



GOVERNANCE, RISK & COMPLIANCE

Survival of the Most Informed: GRC Comes of Age—How to Envision, Strategize, and Lead to Achieve Enterprise Resilience

ADVISORY



Introduction

As the business and regulatory environment continues to evolve, organizations are operating in a world in which traditional strategies and assumptions are failing. In both the short and long term, companies that succeed will be those that can demonstrate resilience—the ability to drive business performance and achieve regulatory compliance in an environment in which these two outcomes must be managed strategically and with agility.

In these circumstances, the “new normal” is nothing like business as usual. Organizations today face ongoing challenges to their old assumptions, and they can no longer rely on history to predict the future. Their business cultures were tested during the economic downturn and too often failed to guide behavior or support sound decision making. Siloed approaches to assurance (including risk management, internal audit, and compliance) meant leaders could not necessarily trust the value of business intelligence. Undisciplined governance efforts exacerbated these problems and often led to false comfort and inadequate oversight.



As the economy begins to recover, the need for cost cutting continues, and increasingly complex business risks are creating new pressures. Boards of directors are facing new stakeholder demands that they be accountable for their organizations' governance systems and business success. They can expect independent challenges from shareholders, unprecedented regulatory scrutiny, and new criteria for board performance.

Management, in turn, is being asked simultaneously to enhance oversight and transparency as well as drive performance and profitability. To survive and succeed, organizations need to address the challenges in business culture, and determine how to rationalize and better balance their assurance efforts to ensure strong governance, risk management, and regulatory compliance.

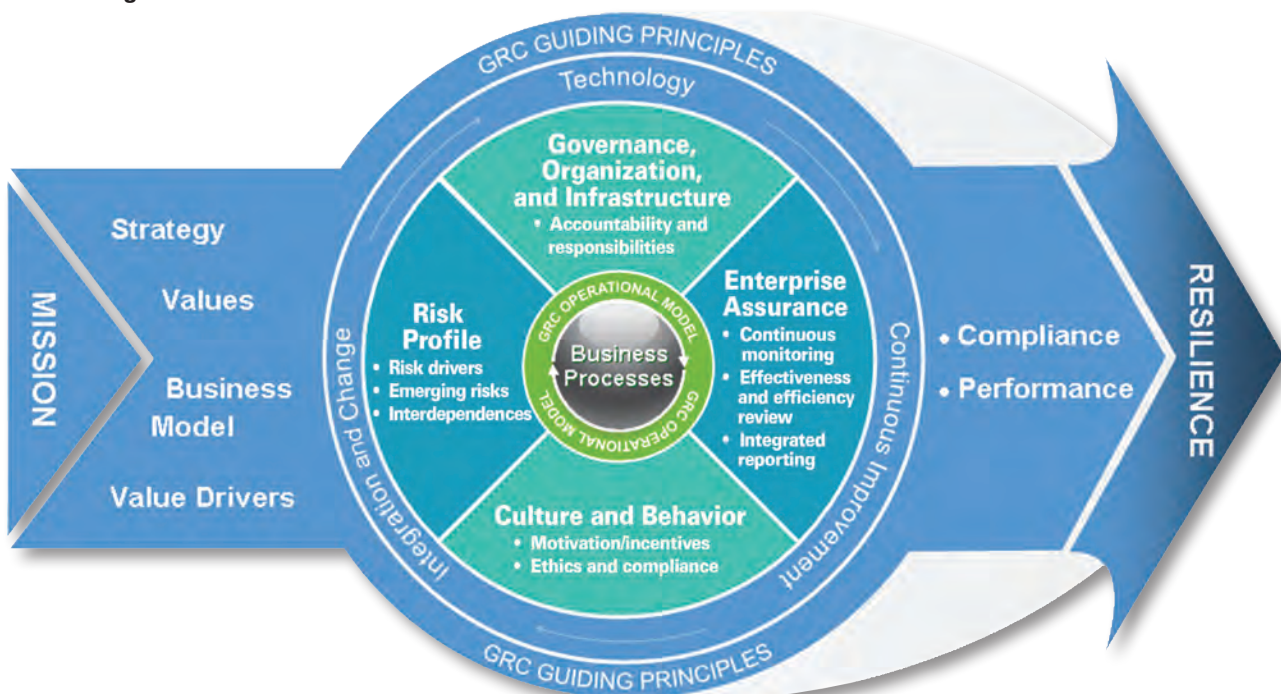
Some organizations may respond to these challenges in a piecemeal or uncoordinated manner because many demands are competing for management's time and available resources. The result would be a patchwork of risk management and compliance processes that may actually increase the risks and costs associated with these activities. Eventually, these processes will need to be rationalized. Otherwise, leaders will likely be left with a false sense of security and a limited ability to control risks, manage change, and drive business value—and the board is left essentially unable to discharge its responsibilities.

