Management  
- Intrusion Detection and Prevention System Management  
- Managed Protection Services  
- Identity and Access Management Services |
| I do not have trained resources to manage the resilience and security life cycle throughout the year. | IBM Resiliency Consulting Services:  
- Resilience Program Management  
- Availability Manager |
|                      | IBM Security Services:  
- Security Event and Log Management  
- Firewall Management  
- Intrusion Detection and Prevention System Management  
- Managed Protection Services  
- Identity and Access Management Services |
Why IBM?
IBM can provide IT risk management services to clients who need to proactively identify, understand, manage and respond to operational risks and business disruptions. Our solutions help organizations maintain continuous business operations, enabling them to better protect their brand and remain a trusted provider to their customers and partners. IBM leverages industry and IT best practices to better understand an organization’s IT risk management needs, help design a security-rich risk management plan to address its unique vulnerabilities and compliance requirements, and help reduce overall risks and costs. As a global leader in enterprise IT solutions, IBM continues to develop products and services to meet evolving risk management needs.

For more information
Learn more about the IBM suite of security and resilience consulting services.

To get additional information about IBM Security Services, visit:

To get additional information about IBM Resiliency Consulting Services, visit: