Information risk management
Executive brief

Strengthen business resiliency with integrated information risk management efforts.

December 2007

IBM Governance and Risk Management
Business alignment, visibility and control

Contents

Executive summary

Information has become a driving force in today's world, and in many ways can be considered the new currency of the 21st century. Since IT serves as the primary mechanism for information flow, storage, access and protection, it has become the central nervous system for the business. As a result, organizations invest significant resources and effort to create agile, cost-effective and high-performing IT environments that facilitate the secure interchange of information.

Unfortunately, many organizations are unable to take full advantage of their information assets, due to the organizational, operational and technical silos existing in today's businesses that add layers of complexity, frustrate risk management efforts and increase costs.

Implementing a holistic approach to information risk management enables organizations to address these challenges, harmonizing their risk management efforts across silos and discrete processes in order to create more flexible, robust and resilient IT and business infrastructures. This executive brief examines the need for effective information risk management and the four primary components that must be considered when building an effective information risk management strategy.

Organizational, operational and process silos put information at risk

For many organizations, information is their most strategic asset. Business systems and infrastructures are designed with the primary purpose of moving information from one point to another. As the currency of the 21st century, information ultimately drives business success.

While governance, risk and compliance investments and efforts are critical to mitigating information risks, too often they add layers of complexity through the creation of disparate data silos, policy control silos, technical control silos, technology silos and other information-related silos that in their disconnected states disrupt the secure interchange of information.

In fact, a 2007 Open Compliance and Ethics Group (OCEG) GRC Strategy Survey found that 84 percent of respondents reported fragmentation of their governance, risk and compliance activities and processes and 65 percent claimed that this fragmentation caused serious business problems due to duplication of efforts, redundant solutions, higher costs and increased risk. Organizations that successfully integrate their governance, risk and compliance efforts can significantly minimize many of these problems.

Organizations benefit from a holistic information risk management enterprise strategy, including an overarching policy definition that will steward the management of data throughout its life cycle, as well as protect data from exposure or damage.

A comprehensive strategy not only addresses governance, risk and compliance concerns, but also helps streamline operations for increased efficiency, reduced costs and improved capacity to leverage information assets. The OCEG GRC Strategy Survey found that 71 percent of respondents that took advantage of opportunities to integrate these activities realized benefits that met or exceeded their expectations.

Information risk management investments typically fall into four main categories:

- **Information security** — Protect and securely share information across the enterprise, partners and customers.
- **Information compliance** — Reduce regulatory, operational and reputation risks, audit costs and audit deficiencies.
- **Information retention** — Support event response to legal, regulatory or investigatory inquiries for information.
- **Information availability** — Plan and deliver continuous and reliable access to information.

Align risk management with business objectives to determine acceptable risk levels

Information risk management strives to enable an organization to remain in line with its risk tolerance. Organizations must not consider risk management's end goal to be the squelching of all information-related risk. Instead, it is to strike a balance between risk and opportunity.

When implemented effectively, information risk management can improve risk mitigation, consolidate efforts, streamline operations and enable an organization to allow the maximum acceptable level of risk to innovate and thrive competitively as a business. Information risk management examines every information domain to assess and prioritize risk factors, and then implements risk controls in a way that enables the efficient coordination of and collaboration between different information silos.

Information risk management provides organizations with a means to prioritize governance, risk and compliance activities and align them with business requirements. Effective information risk management requires four main steps:

- **Assessment** — Identify and assess the organization's information risks and the scope and impact of those risks, determine the organization's tolerance to these risks and prioritize risk mitigation in alignment with the organization's business goals and requirements.
- **Planning** — Leverage industry-standard best practices to create a coherent mitigation strategy to address the areas of risk at all appropriate levels within the organization.
- **Implementation** — Implement the plan and strategy in accordance with standard best practices.
- **Management** — Continuously monitor and measure the effectiveness of the implemented plan and strategy.

These steps feed into an ongoing cyclical process, rather than a one-time, discrete exercise. Insights gained during the management stage feed back into an ongoing assessment. To ensure IT agility and efficiency, the analysis, planning, implementation and management stages of information risk management need to be based on best-practice IT control frameworks such as IT Infrastructure Library® (ITIL®) and Control Objectives for Information and related Technology (COBIT). Once the plan is implemented, it must be continuously monitored to allow preemptive detection, analysis and reaction to threats.

Prioritize governance, risk and compliance activities

Improper risk prioritization is one of the primary obstacles to successful risk mitigation. Overemphasizing certain risks leads to wasted resources,

while underemphasizing others can have disastrous consequences. A well-implemented information risk management strategy assesses and analyzes information risk to determine ways it can potentially affect the enterprise and its value chain, such as impacts on information accessibility, communication flow, ongoing operations and workflow interactions. Understanding the scope and impact of a risk helps teams better determine where they should place their attention.