Survival of the Most Informed

An alternative is to architect an enterprise model that would bring together complex and disparate risk and compliance activities and would direct these efforts more efficiently, in alignment with corporate strategy and supported by organizational culture. Such a model would enhance communication to help leaders gain intelligence and insight into what they may not know now, even if they have enterprise risk management (ERM) and robust compliance processes in place. It would instill agility into critical governance efforts, point the way to emerging risks, and help clarify the organization's strengths and weaknesses so leaders could take advantage of this knowledge in their strategic planning and be better prepared for ongoing change.

To create this model, organizations need a simple yet disciplined approach. The goal is to balance equally important efforts to optimize risk, strengthen culture and behavior, enhance governance, organization, and infrastructure, and ensure enterprise assurance. The result would be an increasingly resilient and informed organization, one whose leaders drive business value from efforts to improve performance and achieve compliance.

Introducing KPMG's GRC Holistic Model®



Source: KPMG LLP, 2009

GRC Comes of Age

In this environment, a holistic approach to governance, risk, and compliance (GRC) can serve as the model that leaders are looking for—the compass that can help them navigate “the new normal” in the short term and thrive in the decades ahead.

Although often considered in the context of a technology tool, GRC is in fact a means of driving maximum value out of the business model. It is a strategic approach to rationalizing risk management, controls, assurance structures and processes, and intelligent use of IT and data management structures supported by a strong organizational culture—ultimately, to deliver performance and compliance and enable enterprise resilience.

How to Envision, Strategize, and Lead to Achieve Enterprise Resilience

This white paper suggests why the most informed leaders will be best prepared to survive and succeed in the new normal, and how GRC can help them achieve those critical survival goals. It describes the benefits of creating a GRC enterprise architecture, tied to corporate strategy and mindful of unique business culture, and explains how a holistic approach to GRC can help leadership respond to ongoing external and internal challenges and develop new resilience as the business and regulatory environment continues to evolve.

10 Questions for Leaders:

Do You Have the Vision, Information, and Capabilities to Achieve Resilience?



1. Does the company have executive leadership for a GRC strategy and guiding principles that is closely tied to performance?
2. Are the roles and responsibilities for GRC formalized in a clearly defined manner?
3. Are changes to the risk and regulatory environment captured in GRC processes?
4. Is the degree of enterprise risk being taken in pursuit of returns understood and communicated?
5. Is technology leveraged or are there plans to do so?
6. Has an effective ethics and compliance program been established to promote right behaviors within the organization?
7. Has a well-defined structure for assurance been established?
8. Is there a coordinated assurance plan that provides independent monitoring and a forum to challenge effectiveness across the GRC spectrum?
9. Do board members understand the potential impact of GRC failures on all stakeholders?
10. Is an early-warning system in place that rapidly informs management and the board of impending concerns?

The Value of Resilience

In this environment, resilience is the key to organizational survival, and GRC is the key to driving resilience. A holistic GRC model helps enable organizations to protect and enhance business value by:

- Aligning GRC to organizational strategy and mission
- Supporting informed decision making driven by robust governance structures, level-appropriate reporting dashboards, and intelligent use of IT and data management based on a set of agreed-upon guiding principles

- Enhancing consistency, transparency, and operational efficiency by rationalizing overlapping risk management efforts, controls, and assurance structures and processes through a common set of risk taxonomy, issues management, and reporting processes
- Supporting an efficient response to the challenges posed by evolving risks and rapidly changing regulatory requirements based on consistent and timely analysis of risk drivers

and performance metrics from business functions including the operations, finance, compliance, and regulatory teams

- Fostering a culture that understands and embraces GRC as a source of competitive advantage
- Orchestrating the four intrinsically linked components—the enterprise risk profile, culture and behavior, governance, organization, and infrastructure, and enterprise assurance

The convergence challenge – Survey Highlights 2010

- The EIU/KPMG LLP survey emphasized that companies have an appetite for the convergence of governance, risk, and compliance. Almost two thirds (64 percent) of survey respondents say that this is a priority for their organization, driven by business complexity, a desire to reduce risk exposure and a need to improve corporate performance. The top four factors influencing this growing interest are overall business complexity (44 percent), the desire to reduce the exposure of their organization to risk (37 percent), a need to improve corporate performance (32 percent), and concern about avoiding

ethical and reputational scandals (32 percent).¹

- The same survey found that the executive management team and regulators are exerting the greatest pressure on organizations to improve their convergence of governance, risk, and compliance functions. They also said work remained to be done before companies achieve full integration of GRC across different areas and regions. Of those surveyed, only 11 percent reported full convergence across geographies, 12 percent across business strategy, 14 percent across business units, and 14 percent across oversight functions.¹

- In addition, people—not technology—present the greatest barrier to successful convergence. Integration is likely to involve a major transformation program, so, perhaps not surprisingly, resistance to change is considered the single biggest obstacle (44 percent), followed by complex convergence processes (39 percent) and a lack of available experts (36 percent). Less than one in ten mentioned technology as a hurdle to overcome.¹

¹ “The convergence challenge” – Global survey into the integration of governance, risk and compliance, January 2010, KPMG International, in co-operation with Economist Intelligence Unit

Envision Enterprise Resilience: The GRC Foundation

Organizations need to ensure that their governance, risk, and compliance management processes evolve to keep pace, anticipate growth, and support efforts to effectively drive organizational resilience.

Leaders must undertake these efforts in an environment in which much is unknown. Long-time assumptions about how to operate, where to obtain capital, where to invest and expect returns, what to expect from customers and suppliers—so many of these variables remain in flux and are being influenced by new stakeholder expectations.

To become resilient to the instability these changes will drive, organizations need a structured process to enable them to consider each emerging factor and its interrelationship with others. With this foundation, companies can make effective decisions without having to know, precisely, how business and economic circumstances could evolve. The GRC architecture would create a more nimble organization, flexible in accommodating change, and help position it to take advantage of emerging opportunities.

Enabled by a comprehensive model for evaluating risks in the context of strategy from the perspectives of the business, regulatory and legal compliance efforts, organizations can take steps to (1) address their stakeholders' focus on governance and risk management, (2) enhance economic business value by improving cost efficiencies, (3) capitalize on evolving opportunities, and (4) minimize losses.

