KPMG
cutting through complexity

Vital Risk Insights

kpmg.com

KPMG INTERNATIONAL

Using business intelligence software to monitor indicators of governance, risk and compliance

Success in today's global marketplace demands that leading companies keep up with the remarkable pace of technological change and innovation, particularly in regard to business intelligence software. Capturing market share often involves taking advantage of social media solutions such as apps on smart phones and tablets, interactive visualization, and scenario modelling. Such solutions are also becoming important tools for tracking the effectiveness of governance, risk management, and compliance activities.

A company that has not yet acted upon and put into place such solutions has an opportunity to design executive dashboards that integrate performance data, risk indicators, and information related to internal control and corporate governance, risk management, and compliance management (GRC). For those companies that do have such dashboards in place, the opportunity exists to expand their scope by including other GRC stakeholders.

Management must keep the board informed of the facts of the company's operating performance, which includes information such as the status of key risks, assurance on critical controls, details of material losses, and developments in the area of compliance.

GRC – where should we be?

Because it is a highly visible member of society in both the local and global sphere, the modern company is expected to uphold community values. Its leadership and board of directors are responsible for enacting and enforcing policies that help ensure the welfare and interests of both its stakeholders and society. Such policies are commonly managed through a structured and formalized GRC system characterized by such aspects as board committees, scheduled reports to leadership and the board and a program of risk management that includes an infrastructure for monitoring the internal controls.

Given the importance of the board's mandate to protect stakeholder interests, it is vital that the board is kept abreast of key facts relating to risks, internal controls, losses and trends. The board has a right to be kept fully advised of significant initiatives by management and that such information will be provided in a timely manner. GRC systems support this reporting and monitoring process based on four principles of good governance: accountability, responsibility, fairness and transparency.

In order for the value of GRC to be fully realized, its information must be reported objectively, and presented in a way that demonstrates any potential impact on the company's strategic objectives, performance targets and financial framework. This implies that information about risks, controls and losses is expressed in numeric terms and in terms of fact-based key risk indicators.

GRC – what are we doing well?

Structured programs to manage risk have become widely accepted in large corporate enterprises, characterized by processes such as formal risk assessments, programs of control testing, and internal risk reporting. Specialized functions address inherent risk exposures ranging from market risk to sustainability risk. Board oversight is provided through governance structures and supported by periodic reporting by management. Compliance management is embedded within the fabric of leading companies and rigorous audit programs help ensure that operations meet regulatory requirements. Generally, accepted standards and processes of GRC have helped to improve these kinds of practices around the world.

GRC – What are our challenges?

Management bias and viewing risk subjectively pose a challenge to many companies. Since management is rewarded for good news and not bad through a program of incentives, the temptation exists to focus on its achievements and downplay mistakes. Overly optimistic reporting can result in incomplete or biased assessments that can harm or have an even fatal impact on a company. Internal reporting processes that depend entirely upon personal interpretation, traffic light ratings and free-form style may expose a company to this problem. This kind of vulnerability is compounded when submissions are presented with no empirical evidence to support them. An increasing number of companies have addressed the challenge of subjectivity and management bias by implementing real-time reports based on actual data. Continuous monitoring also addresses this challenge and provides the ability to respond to identified issues more rapidly.

Thus, instead of depending upon an annual declaration by management on the status of internal controls, companies rely on real-time reports based on actual data pulled from operating systems.

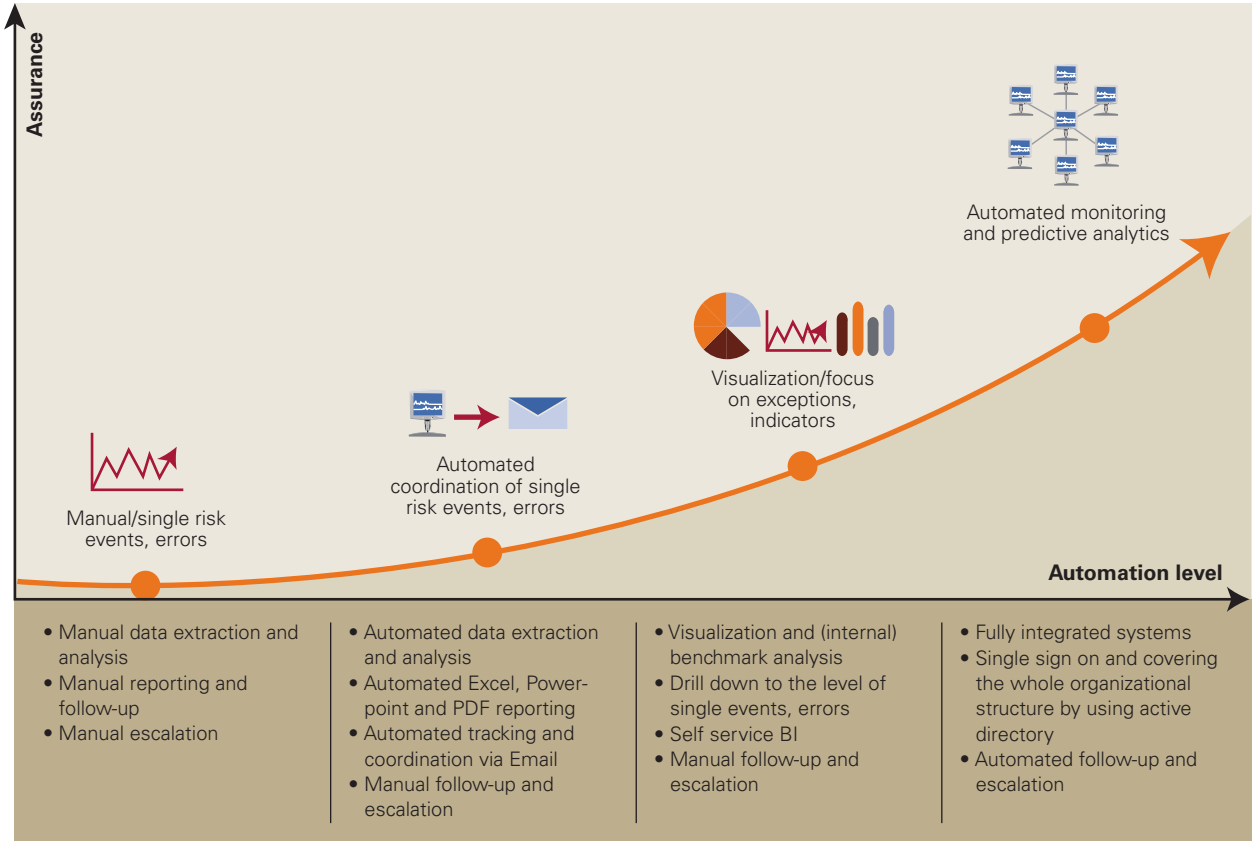
Quantifying non-financial risks is considered difficult if not impossible by many management teams, so essential techniques such as setting risk tolerance thresholds, matching risk values to financial imperatives, and measuring risk concentrations, are often not used at all. Choosing the right indicators of risk is often seen as problematic and too much of a challenge, causing management to adopt simplistic ranking scales in compensation.

Reports and submissions to GRC oversight functions and committees are typically produced on an infrequent or periodic basis rather than in real time. Although substantial time and expense may be incurred in producing such information, a lack of current data may inhibit deep insights into the connection between risk and performance. A single view of GRC and assurance is often not provided to board committees. With no standardized framework, content or methodologies, and these disparate functions can often appear fragmented and disconnected from one another.

A culture of good risk management is notoriously difficult to achieve when these functions are positioned outside of the core business, and weaknesses in management buy-in will be evident in the quality and substance of reporting. Ratings of risks, controls and losses may remain static or not evaluated accurately for fear of being exposed by peers.

GRC requires sound processes and structures in order to function optimally, and the maturity model illustrated above illustrates that a company's GRC maturity normally evolves over time. The importance of having good quality data and master-data for advancing GRC maturity cannot be over-stated. Where there is an existing business intelligence technology in place, it makes good sense to include a meaningful GRC perspective.

KPMG Maturity Model: Continuous Monitoring



> A culture of good risk management is notoriously difficult to achieve when these functions are positioned outside of the core business, and weaknesses in management buy-in will be evident in the quality and substance of reporting.

> The integrated nature of governance, risk management, and compliance dashboards enables its users to gain new insights about connected themes, patterns and trends across the organization, and glean information that is currently not delivered.

How do we get there?

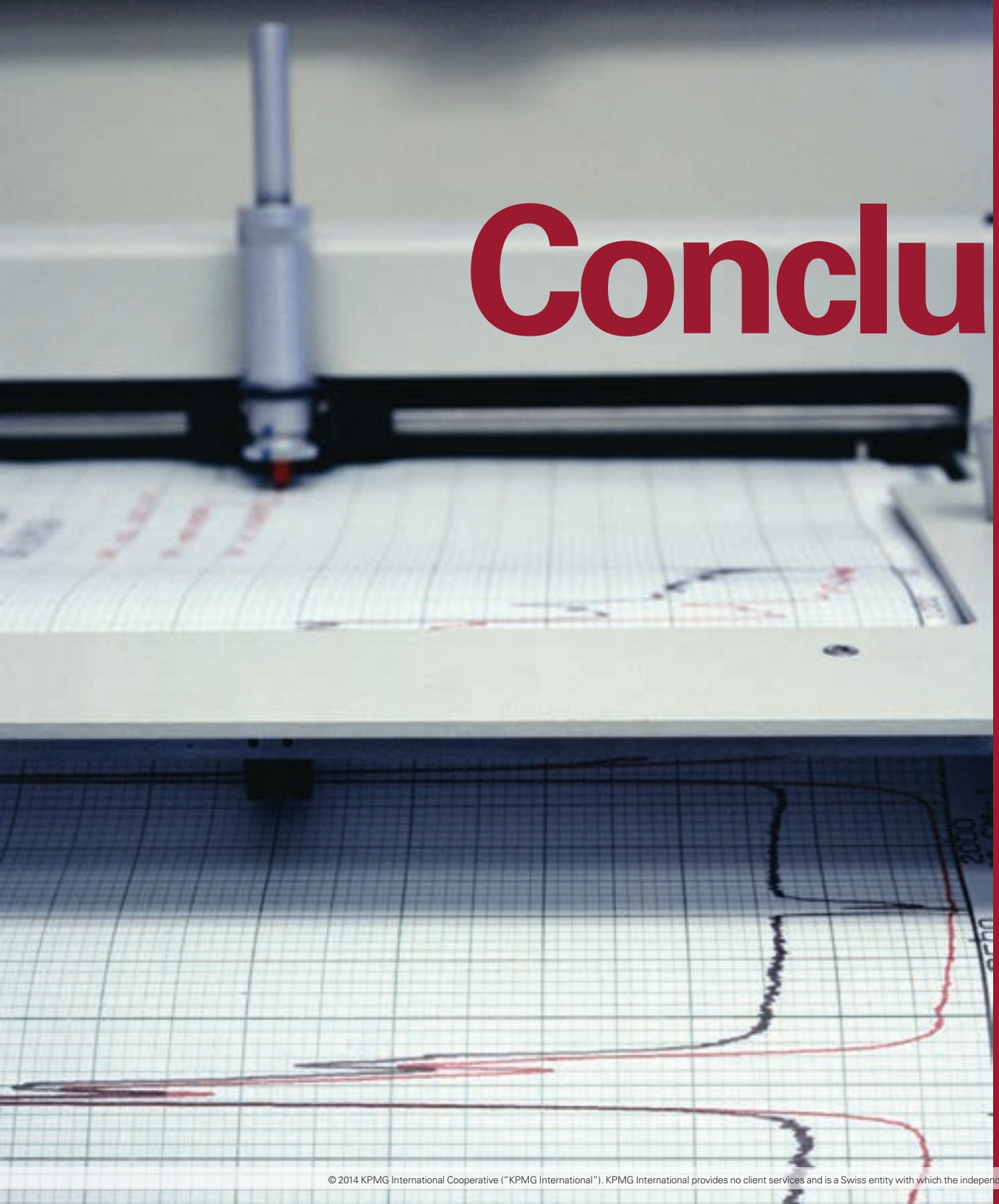
Leading companies are placing more emphasis on dynamic reporting, numeric data, business indicators and measured information, all of which provide deeper insight into risk and allow management to perform governance responsibilities more effectively.

