

Integrating GRC with Performance Management Demands Enterprise Solutions

by Lee Dittmar, Principal, Deloitte Consulting LLP and Peter Vogel, Senior Manager, Deloitte Consulting LLP

Why discrete “tools” are giving way to architected, platform-based strategies that integrate the management of performance, risk, and compliance.

Unnecessary complexity is the bane of business. Risks are becoming more diverse and interrelated; laws and regulations are becoming more complicated; and boards and executives are becoming more accountable for governing the management of performance, risk, and compliance. The activities and controls associated with governance, risk, and compliance (GRC) have expanded accordingly, becoming extraordinarily complex themselves.

Information Quality Isn't Where It Needs to Be

A significant consequence of complexity is poor information quality and the inability to get relevant, accurate, and reliable information to the right place at the right time. Information quality is a ubiquitous challenge — one that consistently arises both in the field and in formal research. For instance, CFO Research Services in collaboration with Deloitte Consulting LLP (Deloitte Consulting) embarked on a survey program in 2005 that illuminated the pervasiveness of poor information quality (IQ) in today's enterprises. The resulting report, entitled IQ Matters, noted that a majority of respondents don't have ready access to high-quality, reliable, useful information on operating and financial performance at their companies.¹ Queried on ten categories of IQ — combinations of the utility, timeliness, and accuracy of financial and operating information — a majority of the senior financial respondents reported room for improvement in every category.

A recent follow on to that study, entitled Look Closer, Look Further, determined that, a full two years later, the needle has still not moved much in a positive direction.² While companies do well at mandated information management activities, such as reporting financial results, it appears they still struggle to produce the timely, accurate, and insightful information needed for strategic planning, supporting board oversight and governance, making investment decisions, and identifying, monitoring, managing, or mitigating

risks. For instance, a near majority, 47 percent of the 443 senior finance and IT executives surveyed, reported that their companies struggle to produce and develop the desired quality of information needed to make good business decisions.

Clearly, companies need to do a better job of generating information that accurately reflects performance and enables more effective management controls — especially since executives are keenly aware of the relationship between better information quality, more efficient and effective GRC, and enterprise value. Eighty-one percent of IQ Matters survey respondents reported that they believe better information can improve profitability; 82 percent reported that they believe it can reduce costs.

These findings beg the question: If so many companies are aware of the risks and rewards, why haven't they done more about it? In response to a recent Deloitte webcast poll conducted in August 2007, 60 percent of respondents reported that a significant barrier is “competing priorities,” which we interpreted as meaning that resources are being channeled into areas that are perceived to be even more pressing. Another and perhaps even more-formidable obstacle, however, is that for a long time the technologies weren't up to the challenge. Consequently, we believe some executives today incorrectly assume that implementing individual solutions for each specific problem is the only option and that taking an enterprise approach is too hard, too expensive, or just not possible. While this perception still lingers, technological advances have dramatically changed the reality. Today, while an integrated, enterprise approach to GRC and performance management is a lofty undertaking, it's not an unassailable challenge.

¹ IQ Matters: Senior Finance and IT Executives Seek to Boost Information Quality, A survey report prepared by CFO Research Services in collaboration with Deloitte Consulting LLP, November 2005.

² Look Closer, Look Further: How to Build a Better Business Case for Improving Information Capabilities, A survey report prepared by CFO Research Services in collaboration with Deloitte Touche Tohmatsu, October 2007.

Governance: Integrating the Management of Performance, Risk, and Compliance

Within most organizations today, information quality is a pervasive problem, and information and controls related to compliance and risk management are still mainly manual and fragmented. While executives are increasingly looking to technology to help meet these needs, most companies simply don't have the IT assets in place to efficiently and effectively turn data into information. In addition, the technological assets they do have are not being adequately used to enable governance, risk management, compliance — or performance management. In short, there is more than just room for improvement; there is a growing imperative to fundamentally change course.

The days of dealing with risk management and performance management in a disjointed and disconnected fashion are rapidly coming to an end. We believe a new approach is needed in order to meet increasing demands for board and executive accountability, achieve cost-effective compliance with ever-mounting regulatory requirements, and manage more effectively the balance between opportunity and risk. The trends are clear. Organizations of all kinds are increasingly being judged by their ability to demonstrate good governance through a transparent, measurable chain of accountability to multiple stakeholders. Good governance demands that the management of risk and compliance can no longer live separate lives from the management of performance.

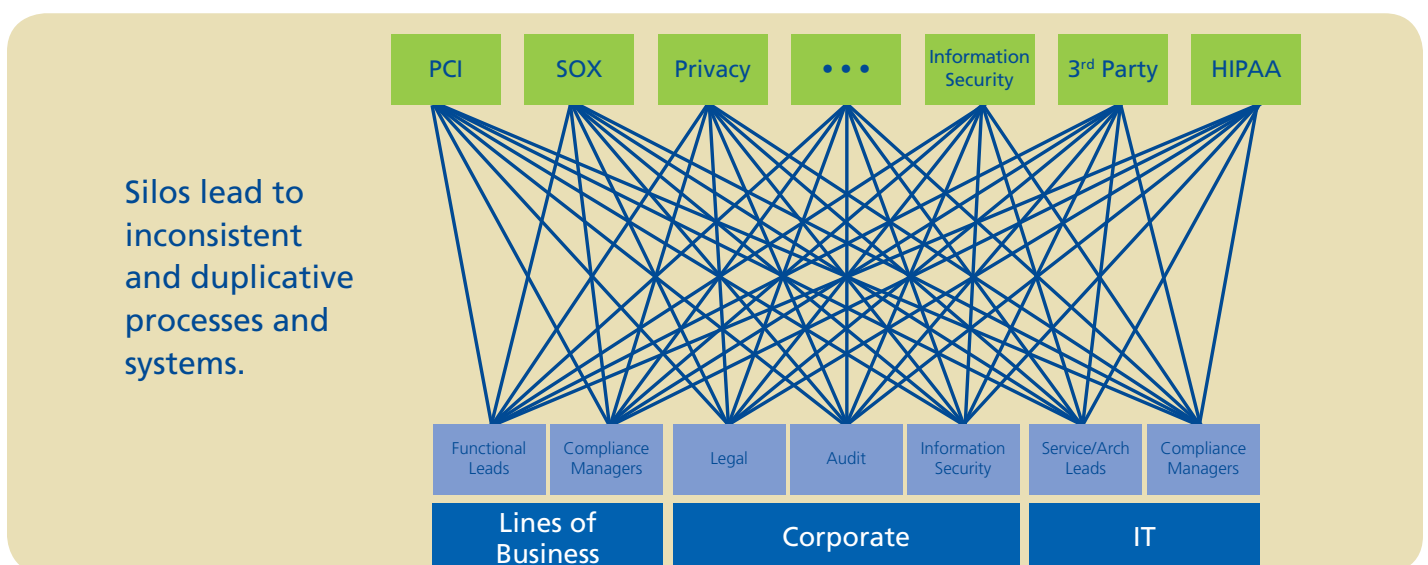
A fundamental premise is the need for an integrated enterprise approach. Risk management must be incorporated into everyday decision-making and baked into core business processes at strategic and operational levels. This means that common information, processes, controls, and systems must be leveraged to simultaneously improve the effectiveness of decisions and produce significant efficiencies and cost savings.

An enterprise perspective is necessary to overcome business-unit, functional, geographic, process, and technology silos. Leveraging common information, processes, and systems, when done right, is more efficient and effective — enabling better recognition, understanding, and monitoring of risks and management of performance.



The Role of Information Technology

We believe that achieving an integrated, enterprise approach to GRC and performance management depends heavily on leveraging information technology. It is not optional. And when it comes to IT for GRC and performance management, there is no single “killer application.” The solution will need to be architected from a portfolio of applications, leveraging existing and new IT assets. Moreover, an effective strategy demands an enterprise platform and extension of and integration with core business systems. It is no longer about discrete, decentralized tools, which produce the complexity illustrated below. An integrated, enterprise technology platform is essential to overcoming silos. This is why SAP's emphasis on Performance Optimization —integrating performance management, GRC, business intelligence, and analytics — should be viewed as more than simply an expansion into new software categories.