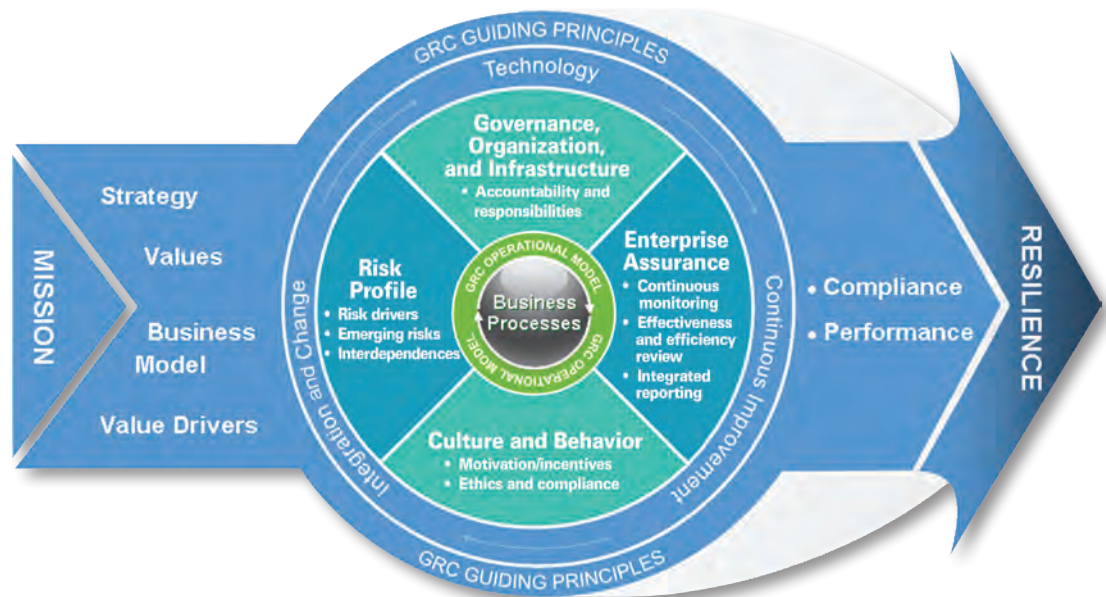


Strategize and Make Choices: KPMG's GRC Holistic Model[®]

Implementing GRC effectively requires a clearly supported vision by the management team. This vision sets the tone for the organization's culture and strategy, and it provides the discipline needed to implement a sustainable process and a flexible technology solution that interfaces with existing systems and processes. Such technology serves as the backbone of an effective risk/compliance architecture, providing timely access to consistent, accurate, and comprehensive information as well as intelligent reporting.

KPMG's holistic approach to GRC is depicted in the model shown in **Figure 1**.

Figure 1: KPMG's GRC Holistic Model[®]



Source: KPMG LLP, 2009

As the compass for an organization's risk and compliance activities, the GRC Holistic Model offers a framework to unite and direct processes to support corporate strategy, allowing the specific components of governance, risk management, and compliance to be evaluated and targeted for reengineering in a modular manner.

The GRC Holistic Model does not propose a centralized approach to risk management. Rather, it recognizes that risk is often managed closest to the point of origination—specifically, the business line and business processes, which are operated by people who know the related risks. The model provides a structure for aligning risk management and compliance activities with governance efforts, organizational culture, and enterprise assurance and reporting. Thus, the model supports a multitude of board and management needs while providing valuable feedback to the strategic decision-making processes. Resilience is not an end-state, but a goal of a continuous process driving improved compliance and performance even in the most challenging environments.

The model begins with efforts to link GRC with the mission of the organization—a critical foundation for the overall approach. As depicted in **Figure 1**, the mission is then translated into the organization's strategic objectives, which cover elements such as:

- **Strategy:** What do we want to achieve?
- **Values:** What do we stand for?
- **Business model:** How do we organize?
- **Value drivers:** What factors are influencing organizational success?

These foundational elements determine the parameters for GRC within the organization and give guidance to the other tactical and operational elements.

The Business Processes

The business processes are at the core of the organization and the GRC Holistic Model. They include processes such as research and development, sourcing of materials, manufacturing of materials, processing of transactions, accounts payable and receivable, procurement, vendor management, and similar functions.

The business processes should have:

- Embedded controls aligned with the risk profile, which is defined based on the strategic objectives.
- Comprehensive reporting capabilities to enable enterprise assurance and strategic decision-making.

Surrounding the business processes is the GRC Holistic Model, the layer at which the governance, risk management, and compliance management is put into practice to drive enterprise assurance. The GRC Holistic Model includes activities relating to the design, implementation, and evaluation of controls within business processes including leveraging information systems and technology to assess the effectiveness of controls.

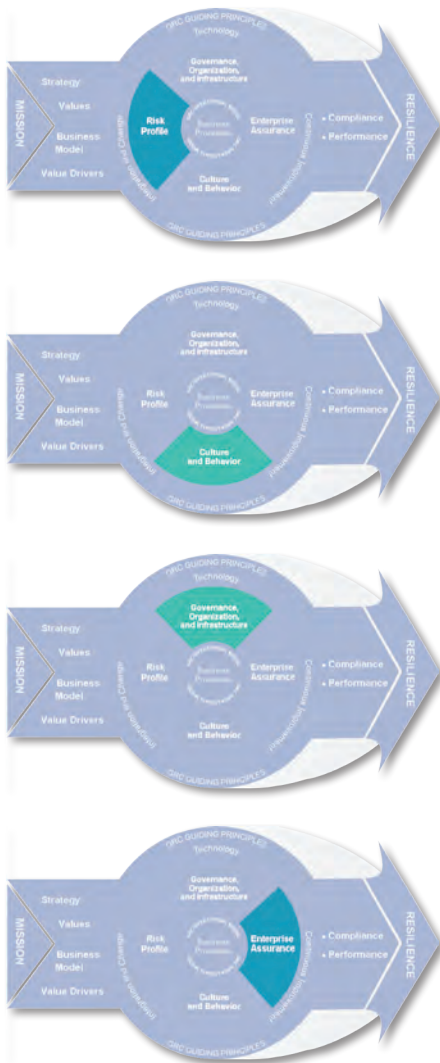


Strategize and Make Choices: KPMG's GRC Holistic Model[®]