Indicators are extracted automatically from operating systems and visualized in customized dashboards using business intelligence software. This provides real-time risk information and helps enable more rapid intervention and decision-making should the need arise. Risk intelligence dashboards can be customized for risk owners and for different role-players within GRC functions.

Instead of ploughing through a bewildering array of wordy documents and spreadsheets, management can use business intelligence software to assemble GRC indicators into one integrated workspace on a screen. There are no restrictions to the type of indicator that may be assembled for GRC dashboards, loss data, audit data, key risk indicators, insurance figures, legal claims, ethics data, survey results, safety statistics, audit scores, regulatory indices, and more.

Measuring the potential net impact of risk with smart indicators in real time helps an organization to leverage value from the GRC program, and aligns its processes to the company's strategic objectives. This can encourage companies to take a more analytical approach and it can assist with identifying opportunities, quicker responses to adverse trends and shaping new improvement initiatives. The integrated nature of GRC dashboards enables its users to gain new insights about connected themes, patterns and trends across the organization, and glean information that is currently not delivered. Aligning GRC information to the company's performance targets leverages the function's value to management and the board of directors.

*Information reflected is entirely fictional and for display purposes only.



Conclusion

The current trend of including GRC activities in one portfolio represents a serious challenge. The subject matter now managed within the GRC portfolio has expanded to include sustainability, forensics, internal audit, insurance, safety, security, business continuity, project risk, stakeholder management, and many other well-established corporate functions. Companies are learning that using smart indicators within business intelligence software is an effective way to keep your finger on the pulse of performance trends, variance and change.

Internal stakeholders with a justifiable interest in GRC and accurate and real-time status and progress reports now includes boards of directors and their committees; executives, operations, risk managers, internal audit executives, assurance providers, and specialist risk and control functions. Business intelligence strategies offer customization and personalized information for these different users. Information, charts and tables are easy to format and data can be imported by easy drag-and-drop from documents and spreadsheets. Business intelligence software has become a driving force and a stakeholder expectation as an integral part of the landscape of GRC. Its availability on mobile devices makes it even more attractive and accessible to management.

Contacts

Americas:

John Farrell
Global ERM/GRC Lead Partner
KPMG in the US
T: +1 212 872 3047
E: johnmichaelfarrell@kpmg.com

Fiona Grandi
Partner, ERM/GRC
KPMG in the US
T: +1 415 963 7812
E: fgrandi@kpmg.com

Deon Minnaar
Americas ERM/GRC
Lead Partner
KPMG in the US
T: +1 212 872 5634
E: deonminnaar@kpmg.com

EMA:

Peter Paul Brouwers
Global GRC technology and
EMA CA/CM Partner
KPMG in the Netherlands
T: +31 40 2502346
E: brouwers.peterpaul@kpmg.nl

Steven Briers
Partner, Risk Consulting
KPMG in South Africa
T: +27 82 719 0517
E: steven.briers@kpmg.co.za

AsPac:

Brad Styles
Partner, Management Consulting
KPMG in Singapore
T: +65 6411 8818
E: bradstyles@kpmg.com.sg

Damion Keasey
Associate Director, IARCS
KPMG Australia
T: +61 2 9335 7173
E: damionkeasey@kpmg.com.au

kpmg.com/socialmedia

kpmg.com/app

Download on the App Store

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

Designed by Evalueserve.

Publication name: Vital Risk Insights. Publication number: 120940. Publication date: April 2014