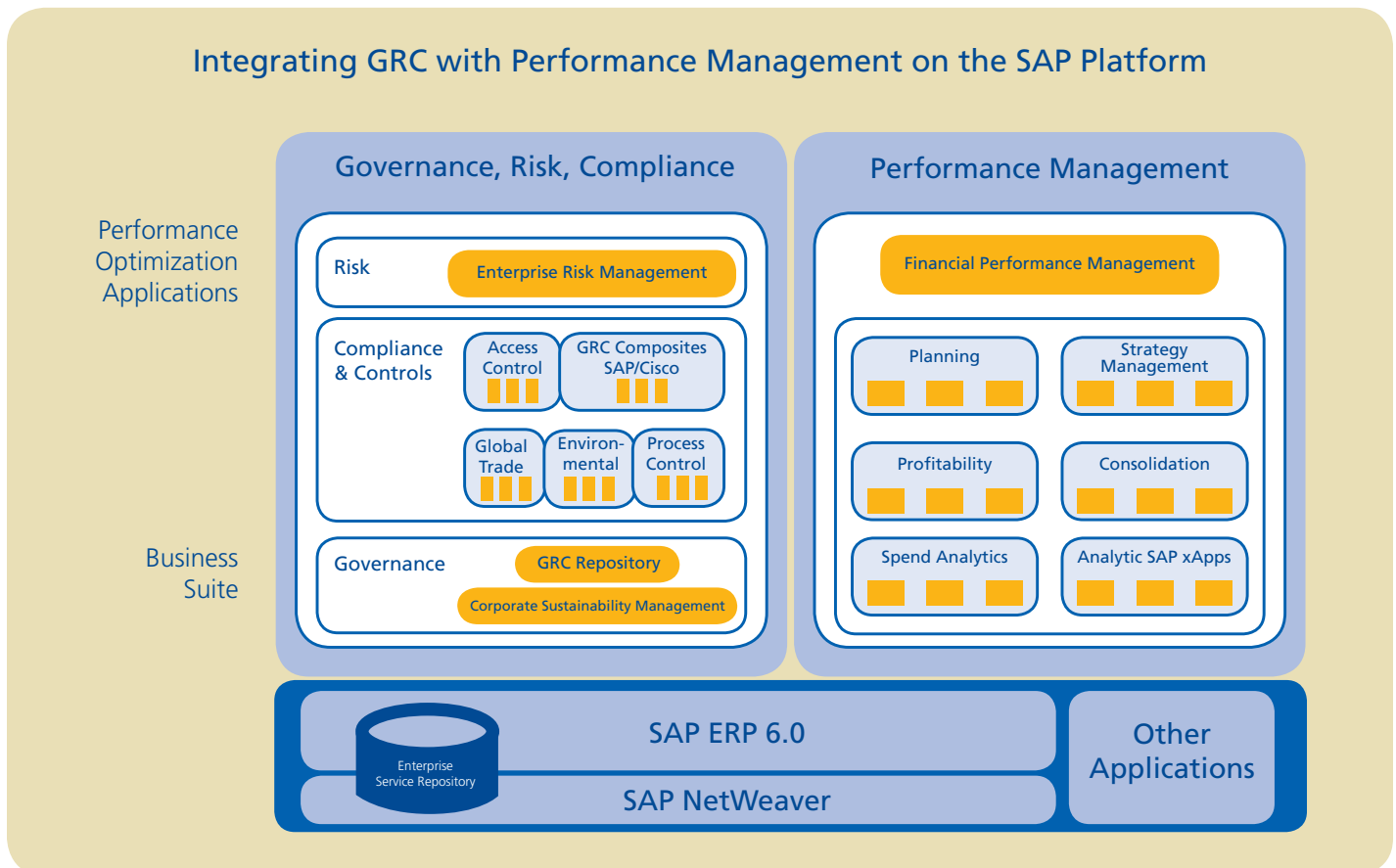
Integrating GRC: A First Step

As an example, SAP's portfolio of GRC applications includes SAP GRC Risk Management; SAP GRC Process Control; SAP GRC Access Control; SAP GRC Global Trade Services; and SAP Environment, Health & Safety (SAP EH&S). The delivery of related GRC business intelligence and analytics is also an integral component of the overall solution roadmap.