(Continued)

Orchestrating the Four Components of KPMG's GRC Holistic Model

Surrounding the business processes (and the GRC Holistic Model) are four key components of equal importance—the risk profile, culture and behavior, governance, organization, and infrastructure, and enterprise assurance—that must be in balance to enable resilience. Evaluating each one in a logical order and determining how to balance them all in the context of the model are central efforts in this holistic GRC approach. By component, these efforts include:



- Risk Profile:** This component focuses on uncovering organizational risks, determining how well they are understood, assessing to what extent they have been quantified and prioritized, and knowing whether this information can be relied upon and used to support daily decision-making. The risk profile is the result of an assessment of exposure areas and potential impacts driven by risk drivers, emerging risks, and interdependencies. It is a pre-condition for an accurate and adequate design and implementation of GRC and sustaining these efforts over time.
- Culture and Behavior:** This component encompasses efforts to influence organizational culture—the basic fabric of an organization that shapes “how we do business here.” The challenge is to make risk management more a discipline that is embedded within the business (i.e., the responsibility of everyone) and less a separate department (i.e., the responsibility of a few). It begins by establishing an effective ethics and compliance program to promote the right behaviors. It also requires making sure key management tools—annual goal setting, strategic planning, budgeting, resource allocation, incentive compensation—are aligned with program objectives rather than sources of mixed messages.
- Governance, Organization, and Infrastructure:** The governance component encompasses both board and management activities. It supports the strategy and determines the effectiveness of decision making. It encompasses the architecture and management of oversight structures; authority, objectivity and stature; roles, responsibilities, and resource capabilities; escalation procedures; and information systems—the means by which the organization governs the business processes. This component also includes the use of tools and systems to enable analysis, efficient monitoring, and reporting. Efforts in this area should be reflected in the embedded controls within the business processes.
- Enterprise Assurance:** The comprehensive evaluation, monitoring, and reporting of the controls embedded within the organization to ensure their effectiveness and alignment with the organization’s strategy, performance indicators, and compliance mandates (e.g., internal audit, compliance, operational auditing).

Encircling the four components are efforts focused on integration and change, GRC technology, and continuous improvement—all critical aspects of a successful GRC implementation.

The results, **Compliance and Performance**, reflect the sustainability of the organization’s business model. These results demonstrate whether key risks have been identified, controls have been effective in managing these risks, and objectives have been met. Achieving compliance and continuously improving performance help the organization move toward the goal of resilience—the state in which it is able to deal with ongoing change, internally and externally, and adapt quickly to unforeseen circumstances. As it continues to evaluate compliance and performance outcomes against its mission and strategy, the organization can ensure alignment and make necessary adjustments.

Lead the Way: Taking Steps to Achieve Resiliency

Corporate leaders can take a comprehensive approach, based on the foundation of guiding principles, to help define the conditions necessary for GRC efforts to be effective. The guiding principles are the agreed-upon ideals of the management team that guide the development and achievement of GRC in the organization. These principles are based on concepts of accountability, responsibility, discipline, transparency, independence, integrity, and communication.

To assess the organization's capacity for achieving resilience, board members can benchmark their oversight efforts against the GRC Holistic Model, assessing whether the compliance and performance objectives are aligned with the vision and business strategy, and determine to what extent they need to challenge management's four key components—the risk profile, culture and behavior, governance, organization, and infrastructure, and enterprise assurance. They can also evaluate their own oversight objectives and determine how they may want to refine them.



Conclusion: A Call to Action

The regulatory and business environment is forcing a fundamental change in organizational culture, governance, risk management, and enterprise assurance. The choice facing organizations is not whether to implement these changes but what approach to take in implementing them. No longer able to rely on historical assumptions, organizations can choose to respond to each new challenge as it emerges. Or, they can envision and establish a comprehensive approach that can drive new compliance and performance capabilities as well as new organizational resilience to evolving circumstances.

