IBM Makes Its Case for Leadership in Governance and Risk Management

Abstract

In May 2007, IBM announced its new initiatives for enabling businesses to solve their governance and risk management challenges. The scope of IBM products and services brought to bear on this announcement illustrates not only the comprehensive nature of the risk management challenge, but the fact that IBM understands its nature, and is well positioned to help businesses of all sizes address the challenge across multiple domains. While the market of governance and risk management tools continues to mature and present IBM with opportunities for further penetration into new and emerging technologies and approaches, the company's portfolio as it is today represents one of the most complete set of products and high-value services for addressing a spectrum of needs, from the design and development of IT services to service management, support and defense throughout the distributed enterprise. This complement of IBM strengths poses a significant challenge to other competitors seeking to stake their claim in this broad and demanding field of high significance to today's more risk-aware business.

Background

The traditional IT management domains of fault, configuration, availability, performance and security management embrace a number of technologies, but they all have one objective in common: the management of risk. This is a new way to view IT management, but it is becoming increasingly critical to the business that recognizes that risks arise in more ways than the obvious negatives of security, compliance, or business malfeasance threats. Risks to the *positive* values for which IT itself exists—the performance, availability and integrity of IT services on which critical business information and processes depend—pose just as great a threat to today's technology-centric business as other forms of risk. This is a view that increasingly resonates with many IT professionals today, reflecting the convergence of a range of priorities that are crystallizing in the integration of IT management technologies and services around the common theme of risk management.

The continuing onslaughts of threats to IT and information security, integrity and availability have played a significant and obvious role in this trend, as has regulatory compliance. Both have been high priorities in IT budgets for the last several years, requiring businesses to implement measures from business continuity planning to mandatory controls, as well as to document the effectiveness of control. The governance of IT is for many businesses a reflection of mandated corporate governance, requiring businesses not only to assure the integrity of IT resources, but to leverage IT controls in the mitigation of malfeasance or business integrity risks. The adoption of an IT control framework such as COBIT is often a response to these requirements. Yet COBIT itself goes beyond security or business integrity risks to address risks to the availability and performance of critical IT services and processes on which business viability depends. These are also objectives shared with best practices in IT service management, such as the IT Infrastructure Library (ITIL). The common interests of these guiding frameworks and practices are illustrated by efforts such as the IT Governance Institute's recent mapping of COBIT 4.0 to ITIL.

These trends illustrate the comprehensive nature of IT management as risk management. They reflect the increased priority given to the management of risks throughout the business, which include financial and business performance risks in addition to those addressable in IT. These latter risks are not, however, entirely outside the realm of IT risk management. For today's business, directly dependent on its IT and information resources, the management of risk in IT has become a central aspect of the management of risks critical to the business itself. This, in turn, is part of the business's changing perception of the value of IT, which is increasingly seen less as a self-contained cost center, and more as the nexus of shared services contributing to the performance of key profit centers throughout the business, as well as to the profitability of the business as a whole.

The fundamental relationship between IT and business risk management is reflected in the continuing advance of solutions that address IT risk as an aspect of business risk, integrating IT risk management with the policies, procedures and processes that define the systematic management of risks to the business as a whole. To the extent that risk management in IT operations and services supports critical business priorities, it may be fairly classified as strategic, not only because of its relationship to business strategy, but in the management of a risk control strategy itself.

Event

With its strong positioning as a leading business enabler backed by a wide range of technology and IT management solutions and services, IBM is in a position to play a leading role in the

evolution of strategic IT governance and risk management. In its May 2007 launch of its Governance and Risk Management initiatives, IBM has showcased not only a significant awareness of the distinctive differentiators it brings to bear on meeting the governance and risk management challenge in IT, but also the value of products, services and acquisitions that have built up a credible portfolio in multiple domains of IT risk management over many months and years.

Central to this initiative is the IBM Tivoli portfolio of Service Management solutions for managing risks to critical IT services. Built on a solid foundation of integrated management solutions consistent with IT Service Management best practices, this solution family also includes fundamental risk controls such as identity and access management, configuration discovery and control, event management, and risk reporting. It has been augmented with key acquisitions such as that of Internet Security Systems, a leading vendor of IT security products and services, and is supported by strongly differentiated assets in IT system design and implementation, in the Rational and WebSphere product families. More than a simple rehashing of the product portfolio, IBM's initiative demonstrates how these assets, supported by the company's well respected global services and risk intelligence organizations, work together to systematically address a range of risk management priorities, from IT service risks to security, governance, and regulatory compliance.