Together, these solutions provide the ability to help a company:

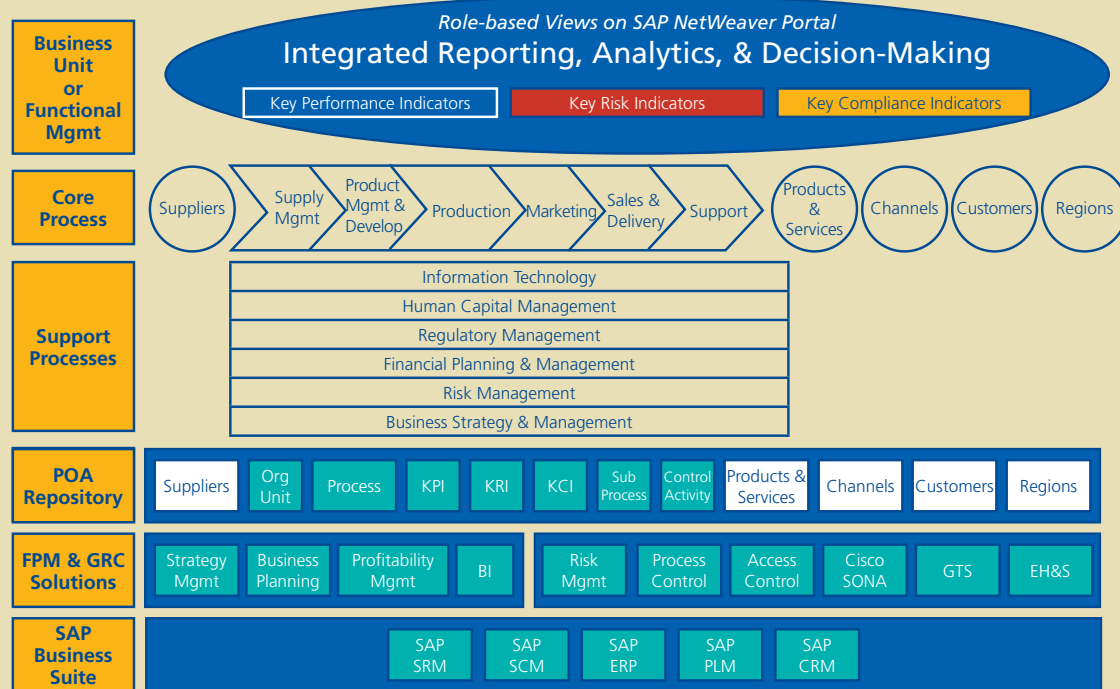
- 1) Identify, assess, mitigate, and manage enterprise-wide risks that potentially jeopardize strategic, financial, and operational performance objectives
- 2) Manage regulatory compliance (and the risks of non-compliance) with Sarbanes-Oxley (SOX), environmental laws and OSHA, customs and international trade regulations, and IT security.

The expectation is that these types of solutions and applications will eventually share a common repository — enabling shared data and business intelligence, actionable analytics, and event management. This is important because meeting regulatory requirements and managing risks that threaten performance can often be addressed by common controls within operational processes. The advent of SOX forced companies to formally document and acknowledge enterprise-wide definitions of a company's collective business processes. There are overlapping requirements and many common controls across SOX, FDA, and HIPAA. Diverse regulations often impose common requirements — *that can and should be addressed by common (not redundant) controls*. Identifying and managing diverse business risks also demands an in-depth understanding enterprise-wide business processes, activities, and controls.



Recognizing these commonalities highlights the significance of an integrated enterprise approach. By mapping requirements to controls, a measurement framework can be established to continuously monitor the effectiveness of processes, activities, and controls in managing specific risks and complying with specific regulatory requirements. In this way, key risk indicators (KRIs) and key compliance indicators (KCIs) can take their rightful place alongside key performance indicators (KPIs) — enabling more comprehensive management reporting and analysis, more integrated and effective decision-making, and a more executable strategy. This construct is illustrated in the graphic below and described further in the following section.

Integrating the Management of Performance, Risk, and Compliance



Integrating GRC with Performance Management: Truly Integrated Performance Management

To continue our example, SAP has acquired and continues to develop Financial Performance Management (FPM) solutions. These efforts are providing companies with capabilities and enable the closed loop of performance management, which encompasses strategy development, planning and budgeting, monitoring execution, adjusting the plan, analyzing profitability, and assessing performance. SAP's strategy, planning, and profitability management solutions — when combined with integrated GRC, business intelligence, and analytics solutions — are aimed at delivering truly integrated performance management.