Organizations then come to realize that they need not protect against every conceivable threat, but instead, should understand and prioritize according to what makes the most sense for the business. This puts an organization in a better position to balance the needs and resources of the business with its needs for information security, information compliance, information retention and information availability.

Information security

Organizations must be able to protect and securely share information across the enterprise, as well as with their partners and customers. This includes enabling secure business collaboration with effective controls that protect intellectual property and the privacy of information, but don't slow down business processes. It means providing anytime, anywhere access to trusted information in context while ensuring the integrity, confidentiality and availability of that information whether it's at rest, in motion, in use or at an end point.

Information risk management helps assess information security priorities and risks, determine where sensitive information resides and provide a means to assess and prioritize vulnerabilities and security gaps. Based on those assessments, an organization can create a threat profile to assess its current security stance and facilitate plans to improve that stance.

A key part of designing and planning is creating an enterprise security roadmap that defines policies, processes and procedures needed to obtain the desired security stance, as well as a blueprint for the enterprise security architecture needed to support it and provide ongoing risk management. What is needed

are common solutions and services that go beyond traditional security, privacy, compliance and operational risk solutions to offer proven technologies and collaborative methods to build consistency and quality control.

Information compliance

Regulatory, industry and legal mandates for maintaining the integrity and privacy of information are continually on the rise. Unfortunately, complex audit and compliance requirements can hamper an organization's effectiveness. Organizations need sustainable compliance strategies. Information risk management helps organizations reduce the complexity and costs of security audits and regulatory compliance, while enabling them to protect against potential financial penalties and damage to their reputation.

Information risk management facilitates an overall compliance strategy that includes defining and implementing policies, processes and procedures for data encryption, records and content management, storage and archiving, retention management, change and configuration management, identity and access management, Web site auditing and in-depth network defense and system protection.

Effective information risk management leverages automated policy enforcement mechanisms and standardized compliance reporting. It provides a means for organizations to monitor user activities in relation to misuse or noncompliance, and then manage incidents using standardized, traceable procedures.

Information retention

Large organizations typically have to manage hundreds of disclosure requests every year, often with the requirement to satisfy those requests in very short timeframes. Lack of responsiveness can result in serious repercussions, including significant fines and penalties. Additionally, organizations have to manage two competing demands in terms of legal discovery – delete information to achieve operational efficiency and maintain information as long as needed to stay compliant.

Information risk management can help organizations create environments that facilitate management of these competing demands and help them respond effectively to legal, regulatory and investigatory inquiries. From early analysis and diagnosis of e-discovery readiness, through e-mail and records management, development of chronological and event-based retention policies to the enterprise-wide search and discovery analytics capabilities, information risk management can help an organization proactively reduce the risks associated with information discovery.

Information availability

An organization's information availability correlates directly with its business resiliency. Disasters can destroy vast amounts of work and data with devastating effects on business viability. However, information availability means more than just having effective disaster recovery measures in place. Five hours of downtime can be just as debilitating – and is far more likely to occur – as the effects of a hurricane or fire. Organizations must take steps to ensure users have continual access to critical information. Disruptions to availability can impede productivity, cause lost revenues, and damage customer loyalty, partner relationships, brand and reputation.

Still, organizations need to understand that not all information is created equal. Information risk management assists organizations in identifying the information that is most critical to their business, prioritizing areas such as intellectual property, financial information, human resource data and customer records. It then leverages best-practice frameworks to create and implement a comprehensive strategy for achieving the desired level of information resiliency, which can include the ability to deliver continuous and secure access to information, optimize employee productivity and stakeholder satisfaction, meet service level agreement requirements and reduce management costs.

Achieve the business benefits of information risk management

By taking a holistic information risk management approach to protecting and managing information, organizations can leverage their technology

investments across their entire enterprises in multiple governance, risk and compliance areas. Information risk management empowers organizations to create models for acceptable security and compliance infrastructures that can be easily overlaid on other segments of the business, such as new operations, branches or franchises. Information risk management enables an organization to deftly manage risk so that it can move forward, innovate and thrive competitively as a business.

Why IBM for information risk management

A vast portfolio of software, hardware and services puts IBM in a unique position to help organizations through any or all of their information risk management challenges. IBM combines deep consultative expertise and education with software, hardware and tools that have broad platform, application and resource support to protect and strengthen the resiliency of an organization's valuable information assets. Turning to IBM as a trusted partner for information risk management enables an organization to create a more flexible, robust and resilient IT infrastructure that translates into a more flexible, robust and resilient business.

For more information

To learn more about information risk management offerings from IBM, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/itsolutions/riskmanagement

About IBM solutions for enabling IT governance and risk management

IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards–based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit **ibm.com**/itsolutions/governance

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

Produced in the United States of America
December 2007

GME14000-USEN-00