Key Ramifications

With this comprehensive initiative, IBM is making a compelling case for its credentials for leading the evolution of IT governance and risk management. Its broad range of technology and service assets are all strengths, but what the initiative also makes quite clear is that the integration of these assets in a comprehensive risk management strategy requires an equally significant pedigree in services—and not just for the integration of risk management tools. Many businesses increasingly see the outsourcing of risk management in areas such as security as a viable alternative to the acquisition and maintenance of tools and expertise in such highly demanding domains. Even before the sequence of acquisitions that solidified IBM's current risk management portfolio, the company maintained one of the world's most highly respected professional services organizations. To this it has added the services and risk intelligence resources of Internet Security Systems, which complement the role of IBM as service provider to many of the world's leading enterprises. At the same time, IBM has not neglected the small to midsized business, with offerings such as its Tivoli Express lines that offer key risk management capabilities such as identity and access management to this market.

This represents a significant challenge to other enterprise leaders poised to play an equally competitive role in the management of risk in IT. With their substantial footprint in enterprise application platforms that serve broad aspects of the business, companies such as Oracle and SAP may also be expected to have a significant impact on the development of IT governance and risk management. Others that have a significant presence in key aspects of IT risk, from infrastructure management to security, can be expected to have an impact on the evolution of the governance and risk market. This includes companies from Cisco to McAfee and more direct competitors among leading management vendors such as BMC, CA and NetIQ. Among these, Symantec—particularly with its recent acquisition of Altiris, which gives it a substantially more significant presence in IT management—is poised to complement its security leadership with leadership in the comprehensive management of IT and IT risks. Microsoft is yet another industry leader whose potential in the risk management market has recently been highlighted, not only by the convergence of its Forefront security portfolio with its System Center management resources, but by its partnership with expertise in IT governance and risk management with vendors such as Brabeion.

Some of these competitors have greater strength in what they offer to the small to midsized business, others in the enterprise. Most have offerings that address both, or which span the truly distributed business that manifests characteristics of both the large enterprise and the small or midsized concern. When it comes to the integration of enterprise IT resources and services, however, few have the *gravitas* of IBM. It is this presence, combined with IBM's systematic acquisition and integration of assets, that represent the company's greatest potential as a competitor in IT governance and risk management, and as a leading influencer of its development.

EMA's Perspective

The management of risk is not something that can be defined by the implementation of a few key products or technologies. It is itself a process that involves systematic assessment of baselines and gaps, planning and implementation of risk controls, monitoring and management, and the measurement of success that informs the continuous improvement of risk management. This does, however, highlight the strengths that could give IBM disproportionate influence over the evolution of comprehensive risk management in IT.

Some of the most significant of these strengths include:

- IBM's extensive Service Management portfolio, which offers a comprehensive and integrated approach to the enterprise as a whole. This speaks to the fundamental value of risk controls, from essentials such as identity

and access management to the integrated values of the Configuration Management Database (CMDB). The CMDB provides a comprehensive inventory not only of IT and information assets, but of their interrelationships and dependencies critical to a realistic assessment of risk. The CMDB also plays a highly valuable role in maintaining control of the risk posture, by enabling the interoperability of risk management solutions in multiple domains. This interoperability is critical for delivering a timely and effective response to risk events. IBM's development of its Tivoli Configuration and Change Management Database (CCMDB) has played a leading role in the company's Service Management initiatives.