A strategic GRC approach can help organizations navigate through “the new normal.” The organization's first step is to assess the connection between its business strategy and the GRC Holistic Model, linked with the outcomes of performance and compliance. The second step is to evaluate the four components—the risk profile, culture and behavior, governance, organization, and infrastructure, and enterprise assurance—they must be balanced with each other and with the organization's needs to enable resilience. The organization's third step is to identify areas to initiate, improve, or strengthen so it can sustain these efforts over time. Benchmarking its efforts against an array of guiding principles can help leaders perceive opportunities for such adjustments. Ultimately, the goal is to rationalize all holistic model components and establish a GRC Holistic Model that is tailored to the needs and goals of the organization.

With a GRC Holistic Model in place, leaders have the information they need to understand business risk drivers in the context of the organization's strategic positioning, anticipate and respond to new stakeholder demands, manage and implement changes efficiently, and evaluate the potential effects of emerging opportunities. GRC can thereby help an organization envision, strategize, and lead toward a new resilience, enabling it to survive and succeed in an environment that will continue to change.

How to Envision, Strategize, and Lead to Achieve Enterprise Resilience:

- Assess the connectivity between the organization's business strategy and the GRC Holistic Model
- Evaluate the alignment of the organizational strategy and GRC Holistic Model with compliance and performance results
- Identify ways to initiate, improve, or strengthen the four GRC Holistic Model components
- Chart your course

KPMG's Related Governance, Risk, and Compliance Publications

Title	Document Type	Description
Understanding and Articulating Risk Appetite	White paper	KPMG's white paper offers an approach for developing an effective risk appetite statement and identifying the main characteristics of a well-defined risk appetite.
Placing a Value on ERM	White paper	KPMG's white paper outlines approaches that could provide a focus to both justifying the ERM program and improving program performance.
The Business Case for a Risk Executive	White paper	This paper is intended to help management and the board understand the critical importance of the RE in an organization of today.
Enterprise Risk Management Overview: Complacency Is No Longer an Option	White paper	KPMG's white paper discusses our Enterprise Risk Management offering. Provides an overview of the steps that comprise KPMG's recommended approach for a practical ERM Program.
Creating Stakeholder Value in the Information Age: The Case for Information Systems Governance	White paper	KPMG's paper focuses on the impact of changes on governance over the organization's Information Systems. It stresses the importance of balancing the new requirements of controls and compliance with those of value and risk in order to assist in achieving sustainable growth.
Preparing for Regulatory Reform	White paper	This white paper provides a brief overview of the complex causes of the financial crisis as well as the regulatory themes that are emerging as multiple regulatory bodies and lawmakers, along with other financial services industry stakeholders, engage in the reform discussion.
Consumer and Investor Protection: The Intersection of Regulatory Compliance and Customer Service	White paper	This white paper provides a brief overview of the themes that are emerging with respect to consumer and investor protection from a regulatory compliance perspective. The paper also focuses on what practices constitute strong consumer and investor protection, regardless of the details of regulatory reform.
The Washington Report – Regulatory Practice Letters	Periodic Publications	These series highlight and detail current legislative and regulatory compliance issues.
Operational Risk Insurance Survey	Survey	KPMG's survey included responses from 26 insurers. More than 85 percent of the companies surveyed had revenues in excess of \$500 million. Respondents were generally Chief Risk Officers or another representative risk professional within the organization.
A Glimmer of Hope: Global Insurance Survey	Survey	This survey examines how the financial crisis is changing the attitude of the global insurance industry to risk and capital management, highlighting some key issues including preventing further losses and positioning their businesses for future growth.
Fraud Survey 2009	Survey	KPMG's Fraud Survey reveals the perceptions of U.S. senior executives as they consider fraud and misconduct risks facing their organizations during a period marked by significant economic downturn, government intervention, pressure.
Integrity Survey 2008-2009	Survey	KPMG's Integrity Survey 2008-2009 takes an inside look at corporate fraud and misconduct based on firsthand experiences and perceptions of more than 5,000 employees nationally across 13 different industries.