The integration of GRC with performance management — at the corporate, strategic, and operational levels — can provide far greater insights and capabilities for protecting and growing value than standalone FPM or standalone GRC approaches. Truly integrated performance management includes and enables the following:

- 1) In the "Business Strategy & Management" process, the development of strategic and operational plans should include the identification and assessment of risks to short- and long-term objectives and plans. Interfacing with the "Risk Management" process to assess the vulnerability and impact of risks inherent to alternative strategies is integral to scenario analysis. Additionally, prioritizing inherent risks may demand risk mitigation tactics that will need to be factored into the annual plan and budgeted for during the "Financial Planning & Management" process.
- 2) The corporate "Risk Management" process should set risk appetite for the organization as a whole, cascading risk tolerances (and related risk management guidance) into planning and performance management processes throughout business units and functional areas. Those who support this process should assist the CFO, business units, and functions with developing appropriate key risk indicators (KRIs) relative to performance objectives and KPIs.
- 3) The CFO-driven "Financial Planning & Management" process should translate the strategic business plan into annual target-setting, revenue projections, and budget development for the upcoming year. Increasingly sophisticated FPM technology can enable plans and budgets built around a company's enterprise-wide business processes, which extend across organizational silos. Recall that these are the same enterprise-wide business processes to which key financial controls are already linked. Planning and management based on enterprise-wide business processes can provide a unifying framework for linking strategic objectives, KPIs, targets, budgeted resources, and recording and tracking of actuals, KRIs, and key controls. The adoption of a planning and management framework, based on the allocation of resources to business processes, encourages necessary collaboration across organizational units. By design, a process-based framework captures resource usage, costs, and other key business indicators that enable an easier path to activity-based costing and profitability analysis. The constructs of these sophisticated analytical approaches are built-in rather than being accomplished through an after-the-fact snapshot assessment.

- 4) The “Regulatory Management” process(es), in addition to supporting and aggregating routine reporting to regulators, has much the same objectives as the “Risk Management” process (albeit specific to compliance with particular regulations and the risks of non-compliance). Compliance objectives, key compliance indicators (KCI), associated activities and controls must be recognized as boundaries within which companies must operate in pursuit of performance objectives. In many cases, the same activities and controls that are necessary to comply with a regulation, such as SOX, are also effective business practices that can have a positive effect on KPI targets, e.g., cost controls contribute to profitability. The role of those responsible for regulatory management processes should extend to assisting the CFO, business units, and functions with developing appropriate KCIs relevant to their operational business processes. The majority of the responsibility for, and costs of, compliance occurs within core operational processes. Accordingly, identification of KCIs, KCI targets, and the cost of compliance must be factored into plans, budgets, and management accountability at all levels of the organization.

While the preceding is not a comprehensive illustration, it should be clear that the starting point for integrating GRC with performance management is seamlessly integrated planning processes that evaluate and balance the pursuit of strategic and financial performance objectives within the guidelines and constraints of risk and compliance objectives. KPI targets, pursued within the boundaries set for KRIs and KCIs, emerge from this integrated planning approach.

We believe an organization that adopts a planning framework that treats enterprise business processes as one of its key planning dimensions will achieve far greater transparency and visibility into the activities that drive performance. A business process planning and management framework can enable these key business indicators (KPIs, KRIs, and KCIs) to link strategy and execution. Cascading these key business indicators to core operational processes (Supply Management, Product Management & Development, Production, Marketing, Sales & Delivery, and Support) can enable the integrated management of performance, risk, and compliance throughout an organization.

Deloitte and SAP

Deloitte Touche Tohmatsu (DTT) Member Firms and SAP are working together to offer services and solutions that better integrate GRC with performance management. Together, we are collaborating to help companies in their efforts to create and preserve value through integrated management of performance, risk, and compliance. This includes assisting companies in their efforts to achieve risk intelligent planning, decision-making, and performance management throughout their organizations. In addition to an award-winning line of SAP consulting services, DTT Member Firms bring a unique combination of consulting services including Strategy and Operations, Risk Management, Tax, Financial Advisory, Human Capital, and Technology Integration. They also focus on several industries including Consumer Business, Technology-Media-Telecommunications, Life Sciences, Financial Services, Energy, and Aerospace and Defense.

This publication contains general information only and is based on the experiences of Deloitte Consulting LLP practitioners. Deloitte Consulting LLP is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Consulting LLP, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

www.deloitte.com

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms have any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names “Deloitte,” “Deloitte & Touche,” “Deloitte Touche Tohmatsu,” or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu. In the United States, services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP, and their subsidiaries), and not by Deloitte & Touche USA LLP.