- The ability to establish risk priorities and manage risks based on an assessment of their criticality is key to effective risk management. Insight into business service dependencies therefore has high value; an issue that poses risk to a critical business service dependency should be given a higher priority. Once risks are identified, the success of a significant reconfiguration required to improve the risk posture depends on visibility into the impact of change on critical dependencies. This is where IBM assets from the Tivoli Business Service Manager to the Tivoli Application Dependency Discovery Manager (TADDM), gained through the acquisition of Collation and a key enabler of IBM's Service Management strategy, play a leading role.
- This also illustrates the importance of risk monitoring—particularly the ability to correlate and identify genuine risks from seemingly unrelated events or outright noise. Such capability is critical to the timely, accurate and effective deployment of effective risk control throughout the business—from the data center, throughout the network, and to the distributed endpoint. These capabilities give risk professionals visibility into, and control over, the comprehensive risk posture as it really is. They also support "audit-worthy" reporting on the effectiveness of risk controls. IBM has brought together multiple assets—products as well as services—in risk event and information management, correlation and control to address these challenges, in its own organically developed solutions as well as in acquisitions, from Internet Security Systems to Micromuse to Consul.
- The documentation of risk controls and processes also includes the ability to maintain accurate and reliable records of risk priorities, policies and procedures developed in accordance with best practices. "Audit-worthy" evidence of control effectiveness and records of change evaluation and authorization are also critical to effective governance and risk management. This speaks to the value of document and content management in risk, supported by IBM not only through risk information management systems such as Tivoli Compliance InSight Manager, but also through IBM storage and information management systems, and acquisitions such as FileNet.
- The assurance that the business can withstand an event that threatens the viability of the business itself has become a significant focus of risk management. IBM information and storage management systems play a significant role here as well, both in assuring the day-to-day availability of information resources, as well as assuring business continuity. Continuity is more than simply assuring data resilience, however. IBM Service Management resources also help assure that the business can recover critical IT services as well as information in the event of damage or loss.
- Not coincidentally, the long list of IBM acquisitions also illustrates an important value in a major vendor seeking to lead in the management of risk—because the challenge involves multiple domains, the ability to integrate acquisitions is key. IBM's generally positive record of integrating its acquisitions into a compatible and comprehensive portfolio will therefore serve it well in coordinating the management of risk on multiple fronts.

Risk management is more than a technology integration exercise, however. Risk also involves human perceptions and interactions, which requires skill in leading and building consensus on risk priorities and cooperative processes. It also requires the management of processes which are themselves vital controls on risk in IT. In terms of technology, examples of IBM strength in these areas include the company's Rational line, for risk mitigation through the modeling and development of IT services and applications, and for the management of the portfolio of multiple projects that make up a comprehensive risk management initiative. In terms of services, IBM service organizations are well poised to aid their customers in implementing risk management best practices.

In terms of day-to-day operations, however, this is a domain in which technology has evolved to automate governance and risk process management, and IBM will need to take note of the market of solutions that automate workflow and processes for establishing risk priorities through survey and consensus, definition of policy, and articulation of risk control procedures. This is workflow that goes well beyond the service desk, purpose-built for governance and risk management, and is not today addressed as comprehensively by IBM products—nor, for that matter, by

many of IBM's major competitors. EMA believes IBM will likely consider and evaluate its opportunities in this market, which has seen its second generation of evolution, and is now entering its third with emerging vendors such as Agiliance and Brabeion that integrate the automation of control procedures with control monitoring, validation, and reporting that incorporates more sophisticated approaches to IT risk analytics. Other technologies that currently play a role in IT risk management—and which either presently are, or in the future could be, candidates for IBM partnership or acquisition—include change control and audit, transaction governance, and emerging technologies in application and database security.

Metrics suggest the role that domains such as business intelligence (BI), decision support, and enterprise performance management can be expected to play as governance and risk management matures. The mitigation of risks to business strategy is integral to the definition of "strategic" risk management. Objective metrics provide decision support in many other domains of business, but the evolution of IT risk metrics is still in its early stages. Its development is further hampered by the dominant influence of unpredictable human actions such as security threats or business malfeasance on the part of insiders, partners or customers. These unpredictable human actions limit the ability to apply risk measurement disciplines that have their roots in the measurable probability of events such as acts of nature. In order to measure risk in a way meaningful to a *specific* organization, the business needs tools that lend themselves to flexibility in risk data analysis, which can help businesses evolve the set of analytics and measurements most meaningful to them.

BI and related technologies can therefore be expected to play a role in the evolution of IT risk analytics as the domain matures. Here too, IBM has shown interest in vendors such as Cognos, but IBM's competitors in enterprise risk management, particularly in the enterprise application space, have already begun to acquire leading vendors, as with Oracle's acquisition of Hyperion, that may influence the evolution of the competitive governance and risk management landscape. The development of IBM's governance and risk management strategy may therefore play a role in whatever direction the company takes in BI and decision management in the future.

But these should be seen more as opportunities for IBM, which has already elaborated a more complete portfolio of IT technologies and services it can bring to bear on risk management than many of its competitors. The fact that IBM has consistently and carefully brought together this portfolio over the last several years itself illustrates that IBM understands the methodical nature of risk management, which should embrace both proactive and reactive measures that are equally well thought-out. This suggests just how significant a role the company is poised to play in the further development of the governance and risk management marketplace, as the management of business risk in IT continues to grow more important, more sophisticated and more valuable to senior executives and operations professionals alike.

Enterprise Management Associates
Phone: 303.543.9500, Fax: 303.543.7687
www.enterprisemanagement.com
1341.052207