View these documents online at www.kpmg.com

Title	Document Type	Description
2008-2009 Anti-bribery and Anti-corruption Survey	Survey	At a time when bribery and corruption prosecutions and enforcement actions across the globe are on the rise, the results of a new KPMG Forensic SM survey suggest that multinational organizations based in the United States continue to be challenged by a number of key issues, which, if addressed, could lower the risk of violating the Foreign Corrupt Practices Act (FCPA) and other global anti-bribery and corruption standards.
Overseas Bribery and Corruption Survey 2009	Survey	KPMG Forensic's Overseas Bribery and Corruption Survey 2009 examines the U.K. and U.S. regulatory framework and assesses the impact of trends in enforcement action, both on legislation and on companies operating in multiple jurisdictions. The survey assesses companies' awareness of, and reactions to, anti-bribery and corruption issues as well as compares the responses against our original 2007 survey in this area. The survey also highlights some of the challenges multinational companies face when comparing legislation across the different jurisdictions in which they operate.
Cross Border Investigations: Effectively Meeting the Challenge	White paper	Based on extensive global research that elicited responses from senior business executives at multinational businesses in 21 countries from all continents, this document discusses the challenges that companies face when performing cross-border investigations and provides insights on how to address such issues.
Six Sigma in the Legal Department: Obtaining Measurable Quality Improvements in Discovery Management	White paper	This white paper explores how law firms and law departments can apply Six Sigma [®] to e-discovery to increase efficiencies and cut costs. With the rising volume of electronic discovery in litigation and investigations, law firms and legal departments are under increasing pressure to rein in discovery costs. Six Sigma [®] —a quality improvement methodology adopted by leading companies—offers opportunities in discovery management as well.
ERP Controls Integration: Sustaining Compliance While Implementing Change	White paper	The white paper explores how automated controls can be improved within ERP systems to achieve better internal controls integration and optimization, thereby realizing business value while sustaining compliance efforts.
Governance, Risk, and Compliance: Driving Value through Controls Monitoring	White paper	This white paper defines the concept of GRC, noting that it is more of a strategic discipline rather than a software solution. It looks at how a GRC strategy centered around controls monitoring can help prevent "surprises" while preserving shareholder value.
Driving Business Value: A Closer Look at ERP Consolidations and Upgrades	Issues Brief	This client issue brief provides a timely perspective on how ERP can be the catalyst for business transformation – and how well-positioned KPMG is to help our clients think beyond their immediate ERP upgrade or consolidation to help them transform their business so they can remain competitive with the nimbleness and flexibility needed to address their organization's short- and long-term business goals.

KPMG Contacts

Global Governance, Risk & Compliance Leader

John Farrell
Partner – United States
212-872-3047
johnmichaelfarrell@kpmg.com

Global Risk & Compliance Service Group Leader

Mike Nolan
Partner – United States
713-319-2802
mjnolan@kpmg.com

Governance, Risk & Compliance Regional Leaders

Americas

Timothy Hedley
Partner – United States
212-872-3496
thedley@kpmg.com

Deon Minnaar
Partner – United States
212-872-5634
deonminnaar@kpmg.com

Angela Hoon
Principal – United States
267-256-1970
ahoon@kpmg.com

Tony Torchia
Partner – United States
412-232-1629
atorchia@kpmg.com

EMA

Steven Briers
Partner – South Africa
+27 11 647 5673
steven.briers@kpmg.co.za

ASPAC

Sally Freeman
Partner – Australia
+61 3 9288 5389
sallyfreeman@kpmg.com.au

Peter Paul Brouwers
Partner – The Netherlands
+31 402 502325
brouwers.peterpaul@kpmg.nl

Michael Lai
Partner – China
+86 21 2212 2730
michael.lai@kpmg.com.cn

Oliver Engels
Partner – Germany
+49 69 9587 1777
oengels@kpmg.com

Stephen Lee
Partner – Hong Kong
+852 2826 7267
stephen.lee@kpmg.com.hk

Special thanks to the contributors of this white paper: John Farrell, Mike Nolan, Evelien Zonneveld, Diane Nardin, Vineeta Saxena, Jarrod Bassman, Debbie Dacey LoPiccolo, Jesal Asher, and Brandon Wetzel.